الجمـــــهوريـــــة الجـــزائريـــــة الديـــمقراطيـــــة الشعبيـــــة
PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
وزارة التعـلـيـــــم العـالـــــي و البـــحث العلـــــــــمي
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
جـــــامعـة عمـــــــار ثليـجي بالأغـــواط
UNIVERSITY AMAR TELIDJI OF LAGHOUAT

كـــلـيـــــــة العلـــــــــوم
FACULTY OF SCIENCES
DEPARTMENT OF COMPUTER SCIENCE

Malicious messages detection and exclusion mechanisms in Vehicular Networks (VANETs)

Thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science (LMD)

Thesis defended on January 03, 2017

Kerrache Chaker Abdelaziz

Jury members

Mr Mohamed Bachir YAGOUBI	Professor	UATL	President
Mr Mustapha Réda Senouci	Associate Professor	EMP	Examiner
Mr Fayçal Bouyakoub	Associate Professor	USTHB	Examiner
Mr Abderrahmane Lakas	Professor	UAEU	Examiner
Mr Nasreddine Lagraa	Professor	UATL	Advisor

Laghouat, January 2016

To my parents, brothers, sisters, and wife.

Learn knowledge and teach it to humanity, learn to be respectful and peaceful and be down to earth to people who taught you and to who you are going to teach, and don't be dictators of knowledge so that your ignorance will presume your knowledge.

-Omar Ibn AL-Khattab-

Acknowledgments

This four-year-long journey was not made alone, being the result of a cooperative learning process where my advisors, my colleagues and several researchers worldwide also made an important contribution.

This thesis would not have been possible without the kind support of my two advisors: Professor Nasreddine Lagraa and Professor Carlos Tavares Calafate. Thanks for your never-ending flow of ideas, energy and efforts. Your contributions and clear-mindedness were only surpassed by your patience towards me. I could never forget your help and support, your trust and friendship.

I would like to express my gratitude to my research advisor at GRC -Networking Research Group-, Professor Juan-Carlos Cano, whose support has also been very important for the completion of this thesis.

Special thanks to Professors Mohamed Bachir Yagoubi, Abderrahmane Lakas, Mustapha Reda Senouci, and Fayçal Bouyakoub for accepting the evaluation of my thesis despite their occupations, it was an honor for me to work with them.

I would also like to thank the remaining members of the Computer Networks Groups (GRC), led by Professor Pietro Manzoni, thank you all: JorgeE, JorgeH, JorgeZ, Ali, Subhadeep, Oscar, Leonardo, Danilo, Sergio, Andres, Willian, Dima, David, Jesus, Cesare, Francisco, and Andrea.

I am grateful to my colleagues at Laboratoire d'Informatique et de Mathématiques (LIM): Sofiane, Ilyes, Abdallah, Lakhdar, Bouziane, Zinelabidine, Younes, Abdelmadjid, Sami, Leila, Soumia, Aicha, and Ines. The joy and enthusiasm they had for their work was motivational for me.

I thank all the members of my family and my future wife for all their love and encouragement. Thanks for always being so supportive, encouraging, patient and for accompanying me in my growth as an individual, teaching me ethical and moral principles that will prevail for all my life.

Finally, I offer my regards to all my teachers since my first day at school and to all those who supported me during the completion of this thesis. Thanks to you all...

Chaker Abdelaziz Kerrache
València, July 2016

ملخّص

شبكات المركبات الذكية تدعم العديد من التطبيقات المتنوعة, هذا الأمر يجعلها عرضة لعدة هجمات تتنوع بتنوع التطبيقات. هذه الأطروحة سمحت لنا بتحديد أهم المشاكل والهجمات الالكترونية التي تستهدف شبكات المركبات الذكية.

ركّزنا في هذا العمل على الهجمات الداخلية القادرة على تجاوز أنظمة الحماية التقليدية المعتمدة على التشفير حيث أن المهاجم في هذه الحالة يمتلك كلمة المرور وكل الوسائل لولوج مختلف تطبيقات الشبكة. تسيير الثقة المستوحاة من العلوم الاقتصادية تعتبر حلا أمنيا اضافيا قادرا على مجابهة الهجمات الداخلية وكذا التكيّف مع خصائص شبكات المركبات الذكية.

اقترحنا في هذه الأطروحة ثلاثة حلول أساسية تعتمد على مبدأ إدارة الثقة (**TFDD, T-VNets, RITA**) ودرسنا قدرة كل حل على مواجهة وايقاف مختلف أنواع الهجمات مثل الثقوب السوداء, الانذارات المغلوطة, التحالف ...الخ.

فيما يتعلق بالمقترح الأول (**TFDD**) فهو يستند على تركيبة مترابطة من الوحدات, كل منها يقول بمهمة محددة. بالإضافة الى ضمان نقل البيانات عبر أقصر طريق آمن (**TFDD**) بإمكانه العمل حتى في ظل وجود نسبة عالية من العقد المهاجمة.

(**T-VNets**) **هو** أول نموذج إدارة ثقة يعتمد على النظام الأوروبّي الموحد **ETSI ITS** فيما يخص الاتصالات بين المركبات الذكية. على غرار (**TFDD**) هذا النموذج قادر على مجابهة هجمات مختلفة دون الاستعمال المفرط لموارد الشبكة.

أما المقترح الثالث (**RITA**) فهو يختلف عن كل الحلول السابقة بقدرته على مجابهة وايقاف الهجمات الذكية وكذا قدرة العقد المهاجمة على التأقلم مع أنظمة الحماية.

نتائج المحاكاة أظهرت كفاءة مقترحاتنا في كشف العقد (المركبات) المهاجمة مع الاستعمال العقلاني لموارد الشبكة.

الكلمات المفتاحية: أنظمة النقل الذكي, شبكات المركبات الذكية, إدارة الثقة.

Abstract

The wide range of applications supported by Vehicular Adhoc NETworks (VANETs) make them vulnerable to various security threats. This thesis has enabled us to identify what are the main threats, adversary models, and security mechanisms associated to VANET environments. We focused mainly on inside attackers able to bypass the classical cryptography-based security mechanisms. Inspired by economic science, trust management is considered as an alternative security solution able to handle authorized and authenticated attackers. Furthermore, trust management has shown its high adaptability to VANET features (i.e, open communication medium, very high mobility, etc.).

In order to handle inside attacks on VANETs, we have proposed three different trust establishment solutions: TFDD, T-VNets, and RITA. For each of these solutions, we have studied different attacker behaviors, as well as heterogeneous types of attacks including Denial of Service (DoS), Blackholes, Grayholes (selective forwarding), Coalition, Platooning, Badmouthing, and detection-avoidance strategies. Furthermore, all proposals are hybrid trust models able to revoke dishonest entities and filter out malicious messages, while considering different communication scenarios and applications.

Regarding the first proposal - TFDD - it is based on a modular architecture, being able to ensure a reliable unicast and multi-hop communication even under DoS attacks, and with a high ratio of attackers.

Our second proposal - T-VNets - is the first trust model able to take advantage of the messaging services provided by the ETSI ITS standard. Through continuous traffic and trust estimations, T-VNets is able to handle not only DoS attacks, but also coalition attacks, without exhausting the network resources.

Concerning our third proposal - RITA - it differs from existing trust-based security solutions by also being able to handle intelligent attack behaviors. In another words, to accounts for attackers able to adjust their behaviour with full awareness of the deployed security rules. Thanks to the introduced risk estimation metric, RITA is able to face not only intelligent attackers, but also those attacks where false recommendations and fake alerts are spread. In addition to the aforementioned proposals, our contributions also include two trust-based lightweight routing and dissemination schemes for VANET environments.

Simulation results evidence shows the efficiency of our proposals at both ensuring high detection ratios and reduced overhead.

Keywords: Intelligent Transportation Systems, Vehicular Networks, Trust

management.

Resumen

La amplia gama de aplicaciones soportadas por redes ad hoc vehiculares (VANETs) hacen que estas sean vulnerables a diversas amenazas de seguridad. Esta tesis nos ha permitido identificar cuáles son las principales amenazas, modelos adversos y mecanismos de seguridad asociados a ambientes de VANET. Nos hemos centrado principalmente en los atacantes internos capaces de eludir los mecanismos de seguridad basados en la criptografía clásica. A partir de las ciencias económicas, la gestión de confianza se considera como una solución de seguridad alternativa capaz de afrontar a los atacantes autorizados y autenticados. Además, la gestión de seguridad ha demostrado su alta adaptabilidad a las características de las VANET (medio de comunicación abierto, red con alta movilidad, etc.).

Con el fin de afrontar ataques en las VANETs, hemos propuesto tres soluciones diferentes basadas en confianza: TFDD, T-VNets y RITA. Para cada una de estas soluciones, hemos estudiado los comportamientos diferentes del atacante, así como tipos heterogéneos de ataques de denegación de servicio (DoS), Blackholes, Grayholes (reenvío selectivo), coalición, Platooning, Badmouthing, y estrategias para evitar la detección. Además, todas las propuestas son modelos de confianza híbridos capaces de revocar entidades deshonestas y filtrar los mensajes maliciosos, teniendo en cuenta escenarios de comunicación y aplicaciones.

Con respecto a la primera propuesta "TFDD", se basa en una arquitectura modular, que permite asegurar un proceso confiable de comunicación unicast y multi-salto con un alto número de atacantes.

Nuestra segunda propuesta "T VNets", es el primer modelo basado en confianza que toma ventaja de los servicios de mensajería proporcionados por el estándar "ETSI ITS ". A través de continuas y reales estimaciones de tráfico, T-VNets es capaz de manejar no sólo los ataques DoS, sino también los ataques en coalición, sin agotar los recursos de red.

Respecto a la tercera propuesta "RITA", esta se diferencia de las soluciones de seguridad existentes (basadas en confianza), por su capacidad de manejar conductas de ataque inteligente. En otras palabras, t representa atacantes capaces de ajustar su comportamiento con pleno conocimiento de las reglas de seguridad desplegadas. Gracias a la métrica de estimación de riesgo introducido, RITA es capaz de afrontar no sólo a los atacantes inteligentes, sino también los ataques donde hay falsas reputaciones y alertas. Además de las mencionadas propuestas, en nuestra contribución también se incluye dos métodos ligeros de enrutamiento y difusión basados en confianza para entornos VANET.

Los resultados de las simulaciones muestran la eficiencia de nuestras propuestas, asegurando un alta probabilidad de detección con una reducida sobrecarga en la red.

Palabras clave: Sistemas de Transporte Inteligentes, Redes Vehiculares, Gestión de confianza.

Résumé

La large gamme d'applications prise en charge par les réseaux véhiculaires Adhoc (VANETs) les rend vulnérables à diverses menaces. Cette thèse nous a permis d'identifier quelles sont les principales menaces, les modèles d'adversaires et les mécanismes de sécurité liés aux environnements VANETs. Nous nous sommes concentrés principalement sur les attaquants internes (attaquants autorisés et authentifiés) capables de contourner les mécanismes classiques de sécurité basés sur la cryptographie. Inspirés des sciences économiques, la gestion de confiance est considérée comme une solution alternative de sécurité capable de traiter et de détecter les attaques internes. En outre, la gestion de confiance a montré sa capacité d'adaptation aux fonctionnalités des VANETs (support de communication partagé, très grande mobilité, etc.).

Afin de faire face aux attaques internes dans les VANETs, nous avons proposé trois solutions basées sur la gestion de confiance: TFDD, T-VNets et RITA. Pour chacune de ces solutions, nous avons étudié les différents comportements des attaquants, y compris le Déni de Service (DoS), trous noirs, transfert sélectif, coalition, convoi d'attaquants, Médisances et stratégies d'évitement de la détection. En outre, toutes les propositions sont des modèles de confiance hybrides capables de révoquer les entités malhonnêtes et filtrer les messages malicieux, tout en tenant compte des différents scénarios de communication.

Concernant la première proposition - TFDD - elle est basée sur une architecture modulaire, étant en mesure d'assurer une monodiffusion et une communication en multi-sauts fiables même sous les attaques DoS et avec un taux élevé d'attaquants.

Notre deuxième proposition - T-VNets - est le premier modèle de confiance basé sur les messages fournis par le standard européen ETSI ITS. Par le biais du trafic continu et des estimations de confiance, T-VNets est capable de faire face non seulement aux attaques DoS, mais aussi aux attaques de la coalition, sans épuiser les ressources réseau.

Concernant notre troisième proposition - RITA - elle diffère des solutions existantes de sécurité basées sur la confiance en étant aussi capable de gérer les comportements d'attaque intelligents. En d'autres termes, le cas où les attaquants sont capables d'ajuster leur comportement avec conscience des règles de sécurité déployées. Grâce à la métrique d'estimation des risques introduits, RITA est capable de faire face non seulement aux attaquants intelligents, mais aussi aux fausses recommandations et alertes.

Les résultats de simulation montrent l'efficacité de nos propositions sur les

deux rapports de détection des attaquants et leur messages malicieux ainsi que la preservation des resources réseaux.

Mots clés: Systèmes de Transport Intelligents, Réseaux Véhiculaires, Gestion de confiance.

Contents

1 Motivation, Objectives and Organization of the Thesis **1**
1.1 Motivation . . . 1
1.2 Objectives of the Thesis . . . 3
1.3 Organization of the Thesis . . . 3

2 Overview of Vehicular Adhoc NETworks (VANETs) **5**
2.1 Intelligent vehicles and autonomous driving: Vision and Reality . . 5
2.2 Vehicular networks and inter-vehicle communication: Terminology 6
2.3 Standards and communication technologies . . . 7
2.3.1 Fundamental Differences Between Europe and United States 8
2.4 Vehicular networks applications . . . 10
2.5 Vehicular networks challenges . . . 10
2.6 Summary . . . 10

3 Vehicular networks security issues and existing Trust management solutions **13**
3.1 Overview . . . 13
3.2 VANET security requirements and threats . . . 14
3.2.1 VANET security requirements . . . 14
3.2.2 VANET threats . . . 15
3.2.3 Distinguishing Cryptography from Trust . . . 20
3.3 Trust management for VANETs . . . 22
3.4 Attacks bypassing trust management . . . 29
3.5 VANET trust models' evaluation methods . . . 30
3.6 Open research issues . . . 36
3.7 Summary . . . 36

4 Trust Establishment Proposals for Vehicular Networks **37**
4.1 Overview . . . 37
4.2 TFDD: a Trust-based Framework for Reliable Data Delivery and DoS defense in VANETs . . . 37
4.2.1 System model . . . 37
4.2.2 Proposed modular solution . . . 38
4.2.2.1 Neighboring Evaluation Module . . . 40
4.2.2.2 Messages Classifier Module . . . 42

4.2.2.3 Intrusion Detection Module (IDM) . . . 42
4.2.2.4 Delayed Verification Module . . . 44
4.2.2.5 Decision Module . . . 46
4.2.3 Performances evaluation . . . 51
4.2.3.1 Simulation parameters . . . 51
4.2.3.2 Results discussion . . . 51
4.3 T-VNets: a novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS . . . 59
4.3.1 T-VNets architecture . . . 59
4.3.1.1 Trust metrics . . . 61
4.3.1.2 Adversary model . . . 62
4.3.2 Proposal details . . . 62
4.3.2.1 Vehicle-to-vehicle trust . . . 62
4.3.2.2 RSU-to-vehicle trust . . . 66
4.3.2.3 Global trust computation . . . 67
4.3.2.4 ETSI-based trust establishment . . . 68
4.3.3 Trusted communication and data routing . . . 75
4.3.4 Performance evaluation . . . 77
4.3.4.1 Network performance . . . 79
4.3.4.2 Security performance . . . 81
4.3.4.3 Dishonest nodes detection efficiency . . . 81
4.4 Trusted opportunistic alerting system . . . 84
4.4.1 Inter-vehicular trust establishment . . . 85
4.4.2 Opportunistic alerts dissemination . . . 88
4.4.3 Simulation results . . . 89
4.5 Summary . . . 94

5 Enhancing VANET trust to address detection avoidance strategies 95
5.1 Overview . . . 95
5.2 RITA Overview . . . 96
5.3 RITA details: Trust and risk estimation . . . 98
5.3.1 Vehicle-to-vehicle trust computation . . . 98
5.3.1.1 Direct trust computation . . . 99
5.3.1.2 Indirect trust computation . . . 99
5.3.2 Risk estimation . . . 101
5.4 Multi-hop information dissemination using RITA . . . 102
5.4.1 Multi-hop dissemination of safety messages . . . 102
5.4.2 Multi-hop dissemination of data messages . . . 105
5.5 Performance evaluation . . . 107
5.5.1 Determining the optimal parameter settings . . . 108
5.5.2 RITA attackers detection performance . . . 110
5.5.3 RITA messages delivery performance . . . 111
5.6 Summary . . . 113

6 Future Trust models for VANET: Design and discussion 116
6.1 Overview . . . 116
6.2 Hierarchical Adaptive Trust Establishment Solution for Vehicular Networks . . . 116
6.2.1 Data design . . . 117
6.2.2 Inter-vehicular trust computation . . . 117
6.2.2.1 Direct trust computation . . . 118
6.2.2.2 Vehicles recommendations combination . . . 120
6.2.2.3 Roadside unit recommendation computation . . . 120
6.2.2.4 Trusted authority recommendation computation . 121
6.2.3 Simulation results . . . 122
6.3 Integrating the user honesty factor through Online Social Networks (OSNs) . . . 125
6.3.1 Social trust and socially-aware networking . . . 125
6.3.2 Trust in Online Social Networks (OSNs) . . . 127
6.3.3 Trust computation in Vehicular Networks and Online Social Networks . . . 127
6.3.4 Socially-aware trust model overview . . . 129
6.3.5 Trust computation . . . 130
6.4 summary . . . 132

7 Conclusions, Contributions and Future Works 134
7.1 Contributions Related to the Thesis . . . 136
7.1.1 Journals . . . 136
7.1.2 International Conferences . . . 137
7.2 Future works . . . 139

List of Algorithms

1 Neighboring evaluation module's tasks 41
2 Intrusions' detection process 43
3 Neighbors's trust updates using the analysis sub-module 49
4 Attackers detection using the analysis sub-module 49
5 Data delivery process 50
6 Best next hop selection 51
7 Vehicles cooperation evaluation 65
8 Segments' trust and traffic estimation 72
9 Trust-aware DEN messages dissemination process 74
10 Events reporters honesty using DENMs similarity 75
11 Trust-aware inter-vehicular communication 76
12 DENM multi-hop dissemination 89
13 Safety messages multi-hop dissemination using RITA 105
14 Data messages multi-hop dissemination using RITA 107

List of Figures

1.1 An example of several applications and communication technologies interconnected to establish an ITS scenario [ETS]. 2

2.1 Intelligent vehicles vision. 6
2.2 V2X communication scenarios. 6
2.3 ITS communication technologies [ETS]. 7
2.4 Major standardization efforts for VANET [HL08]. 8
2.5 Frequency channel allocation. 9
2.6 Europe versus U.S. standards for VANET [HL10]. 9
2.7 VANET applications. 12

3.1 Application-oriented VANET security threats. 16
3.2 Main VANET security attacks. 17
3.3 Inside and outside attackers in VANET. 21
3.4 VANET security requirements and trust management use cases. . . 23
3.5 VANET security threats and attacks against trust management. . 30
3.6 Intelligent dishonest behavior. 31
3.7 Evaluation tools of existing trust models for VANETs. 32

4.1 Message format 38
4.2 Overview of the proposed framework 39
4.3 Allocation of the initial trust value 41
4.4 Traffic priorities defined in the WAVE standard 42
4.5 Statistical information gathered 43
4.6 Different node behaviors in terms of traffic injected on the channel throughout time 44
4.7 Proposed trust building scheme which combines different direct, indirect and role-based metrics 46
4.8 The two cases of clear behavior 47
4.9 Cases of uncertain/doubtful behavior 48
4.10 Impact of the DVM on the detection ratio of dishonest nodes . . . 53
4.11 Impact of the RL (official vehicles) on the detection ratio of dishonest nodes 54
4.12 Impact of dishonest vehicles on the detection ratio 54
4.13 Malicious messages' lifetime (in number of hops) 55

4.14 Impact of the DVM on the false positives concerning dishonest nodes detection . . . 55
4.15 Impact of the RL (official vehicles) on the false positives concerning dishonest nodes detection . . . 56
4.16 Impact of the DVM on the false negatives concerning dishonest nodes detection . . . 56
4.17 Impact of the RL (official vehicles) on the false negatives concerning dishonest nodes . . . 57
4.18 Evolution of the average trust of attackers . . . 58
4.19 Bandwidth usage ratio in the case of a DDoS attack . . . 59
4.20 Proposed trust establishment architecture. . . . 60
4.21 Adversary model, best path selection and routing different cases. . 63
4.22 Vehicle-to-vehicle trust modules. . . . 63
4.23 RSU-to-vehicle trust modules. . . . 66
4.24 Global trust computation. . . . 68
4.25 Events' trust, segments' trust, and traffic estimation modules. . . . 69
4.26 An example of traffic density and segment's trust information. . . 70
4.27 Additional Fields. . . . 71
4.28 DENM format. . . . 73
4.29 Trusted communication and data routing modules. . . . 76
4.30 Link duration estimation. . . . 77
4.31 Simulated scenario of Valencia city, Spain. . . . 78
4.32 Average end-to-end delay of unicast data messages. . . . 79
4.33 Packet delivery ratio. . . . 80
4.34 Generated Overhead. . . . 80
4.35 Dishonest nodes detection ability during 300s of simulation time. . 81
4.36 Dishonest nodes detection for different densities. . . . 82
4.37 Dishonest nodes detection effectiveness when varying their number. 83
4.38 Generated false positive. . . . 83
4.39 The different trust metrics' impacts. . . . 84
4.40 Generated Overhead by T-VNets in different versions. . . . 85
4.41 The proposed protocol stack. . . . 86
4.42 Proposed DENM extension. . . . 86
4.43 Simulated scenario of Laghouat city, Algeria. . . . 90
4.44 Detection performances for different vehicular densities when 15% or 25% the vehicles are dishonest. . . . 91
4.45 Alert messages loss ratio for different densities when 0%, 15% and 25% of the vehicles are dishonest. . . . 92
4.46 Wrong decisions ratio for different densities when 15% and 25% of the vehicles are dishonest. . . . 92
4.47 Detection performances compared to TROUVE and FACT proposals for different vehicle densities (Φ=25%). . . . 93
4.48 Message loss ratio when compared to TROUVE and FACT proposals for different vehicle densities (Φ=25%). . . . 93

5.1 Intelligent dishonest behavior. . . . 96

5.2 Proposed risk-aware modular trust establishment architecture ensuring reliable message dissemination. 97
5.3 Proposed beacon format extension. 100
5.4 Safety message extension. 103
5.5 Per-vehicle dissemination areas. 104
5.6 Simulated scenario of Laghouat city, Algeria. 108
5.7 Required number of interaction for an efficient trust establishment. 109
5.8 Required number of neighbors for an efficient trust establishment. 110
5.9 α factor selection. 111
5.10 *RITA* detection performance for different vehicular densities in the presence of intelligent attackers. 112
5.11 Detection performances compared to AECFV and T-CLAIDS for different densities (35% dishonest vehicles). 112
5.12 Detection performances compared to AECFV and T-CLAIDS for different dishonest vehicles ratios (400 vehicles scenario). 113
5.13 RSUs distribution in the simulated scenario of Laghouat city, Algeria. 114
5.14 Average end-to-end delay required to reach an RSU for different vehicle and RSU densities (35% of dishonest vehicles). 114
5.15 Packets loss ratio for different vehicle and RSU densities (35% of dishonest vehicles). 115

6.1 Piggybacking of recommendation contents. 117
6.2 Traffic priorities defined in the WAVE standard (also known as Access Categories). 118
6.3 Proposed architecture. 119
6.4 Example of dishonest nodes detection. 121
6.5 Simulated scenario of Laghouat city, Algeria. 122
6.6 Detection performance for variants of the proposed scheme when varying vehicular densities (25% of dishonest vehicles). 123
6.7 Detection performances when varying vehicular density for 15% and 25% of dishonest vehicles. 124
6.8 Wrong decisions ratio of our proposal for different densities when 25% of the vehicles are dishonest. 124
6.9 Average end-to-end delay for our proposal under different vehicular densities when 25% of the vehicles are dishonest. 125
6.10 Dishonest vehicles trust variability throughout a 200-vehicle simulation (25% dishonest). 126
6.11 Honest vehicles trust variability throughout a 200-vehicle simulation (25% dishonest). 126
6.12 Socially-aware networking overview [XLL+15]. 128
6.13 Trust establishment in OSNs. 129
6.14 VANET trust vs OSN trust. 130
6.15 Proposal Overview. 131
6.16 An example trust evaluation distribution for 50 nodes. 132
6.17 An example of trust evaluation distribution with 50 nodes. 132

7.1 Main shortcomings of VANETs' Trust models. 135

List of Tables

2.1 Main VANET challenges. 11

3.1 Security threats target and solutions category. 20
3.2 Features of Trust-based and Cryptography-based solutions. 22
3.3 Trust-based solutions common classification. 23
3.4 Main trust-based solutions. 24
3.5 Simulation tools and performance evaluation metrics. 34

4.1 TFDD Notations 38
4.2 TFDD simulation parameters 52
4.3 T-VNets Notations. 64
4.4 T-VNets simulation parameters. 78
4.5 Simulation parameters. 90

5.1 RITA simulation parameters. 107

6.1 Simulation settings. 122

List of Acronyms

AECFV An accurate and efficient collaborative intrusion detection framework to secure vehicular networks

CAM Cooperative Awareness Message

C-ITS Cooperative Intelligent Transport Systems

DDoS Distributed Denial of Service

DENM Decentralized Environmental Notification Message

DTR Direct Trust

ETSI European Telecommunications Standards Institute

ETR Event's Trust

GTR Global Trust

ICT Information and Communication Technologies

IDM Intrusion Detection Module

ITR Indirect Trust

ITS Intelligent Transport Systems

LS Link Stability

OSN Online Social Network

PKIs Public Key Infrastructures

RITA RITA: RIsk-aware Trust-based Architecture for collaborative multi-hop vehicular communications

RSU RoadSide Unit

TA Trusted Authority

TFDD A Trust-based Framework for reliable Data Delivery and DoS defense in VANETs

THH High threshold

THL Low threshold

Tr Trust evaluation

T-CLAIDS Collaborative trust aware intelligent intrusion detection in vanets

T-VNets A novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS

VANETs Vehicular Adhoc NETworks

Chapter 1

Motivation, Objectives and Organization of the Thesis

1.1 Motivation

According to statistics provided by the *Association for Safe International Road Travel* (ASIRT[1]), more than 1.3 million people die in road traffic accidents each year worldwide. In addition, it is estimated that more than 90% of fatal accidents could be avoided through cooperative driving. However, such cooperation-based system requires communication technologies not available in our classical vehicles. Thus, many new concepts have been introduced such as intelligent vehicles, autonomous vehicles, self-driving cars, and cooperative driving; all of them refer to vehicles with more than 100 processors, sensors, and antennas, enabling them to detect, gather, analyze, and share different kinds of information [VBC13]. The inter-vehicular communication system is now known as Vehicular Ad hoc NETworks (VANETs). Furthermore, this inter-vehicular system is only a part of a wider system encompassing all kinds of transportation systems, which is known as Intelligent Transportation Systems [MM99].

Intelligent Transportation Systems (ITS) involves all types of communication in vehicles, between vehicles (e.g. car-to-car), and between vehicles and fixed locations (e.g. car-to-infrastructure). However, ITS are not restricted to vehicular networks, but they are also including the use of information and communication technologies (ICT) for rail, water and air transport, along with navigation systems (see Figure 1.1).

Vehicular Ad hoc NETworks (VANETs) have always been considered the keystone of Cooperative Intelligent Transportation Systems (C-ITS) [Fes14]. Such communication systems have been deployed mainly to enhance safety on roads and to improve the passengers' comfort. Similarly to other open and dynamic networks, vehicular ad hoc networks suffer from different security threats, where

[1] http://asirt.org/initiatives/informing-road-users/road-safety-facts/road-crash-statistics (Visited the 4th of May 2016)

Figure 1.1: An example of several applications and communication technologies interconnected to establish an ITS scenario [ETS].

the most dangerous ones are those targeting safe message generation and dissemination.

Many solutions have been proposed to ensure a secure and trusted delivery of such messages, as well as comfort messages. Nevertheless, finding a balanced tradeoff between security, efficiency, and network requirements remains an open challenge. Furthermore, existing solutions for securing vehicular communication can be divided into two categories: trust-based solutions and cryptography-based solutions, including the standardized 1609.2 and ETSI ITS security models [Com13, ETS12]. Cryptography-based solutions are known to provide excellent results for most security needs. However, all solutions in this category generally focus on outside attackers and introduce additional delays, limiting their usefulness in highly dynamic and delay sensitive networks such as VANETs [Pat16].

Trust management solutions [BFIK99], which are based on economic science, have attracted the research community because of their two main features:

- They can ensure highly trusted communications while promoting low-delay delivery without exhausting network resources.
- They can face inside attackers that bypass all cryptography-based security measures deployed.

Also notice that, for safety critical cases, exchanged traffic should be sent in clear without any encryption, same as most of VANET applications. Taking all the aforementioned issues into account, establishing trust to enhance vehicular communications security seems like a worthwhile strategy.

1.2 Objectives of the Thesis

In this thesis, we propose showing how trust management can enhance vehicular communications security, highlighting its adaptability to vehicular environments, as well as possible extensions to face new kinds of threats.

The first objective of this thesis is to provide an overview and identify the main challenges associated to vehicular networks, their applications and communication technologies.

The second objective is to identify what are the most dangerous security threats, and to study the trust management applicability in VANET contexts, together with its features compared to the classical cryptography-based security models.

The main objective of this thesis is to propose and evaluate efficient trust establishments schemes able to face most VANET internal threats with respect to its nature and applications. Accommodating our proposal to ongoing standardization efforts is one of our key goals.

In this thesis, we also show what are those threats able to bypass trust management solutions, while proposing an approach able to face such threats. Finally, we try to take advantage of the upcoming socially-aware networking paradigm to consider the human honesty factor in our trust establishment proposals.

1.3 Organization of the Thesis

This thesis is organized as follows: in the next two chapters we make a background introduction to Intelligent Transportation Systems (ITS), vehicular networks, and the main VANET security threats, including a review of the existing trust-based solutions discussing their advantages and drawbacks. Hence, in chapter 2 we provide an overview of Vehicular Adhoc NETworks in which we briefly describe the history of VANETs, introduce commonly used terms, and refer to the main communication technologies, together with the main VANET applications and open challenges.

Chapter 3 is dedicated to VANET security challenges; in particular, in this chapter we show what are the main security requirements and threats, and we also present what are differences between cryptography and trust. In addition, this chapter provides an adversary-oriented review of the existing trust-based solutions and their evaluation methods. We conclude the chapter by pointing out those issues that remain open, along with some concluding remarks.

Chapter 4 details our two main trust establishment proposals for vehicular networks that are able to face both types of availability-related threats. Our proposals, namely TFDD and T-VNets, rely on both inter-vehicular communications and vehicle-to-RSU (RoadSide Unit) communications. Both proposals introduce a relay selection strategy adaptable to different VANET applications. While TFDD acts separately to the existing standards, T-VNets takes advantage of messaging services standardized by the ETSI ITS group to establish trust, hence clearly reducing the additional trust establishment overhead. In this chapter we also describe our safety-oriented proposal, which is mainly dedicated to the

alert-spreading problem. For both proposed solutions, we provide both a security-related and a network-related performance analysis to determine their effectiveness when compared to existing solutions.

In chapter 5 we describe our proposal, called RITA, where we extended the usual trust establishment procedure with a risk estimation analysis to handle intelligent attacks. Such attackers keep over the detection threshold, only providing positive recommendations about each other, and they spread false alerts. We show experimentally that RITA is able to achieve significant detection improvements when facing such attackers.

Chapter 6 focuses on the human honesty factor consideration. We start by first describing our hierarchical three-level trust establishment proposal, and we then extend it using online social networks. Through this social dimension, drivers honesty degree is then classified into three categories: trusted, doubted, and untrusted. Afterward, the human honesty factor is associated to the overall trust evaluation to enhance the detection efficiency and reduce the margin of error.

Finally, in Chapter 7, we present a summary of the main results of this thesis, along with some concluding remarks. We also include a list of the publications related to the thesis, and we comment on future research works that can be derived from the work here presented.

Chapter 2

Overview of Vehicular Adhoc NETworks (VANETs)

In this chapter, we explain some notions and notations related to VANETs, intelligent vehicles, existing communication technologies and standards, together with the main VANET applications and security issues.

2.1 Intelligent vehicles and autonomous driving: Vision and Reality

Intelligent vehicles and autonomous driving paradigms have been presented at first by General Motors at the 1940 World's Fair[1]. For many reasons, including the 2nd World War and the reduced number of vehicles worldwide, the development of such cooperative systems has been delayed, having again started to draw attention by the end of the 80's and beginning of the 90's, with the focus oriented to self-driving vehicles.

In ITS solutions, vehicles share their status and their view of the current road and traffic conditions with other vehicles to improve traffic safety, efficiency and comfort (see Figure 2.1). The main messages exchanged can be divided into two types:

- Periodic status information.
- Event-triggered emergency warnings.

These messages ensure two main goals:

- Warning the driver in time to react.
- Providing the car with enough information to act autonomously.

[1] The 'future highway' at 14:27: https://www.youtube.com/watch?v=tAz4R6F0aaY (Watched the 11th of January 2016)

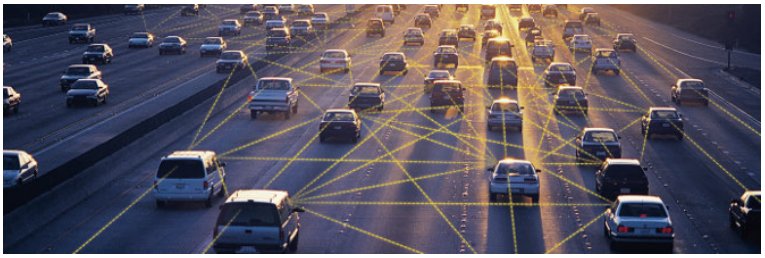


Figure 2.1: Intelligent vehicles vision.

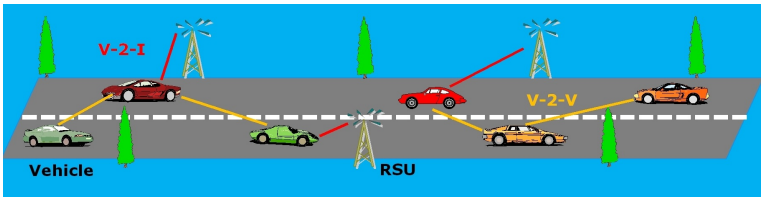


Figure 2.2: V2X communication scenarios.

2.2 Vehicular networks and inter-vehicle communication: Terminology

From the many notions and terms introduced in VANET-related literature, four of them are particularly relevant:

- ***Cooperative ITS (C-ITS):*** A cooperative intelligent transportation system is a subset of the global ITS system mainly represented by vehicular networks.
- ***Vehicle-to-vehicle (V2V):*** This paradigm represents the direct communications among every pair of vehicles.
- ***Vehicle-to-Infrastructure (V2I):*** This term, also known as V2R for Vehicle-to-Roadside unit, represents the communication between vehicles and the infrastructure deployed on roadsides. These RoadSide Units (RSUs) are divided into static and semi-static infrastructures, and they are deployed in a sparse or strategical manner.
- ***VANET:*** As shown in figure 2.2, the VANET paradigm represents the combination of all above terms, starting by inter-vehicular communication (V2V), extending it to vehicles-to-infrastructure communication (V2I), and ending by creating a cooperative intelligent transportation system.

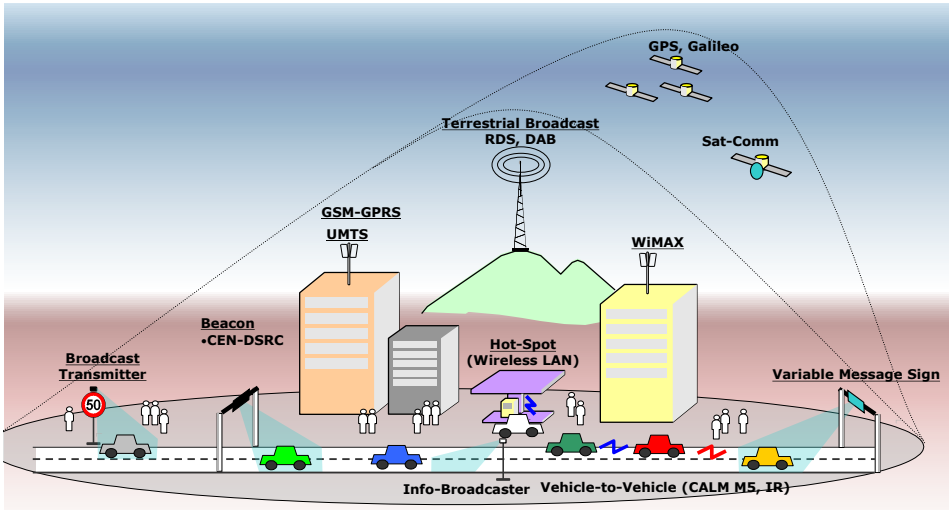


Figure 2.3: ITS communication technologies [ETS].

2.3 Standards and communication technologies

As illustrated in figure 2.3, three levels of communication technologies are involved in ITS: (i) Short range (from 10 to 30 meters), (ii) Medium range (from 300 to 800 meters), and (iii) Long range (more than 1 km).

For short-range communications the main technologies adopted are Infrared and Radar. This range is used by a few applications like road tolling and borders' access control. More detailed information about short-range communications is available on the CEN DSRC (5.8 GHz) standard.

Regarding long-range communications, available technologies belong to the cellular family of solutions (3G/4G) to support some applications including safety applications with moderate time constraints, transport efficiency, and vehicle-2-backoffice reports.

For VANETs and VANET-related applications, the used set of technologies typically rely on medium-range microwave technology. In particular, the specific standard for VANET communications is IEEE 802.11p, which is associated to the 5.9 GHz frequency. This standard is integrated into wider-scope standards such as Wireless Access in Vehicular Environments (WAVE), Communications Access for Land Mobiles (CALM), and Dedicated Short Range Communication (DSRC).

The IEEE 802.11p standard has been developed mainly to support time critical safety, transport efficiency, as well as vehicle-to-vehicle and vehicle-to-infrastructure communication applications. Furthermore, for comfort applications such as Internet hot spots, stationary vehicles, and other non-safety critical applications, the IEEE 802.11 b/g (WLAN) standard is also used within the 2.4 GHz frequency band.

Major standardization of VANET protocol stacks is taking place in the U.S., in Europe, and in Japan, corresponding to their dominance in the automotive indus-

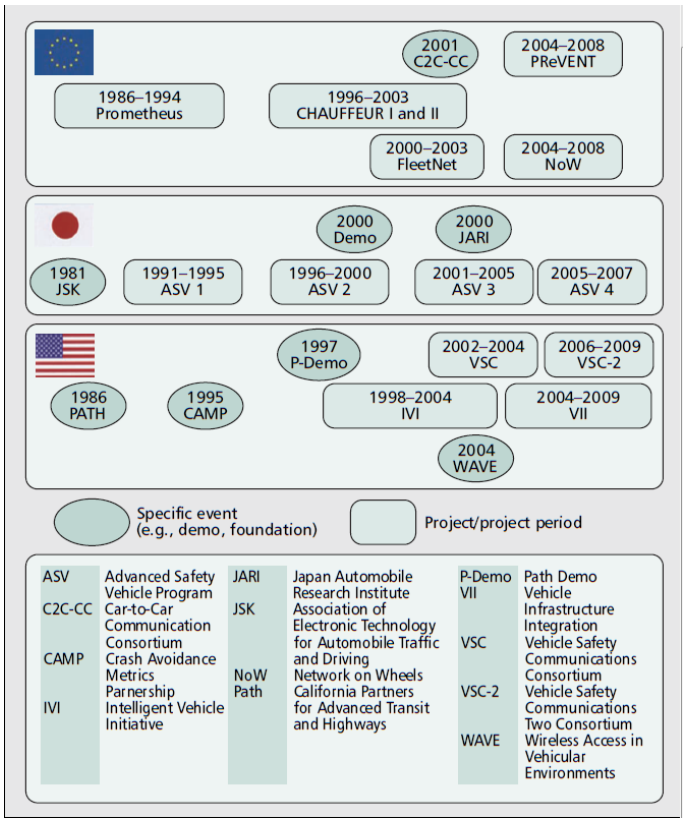


Figure 2.4: Major standardization efforts for VANET [HL08].

try [SD14]. Figure 2.4 presents an overview of pioneering activities and milestones that show the evolution of the topic of VANET research around the globe.

2.3.1 Fundamental Differences Between Europe and United States

As illustrated in figure 2.5, in the U.S., the IEEE 1609 WAVE (Wireless Access in Vehicular Environments) protocol stack builds on IEEE 802.11p WLAN operating on seven reserved channels in the 5.9 GHz frequency band. The WAVE protocol stack is designed to provide multi-channel operation (1609.4)(even for vehicles equipped with only a single radio), security (1609.2), and lightweight application layer protocols. Within the IEEE communications society, there is a technical committee on Vehicular Networks and Telematics Applications (VNTA). The charter of this committee is to actively promote technical activities in the field of vehicular networks, V2V, V2R and V2I communications, standards, communications-enabled road and vehicle safety, real-time traffic monitoring, intersection manage-

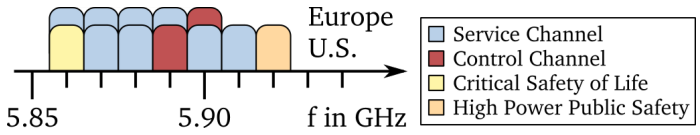


Figure 2.5: Frequency channel allocation.

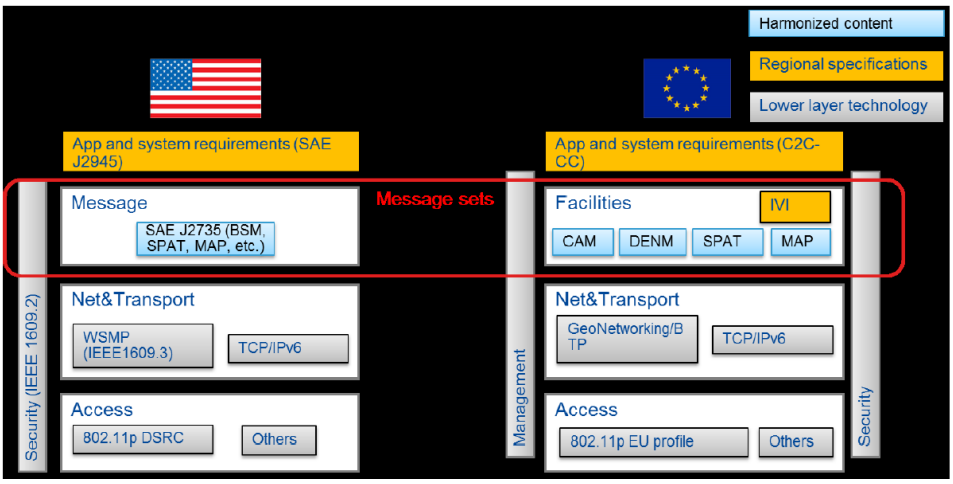


Figure 2.6: Europe versus U.S. standards for VANET [HL10].

ment technologies, future telematics applications, and ITS-based services.

In Europe, ETSI ITS builds on a variant of the same radio technology with some adaptations operating on up to five reserved channels in the 5.9 GHz frequency band. The ETSI ITS G5 protocol stack is designed to provide multi-radio multi-channel operation, security, and a complex hierarchy of higher layer protocols integrating a broad range of basic services.

Figures 2.6 illustrates differences and common aspects between both European an U.S. standards for VANET.

Over the medium access control layer, the differences are either withing the networking and transport layer where the U.S. standard uses the Wave Short Message Protocol (WSMP) (1609.3). Whereas, Europe standard opted for a GeoNetworking strategy. The messaging services layer called 'Facilities' in the European standard and 'Message' in the U.S. standard. These layers rely on the peiodically exchanged and event triggered messages (CAM and DENM) for the European standard. Whereas, in the U.S. standard, the messages playing the same role are

called Basic Safety Messages (BSM).

For the security concerns both sides of the Atlantic uses almost the same specifications based on 1609.2 standard [sec12b] with some upates in the european ETSI TS 102 731 standard.

As specified in [sec12a], most of IEEE 1609.2 standard services are mapped to the european ETSI TS 102 731 standard including the enrolement, authorization, encryption, and decryption of single messages. However, some services such as: Security associations, accountability, misbehaving ITS-S reports are not directly mapped to the European standard. For instance, in ETSI TS 102 731 Accountability services are provided at a higher layer than is addressed by IEEE 1609.2 Association. Hence, this service is not directly mapped.

For CAM, and DENM the originator shall sign outgoing messages using IEEE 1609.2 [sec12b] at the facilities layer in the stack. The CAM or DENM content shall form the payload of the ToBeSignedData element of the SignedData structure defined in clauses 6.2.7 and 6.2.3 of IEEE 1609.2 [sec12b] respectively, same as BSM type 1 (CAM in Europe) and BSM type 2 (DENM in Europe).

2.4 Vehicular networks applications

The number of VANET applications is growing at a steady pace, most of them focusing on enhancing road safety. However, comfort and efficiency applications, such as Internet access and map updates, can also be supported alongside with safety applications. VANET applications can also be classified based on the required level of cooperation among vehicles, or also based on their timing constraints, as illustrated in figure 2.7.

Notice that the most important VANET applications belong to the safety area, in particular those requiring a high level of cooperation among vehicles and reduced message-exchange delays.

2.5 Vehicular networks challenges

Many challenges and issues arise when attempting to deploy vehicular network solutions. Some of them are environmental, such as the contraints of urban scenarios compared to rural environments, while others are related to industrial costs, and yet others are human-related contraints. Table 2.1 summarizes the main challenges of VANET for the sake of completeness.

In addition to all the aforementioned challenges, and similarly to what occurs in other types of networks, a wide range of security issues must likewise be handled efficiently when moving towards a secure and efficient VANET. Security issues will be pointed out in the next chapter.

2.6 Summary

In this chapter, we presented an overview of vehicular adhoc networks, including the main smart-vehicle features, along with frequently used terms, applications,

Table 2.1: Main VANET challenges.

Issue	**Description**
Mobility	• High speeds causing rapid and frequent topology changes. • Limited communication time between nodes. • Highly variable network density.
Human factor	• How to present data/recommendations to the driver without distraction and information overload. • Different drivers = different capabilitites, reaction times, etc. • Resistance to have driving taken out of our hands.
Interoperability	• Cooperation and interoperability between car manufacturers and transport organizations.
Connectivity	• Choice of antenna and their placement. • Choice of communications frequency and bandwidth.
Positioning	• Accuracy of of-the-shelf GPS receivers.
Market penetration rate	• How to integrate unequipped vehicles (at the beginning).
Timing	• How to make sure that access to the medium is ensured whenever needed (MAC protocol). • How to avoid congestion and safety packet dropping. • How implement and maintain QoS.
Reliability	• How to make sure that the data is correctly received by the intended recipient. • How to solve the conflict between timing and reliability.
Cost	• Choice of communications technology. • Number of antennas.
Urban environment	• Connectivity issues due to buildings. • High number of communication nodes. • Presence of vulnerable road users. • Integration into the 'smart city' concept. • Risk scenarios: intersection warning, vulnerable road user warning, etc.
Rural environment	• High speed. • Limited physical safety features (e.g. guardrail, separation between driving directions etc.). • Sparse traffic. • Risky scenarios: overtaking, bad weather, low driver attention, animals, etc.
Highway environment	• Very high speed. • Potentially very high node density. • Risky scenarios: blind spots, lane changes, rear-end collisions.

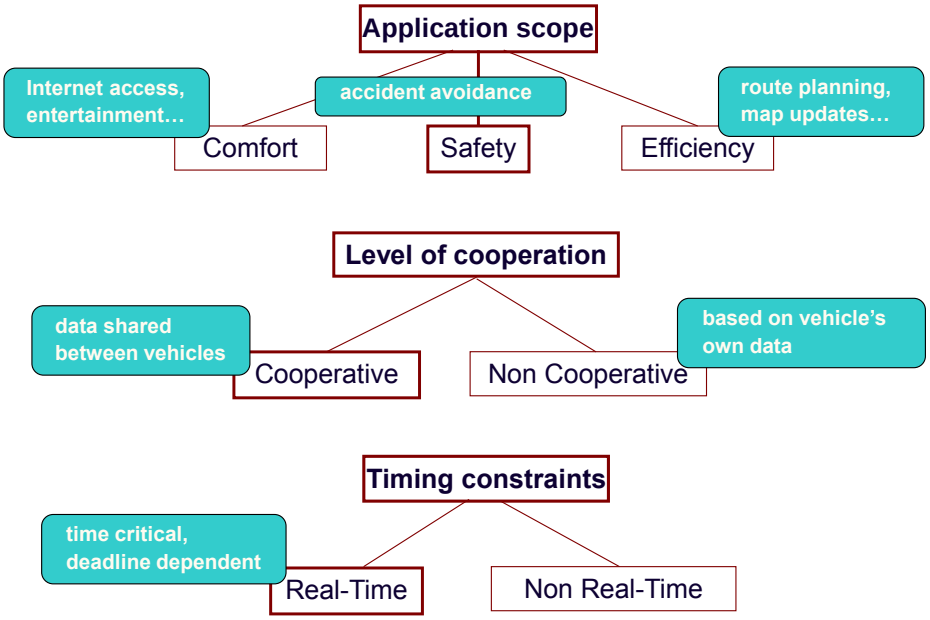


Figure 2.7: VANET applications.

and challenges, thereby serving as a guide to the reader. The next chapter will be dedicated to security issues in VANETs, and also to trust management enhancements required when facing inside attackers.

Chapter 3

Vehicular networks security issues and existing Trust management solutions

3.1 Overview

Ensuring secure and trusted communications within Vehicular Ad hoc NETworks (VANETs) is a complex task due to the different threats to be addressed [RH05], where the most dangerous ones are those seeking safety and alert services.

Tremendous efforts have been made by researchers at both academia and industry to provide security solutions for all kinds of networks including VANETs. Most of the existing security solutions for VANETs inherit cryptography efficiency in terms of secure and confidential communications, and they use different software and hardware components to reach their goals such as certificates [LHH08], signatures [GBW07], Public Key Infrastructures (PKIs)[WLLS10], intrusion detection systems [LHSW04], and trusted third parties [HL06].

On the other hand, in some critical cases like the high mobility and the absence of deployed infrastructures, cryptographic solutions cannot perform as well as expected because they mostly fail in highly dynamic and infrastructureless environments. In addition, if an authorized and authenticated user becomes malicious or is under the control of an attacker, classical cryptography solutions are easily overtaken. Hence, to fill the gap of cryptography against inside attackers, trust management is usually adopted. It was inspired from economic science [But91, MDS95], and can be used for different networks and applications. Trust can be defined as a subjective belief of a peer about other peers belonging to the same society or geographical zone [RK05].

For the VANET case, trust establishment is based on the evaluation of direct historical interactions, as well as on the indirect recommendations among vehicles that are gathered. Thus, trust evaluation is mostly made based on the recent history regarding data exchanges, and does not have any negative impact on message

treatment and transmission delays.

Existing trust models for VANETs are generally classified into entity-oriented, data-oriented, and hybrid trust models depending of the revocation target, which can be either dishonest entities, malicious messages, or both of them [Zha11].

As mentioned above, in the scope of VANETs, trust mostly addresses inside attackers as cryptography has already showed its efficiency in handling outside unauthorized attacks attempts. Hence, trust management and cryptography can be seen as complementary components in securing vehicular communications. In other words, trust mainly deals with inside attackers in those situations where cryptography completely fails, also contributing to enhance cryptography in case of delay-sensitive infrastructureless environments, which is the case of a VANET.

In this chapter we clearly point out when and where trust is a better choice than cryptography, and the opposite. We also explain the main features, differences, advantages and drawbacks of both trust and cryptography. In addition, an adversary-oriented survey of the existing trust establishment solutions is also provided. We show some specific attacks trying to bypass both cryptography and trust solutions, and how the latter can be enhanced to detect such threats. Finally, we show how the existing trust models for VANETs are usually evaluated.

3.2 VANET security requirements and threats

Same as all kinds of networks, in addition to the security concerns, VANET security requirements are divided into four main axes: availability, authenticity, confidentiality, integrity, and non-repudiation [RH07]. However, in VANET environments, attacks addressing availability are the most dangerous since they directly affect safety-critical situations. In the following sections, we describe the different VANET security requirements, and we then classify the main existing threats.

3.2.1 VANET security requirements

Securing vehicular communications is a complex issue, with plenty of challenges to be addressed which can be grouped in six different requirements.

1. **Availability:** it is the most important factor to account for in VANETs since it is directly related to all safety applications. Maintaining the network's functionality is an availability issue, and so a security framework should ensure the presence of the required information or service, as well as the communications bandwidth, at any time. Hence, the most dangerous attacks taking place in VANETs address availability more than any other security aspect. Both trust-based and cryptography-based approaches allow securing the network in the presence of an infrastructure, although trust-based approaches are a better option for fully distributed scenarios.

2. **Authenticity:** it is also among the major security aspects to account for. It includes identification, authentication, and access control. By adopting security certificates and signatures, it represents the first line of defense

against any external danger. Vehicle authenticity can be ensured by using cryptographic solutions.

3. **Confidentiality:** Through the certificates and the shared public keys all exchanged messages can be encrypted and, hence, all peer-to-peer communications can become confidential (illegible) for all intermediate vehicles. However, in a VANET context, safety messages and neighboring discovery messages (beacons) should remain clear and readable by all receiving vehicles. Also notice that confidentiality is ensured through cryptography solutions, and not trust solutions.

4. **Integrity:** Data integrity and trustiness is about ensuring that messages have not been dropped, modified, reduced or injected by an intermediate node. Achieving these requirements is a difficult task in any distributed system. In the specific case of VANETs, it can be ensured through the public key infrastructure and cryptography revocation mechanisms.

5. **Non-repudiation:** it is useful when a certain node tries to deny that it was sending specific messages. Signatures are the main technique used to avoid this kind of attack. Hence, only cryptography approaches can satisfy this particular requirement.

6. **Privacy:** Vehicle privacy is an important issue in VANETs, as it includes both position and identity privacy. Pseudonym changing techniques are the main solution adopted to provide this security service.

To satisfy all the aforementioned requirements, cryptography and trust have been combined together in many approaches [SS15, PBH+07, SH16]. In fact, they are also used together in secure key distribution [Yeu06, WMWY15] and privacy-preserving communications [FKL16, WZWG16].

3.2.2 VANET threats

Same as any open network using a shared medium, VANETs suffer from a variety of vulnerabilities. In fact, the damage associated to some security attacks can withhold the different applications from performing correctly. Even if the target is a specific service, for sure other related services will be affected as well. Since VANET applications can be classified into safety, security, and infotainment, we provide in the following sections an application-oriented classification of the main VANET threats. In particular, this classification shows which kind of applications attacks are affecting the most. Anyway, we should keep in mind that every attack has a negative impact on all kinds of applications, and not only on one of them.

Figure 3.1 summarizes the main existing threats, and which applications are affected the most according to the three categories defined below:

- Attacks addressing security and confidential communications;
- Attacks addressing safety applications;
- Attacks addressing infotainment applications.

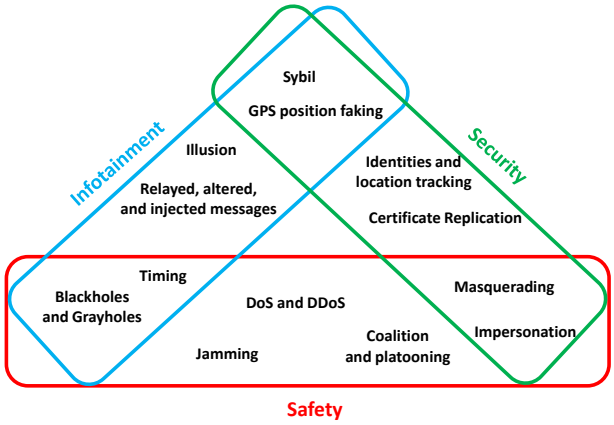


Figure 3.1: Application-oriented VANET security threats.

1. **Attacks addressing security and confidential communications:**

   Achieving secure and confidential communications is a main concern on all networks, also including safety and infotainment. Thus, VANET security suffers from many threats including, but not limited to, the certificate replication attack, the eavesdropping attack, and identity/location privacy attacks.

   Certificate Replication attack:

   In this attack a dishonest node uses a certain number of replicated certificate at the same time to avoid being traced/tracked by the authority or other vehicles. Dishonest vehicles can behave smartly also by discarding any detected certificate to avoid being black-listed or identified using this detected certificate (see figure 3.2 (I)).

   Eavesdropping attack:

   Recently known as APT for Advanced Persistent Threat [Dal09, Tan11], eavesdropping attacks occur when a dishonest vehicle with a valid certificate behaves as a spy, therefore gathering all possible information. Notice that the impact of such a passive behaviour on the network is not instantaneous or very evident, but it can nevertheless be the cause of many attacks on privacy and cyber security [WTL05, BL04].

   Attacks on privacy:

   Vehicles/Driver identities/location privacy should always be ensured. Various kinds of attacks can be launched against privacy-preserving systems, including both tracking systems and the advanced persistent threat described

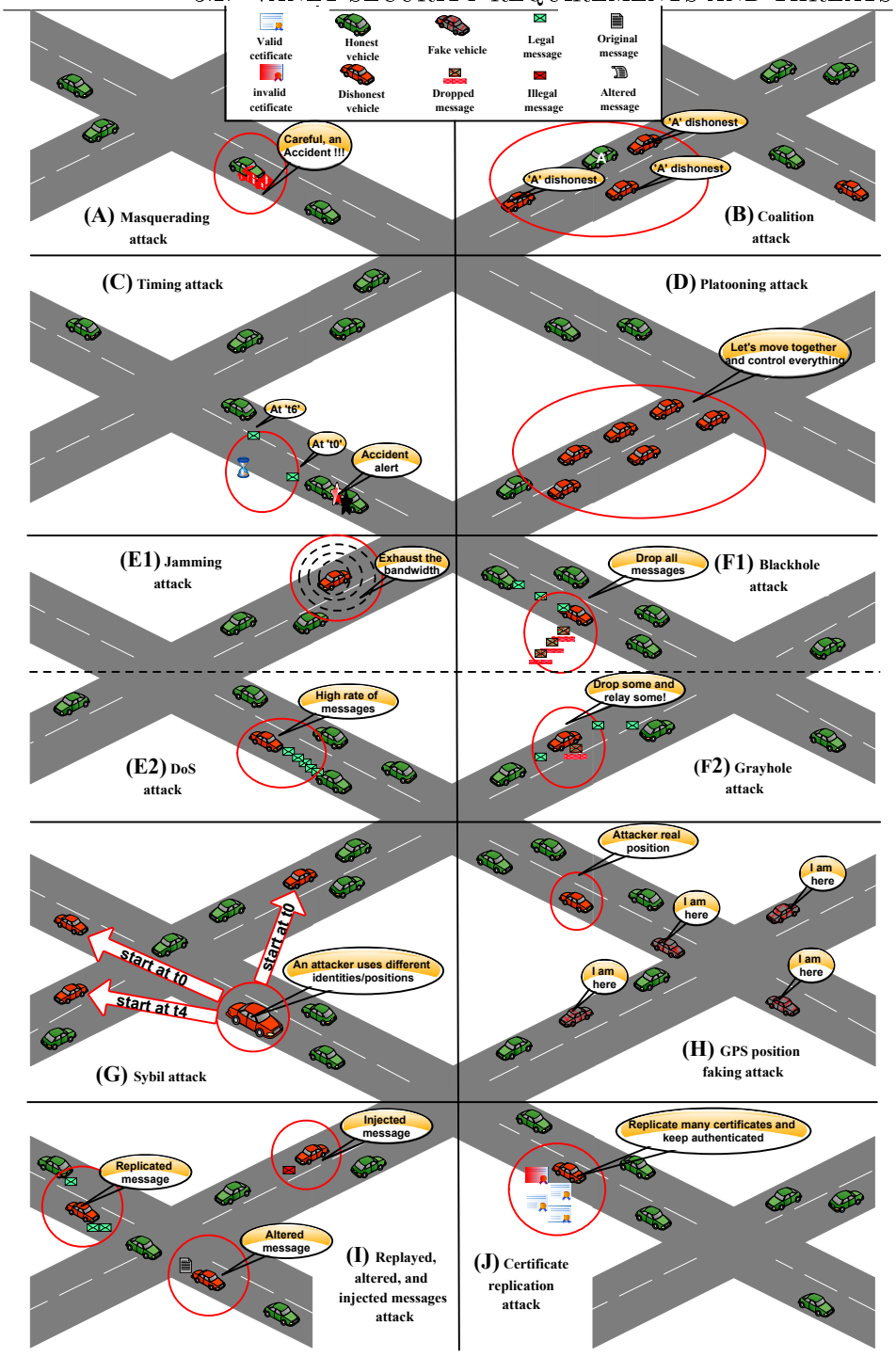


Figure 3.2: Main VANET security attacks.

above. Similarly to eavesdropping attacks, the impact of attacks addressing privacy appear in a delayed manner, meaning that an attacker can use its target identity, location, or certificate to launch another attack without being detected.

2. **Attacks that endanger safety applications:**

   Safety applications are the main aim of cooperative ITS. Since all safety applications are based on multi-hop and delay-sensitive information exchange, attacks focused on this category are mostly related to the channel occupation.

   Denial of Service attacks:

   This famous type of attack known as DoS occurs when a set of dishonest vehicles send a high rate of messages, effectively blocking all possible actions by the target. This attack can be launched in a distributed manner by many attackers simultaneously, hence becoming a distributed DoS (DDoS) which is similar to the coalition attack with a target/time synchronization [BH07](See figure 3.2 (F2)).

   Jamming attack:

   As shown in figure 3.2(F1), this attack is similar to the DoS attack, but now the target is the shared bandwidth. It occurs when a dishonest vehicle tries to hold channel access continuously through different strategies including beacons, frequency changing, medium access backoff cheating, and alert injection. This is among the most dangerous attacks for safety applications since it avoids that valid safety alerts are disseminated.

   Coalition and platooning attack:

   This attack occurs when a group of dishonest vehicles situated in the same geographical area or moving together collaborate for malicious purposes such as excluding honest nodes from network operations, malicious bandwidth usage, or service consumption in the case of vehicular clouds. Figures 3.2 (A) and (C) illustrate these types of attacks.

   Betrayal attack:

   Similar to the masquerading attack, the betrayal attack occurs when a honest vehicle suddenly turns into a malicious node and starts sending malicious messages or fake alerts.

3. **Attacks on infotainment applications:**

   Infotainment applications are all those related to passengers' comfort, and most of them are based on relay selections strategies for message exchanges. Bellow we list the most dangerous attacks on infotainment applications.

   Replayed, altered, and injected messages attack:

   As illustrated in figure 3.2(J), dishonest vehicles can replicate many copies of the same message, modify the message, or create and inject new messages in the system while acting as a relay node for inter-vehicular communication.

These attacks can clearly reduce the performance of all network applications, as well as the exchanged data trustiness.

Illusion attack:

This attack is mostly related to hardware components, and it occurs when an authenticated attacker implements some vulnerabilities at the sensing level. Hence, generated information is not valid.

4. **Common attacks against both security and safety applications:**

   In addition to the aforementioned attacks, security and safety applications also share some common vulnerabilities including the following:

   Masquerading attack:

   The adversary in this attack is a dishonest vehicle that uses a valid identity/certificate called mask to take advantage of network resources. Hence, it can perform maliciously without being detected (See figure 3.2 (B)).

   Impersonation attack:

   This attack occurs when a vehicle provides its valid identity to an attacker. This way, the latter can launch attacks able to bypass the authentication process.

5. **Common attacks against both security and infotainment applications:**

   Some attacks have almost the same severity level on both security and infotainment applications, and the main attacks are the Sybil and the GPS position faking attacks.

   Sybil attack:

   This attack is similar to the botnet attack where an attacker is able to manage a certain number of controlled/penetrated vehicles, and so launches attacks using these vehicles as shown in figure 3.2(H). Hence, the attackers can be either honest vehicles that lack security measures, or dishonest vehicles.

   GPS position faking attack:

   The second attack in this category is illustrated in figure 3.2(G), and it occurs when an attacker broadcasts fake positioning information which can punish certain applications based on geographical routing, or even nodes located at that same falsified position.

6. **Common attacks against both safety and infotainment applications:**

   Last but not least, some attacks are dangerous for both safety and infotainment applications. These attacks are mainly timing attacks, blackholes and grayholes.

   Timing attack:

the delay in the packet delivery process can be even more dangerous than actually dropping these packets. The principle of this attack is that the dishonest vehicles store the transmitted packets for certain period of time before sending them again, which can cause plenty of problems to both safety and infotainment applications. This case is illustrated in figure 3.2 (D).

Blackhole attack:

Massive packet dropping is also among the known attacks. It consist of discarding absolutely all received packets as illustrated in figure 3.2 (E1).

Grayhole attack:

Finally, the last attack, which is also known as selective forwarding, occurs when a dishonest vehicle randomly selects some packets to forward while dropping the others to avoid being detected. This principle is illustrated in figure 3.2 (E2).

Besides the application-oriented classification, table 3.1 shows what are the security services targeted by every attack, it shows also in which category these attacks are better handled by either trust or cryptography

Table 3.1: Security threats target and solutions category.

Type of attack	**Targeted service**	**Trust-based solutions**	**Cryptography-based solutions**
Certificate Replication attack	Authenticity	-	√
Eavesdropping attack	Confidentiality, Privacy	√	√
Tracking/Tracing attacks	Privacy	-	√
Denial of Service attack	Availability	√	√
Jamming attack	Availability	√	√
Coalition and platooning attack	Availability, Non-repudiation, and Privacy	√	-
Betrayal attack	Availability, Integrity	√	-
replayed, altered, and injected messages attack	Availability, Integrity	√	√
Illusion attack	Integrity	√	-
Masquerading attack	Integrity	√	-
Impersonation attack	Authenticity, Non-repudiation	√	√
Sybil attack	Availability, Non-repudiation	√	√
GPS position faking attack	Availability, Non-repudiation	√	-
Timing attack	Availability	√	√
Blackhole attack	Availability, Integrity	√	√
Grayhole attack	Availability, Integrity	√	√

3.2.3 Distinguishing Cryptography from Trust

Trust management can be seen as an additional security level to address the shortcomings of classical cryptography solutions, being typically required against inside attackers in possession of valid certificates (see figure 3.3).

From a security perspective, both trust and cryptography can be used against a group or a single attacker within the network. However, differently from trust-based solutions, cryptography cannot handle inside attackers. Both techniques

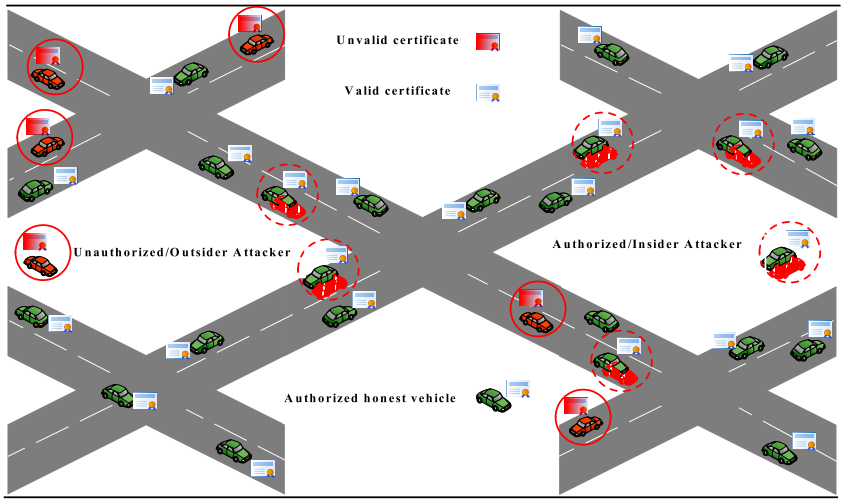


Figure 3.3: Inside and outside attackers in VANET.

can detect rational (the attacker uses a predefined strategy in order to reach a defined benefit and the attack stops once the aim reached) and irrational (a suicide bombing attack for instance).

Notice that both techniques handle only active attackers. Thus, passive attackers remain mostly undetected since they do not perform any malicious action. Notice that the aim of such passive attacks is to gather as much information as possible in order to prepare for another more dangerous attack. Advanced-persistent-threat (APT) attacks are the main example of such passive, hard to detect, and dangerous behaviour [Tan11, SE13, Bre14]. In addition, it is worth highlighting that cryptography-based solutions have a higher detection accuracy compared to trust-based solutions.

From a network perspective, trust management solutions are mostly dedicated to distributed and semi-centralized computing since they are more effective than cryptogrphy in mobile networks and independently of the exchanged traffic. On the contrary, cryptography-based solutions can achieve high performance levels especially in the case of centralized computing and delay-tolerant traffic.

Table 3.2 summarizes the main differences between cryptography-based and trust-based solutions for improving VANET security.

Taking both cryptography and trust features into account, figure 3.4 summarizes VANET security requirements together with trust management use cases. It shows that cryptography can be used for all authentication/authorization cases, confidential communication, and both non-repudiation and data integrity. Differently from it, trust is instead applicable to privacy preservation, availability, distributed key distribution and message delivery.

Table 3.2: Features of Trust-based and Cryptography-based solutions.

	Trust-based solutions	**Cryptography-based solutions**
Adversary model	Single/group	Single/group
	Insider	Outsider
	Rational and irrational	Rational and irrational
	Active	Active
Architecture	Distributed and semi-centralized	semi-centralized and centralized
Traffic	Delay sensitive and delay tolerant	Delay tolerant
Network topology	Stable and high dynamic	Stable or quasi stable
Robustness/accuracy	Medium	Robust

3.3 Trust management for VANETs

Despite their many advantages, we find that all cryptography-based approaches are prone to introduce excessive delays in order to accomplish all the checks required since the computation power of an On Board Unit (OBU) is limited. Also, the verification of messages coming from unknown vehicles involves exchanging public certificates, which leads to a high message overhead. Notice that, even though we translate the verification tasks to a nearby RSU, the huge number of messages sent in a small time period does not allow reducing this delay, which becomes critical especially in safety-related scenarios [YMF06]. Thus, most of the existing protocols focus on vehicle-to-infrastructure communication, and try to perform a quick batch verification of the exchanged messages [ZLLH08, ZLL$^+$08, CYHL11].

Since in this chapter we focus solely on the trust-based solutions, for a detailed description about cryptography-based solutions we refer the reader to some works including but not limited to [MBOH14, KKPG16].

Trust management was mainly conceived to decide whether to believe or disbelieve information asserted by other peers. This belief should only take into account statements coming from trustworthy peers. As shown in table 3.3, existing Trust-based solutions for VANETs are usually classified into entity-based [HRGD13, Yan13, DLJZ10], data-based [RPGH08, GLSB13], and hybrid trust models, depending on the revocation target, which can be dishonest entities, malicious messages, or both of them [ZCC13, KC14, SS15].

Existing works have chosen different architectures; some of them are RSU-based, others are fully distributed, and yet others deal with privacy issues. Moreover, many works consider official vehicles (e.g. police cars, ambulances, etc.) as fully trustable, thus having a positive impact on securing communication among vehicles.

It is also worth pointing out that most works deal with all kinds of messages and applications, while only a few ones are specific to event-related and alert dissemination situations.

Table 3.4 summarizes the main existing works in chronological order:

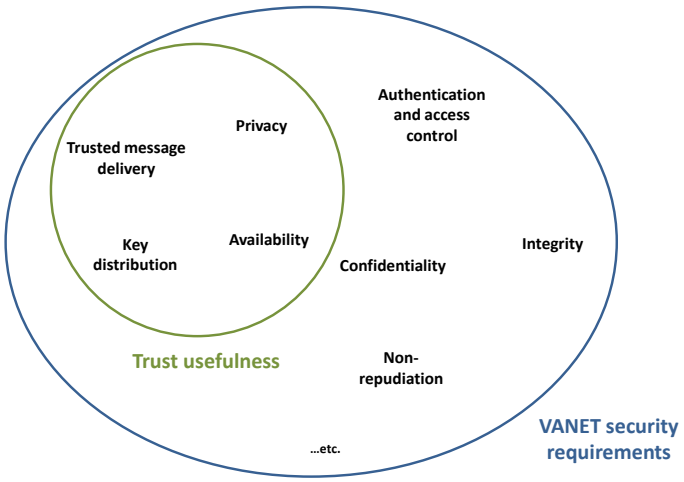


Figure 3.4: VANET security requirements and trust management use cases.

Table 3.3: Trust-based solutions common classification.

	Revocation target		
	Dishonest entities	*Malicious messages*	*Both*
Golle et al.[GGS04]		√	
Dotzer et al.[DFM05]			√
Raya et al.[RPGH08]		√	
Gerlach[Ger07]	√		
Tajeddine et al.[TKC10]	√		
Ding et al.[DLJZ10]		√	
Gazdar et al.[GRBB12]			√
Sahoo et al.[SPBN12]	√		
Zhang et al.[ZCC13]			√
Marmol et al.[MP12]		√	
Yang [Yan13]		√	
Haddadou et al.[HRGD13]	√		
Li et al.[LLLS13]			√
Chen and Wei[CW13]		√	
Gurung et al.[GLSB13]		√	
Kumar et al.[KC14]			√
Shaikh and Alzahrani[SA14]			√
Sedjelmaci and Senouci[SS15]			√
Jesudoss et al.[JRS15]	√		
Khan et al.[KAS15]	√		
Rostamzadeh et al.[RNT+15]			√
Haddadou et al. [HRGD15]			√

Table 3.4: Main trust-based solutions.

	Topology				**Purpose**			**Additional parameters**		
	Organization		*Architecture (Use of RSU)*		*Privacy*	*Safety*	*Infotainment*	*Role of vehicles*	*Trusted third party*	*Message analysis*
	Flat	Clustered	With RSU	Without RSU						
Golle et al.[GGS04]	X		X		X		X			
Dotzer et al.[DFM05]	X			X		X				X
Raya et al.[RPGH08]	X			X			X	X		
Gerlach[Ger07]	X			X			X		X	
Tajeddine et al.[TKC10]		X		X	X		X		X	
Ding et al.[DLJZ10]		X		X			X			
Gazdar et al.[GRBB12]	X			X		X				
Sahoo et al.[SPBN12]		X	X				X			
Zhang et al.[ZCC13]		X		X			X	X	X	
Marmol et al.[MP12]	X		X			X				
Yang [Yan13]	X		X			X		X	X	
Haddadou et al.[HRGD13]	X			X			X			
Li et al.[LLLS13]	X			X			X		X	
Chen and Wei[CW13]	X			X	X					
Gurung et al.[GLSB13]	X			X		X				X
Kumar et al.[KC14]	X			X			X			
Shaikh and Alzahrani[SA14]	X			X		X				
Sedjelmaci and Senouci[SS15]		X	X		X		X		X	
Jesudoss et al.[JRS15]		X	X		X	X				
Khan et al.[KAS15]		X	X		X		X	X		
Rostamzadeh et al.[RNT+15]	X			X		X	X		X	X
Haddadou et al. [HRGD15]	X			X			X			X

Existing trust models can be classified according to the communication strategy adopted as follows: (i) inter-cluster communication where a chosen vehicle makes the messages relay decision according to its cluster member opinions; (ii) flat communication where all vehicles behave autonomously; or (iii) when vehicles are within the range of an RSU, the latter plays the role of a sink handling all communications.

Overall, we find that most of the existing trust models focus on routing, path disruption, and resource exhaustion attacks including blackholes and bogus messages' injection. In the following, we survey and classify the main existing works depending on their adversary models.

1. *Trust-based solutions against replayed, altered, and injected messages*

   This kind of attacks can cause huge damage, especially in safety-related contexts. Hence, most of the existing works fall under this category.

   The *entity-oriented trust models* presented in [HRGD13, Yan13] try to revoke nodes that are sending falsified messages and fake information, respectively, using different techniques. Haddadou et al. [HRGD13] chose to associate a credit value to each neighbor vehicle. This credit will increase or decrease depending on the concerned neighbor's messages trustiness. Hence, this credit will be quickly decreased when replaying or injecting new messages. Concerning Yang's solution [Yan13], it uses the Euclidean distance to compute the similarity between nodes in terms of reported events and deletes the redundant or inadequate messages. Unfortunately, the first solution does not differentiate between direct and indirect trust, while for the second it faces a huge problem in the case of simultaneous events.

   The work in [DFM05] presents a distributed reputation system called VARS. In this proposal, peers can generate opinions about a message based on the aggregated opinions of other nodes and the evaluation of direct interactions with the sender. In order to give more importance to the opinions coming from the closest nodes to the reported event, Dotzer et al. distinguish three areas: event, decision and distribution. The main disadvantage of this scheme is the overhead added to messages by including the other trusted nodes' opinions. In addition, the case where a malicious node is the first to report about other nodes is not well investigated, as its opinion will affect all opinions that follow.

   The detection of attacks related to message quality is a process that is usually based on messages themselves, which explains why some of the existing works within this category are *Data-oriented trust models* [GGS04, GLSB13].

   Golle et al.[GGS04] have adapted a signature-based technique in which every received message is compared to a typical model of legal VANET messages. The problem with this solution is that it is not feasible to actually build such a global model; in addition, all new legal messages will be dropped as well. Unlike [GGS04], Gurung et al. [GLSB13] use three main metrics to classify received messages into either legal or malicious messages; these metrics are content similarity, content conflict, and routing path similarity.

However, in addition to its high time complexity, this solution does not take into account the high level of mobility associated to VANETs, nor the case of node sparsity.

A distinguished reputation scheme for VANETs based on a fuzzy computational model is developed in [DLJZ10]. In this work, nodes are classified regarding their closeness to the events as follows: event reporter (ER), event observer (EO) and event participant (EP). Moreover, using the messages' timestamp, they define six degrees of message honesty representing the combination of the three previous classes and the freshness of information. Nevertheless, this event-based scheme is very limited, and it cannot preserve a good message quality because, except for safety messages, the other kinds of messages are not related to a specific event.

Some *Hybrid trust models* have been also proposed in this same context. In particular, Zhang et al. [ZCC13] propose a semi-distributed trust framework for message propagation and evaluation; in their approach, the clusterheads are responsible for broadcasting and then gathering opinions about the broadcasted messages. Afterward, they decide either to drop untrustworthy messages or relay legal messages with the aggregated opinions to the next cluster in order to continue with the dissemination process. Similarly to other cluster-based techniques, the clusterhead election and the probability of malicious nodes becoming clusterheads are the main problems of this solution. Differently from the aforementioned work, Marmol et al. [MP12] prefer associating a confidence value to exchanged messages, in addition to the gathered recommendations from both RSU and nearby vehicles, to build three fuzzy sets (no trust, +/-trust, trust). The message will be dropped if it belongs to the first set, accepted but not forwarded for the second set's case, and both accepted and forwarded for the trusted messages set. The number of recommendations and their trustworthiness remain as the pending problems of this solution.

2. *Trust-based solutions against blackholes*

   Inter-vehicular communication is the enabling process supporting ITS over VANETs. Hence, forcing nodes to be collaborative is an indispensable task. Solutions falling under this category try to detect selfish nodes acting as blackholes in order to ensure a more efficient forwarding process for both safety and data messages.

   The *Entity-oriented trust model* proposed by Khan et al. [KAS15] proposes computing a distrust level for every neighbor acting as a blackhole through a watchdog technique. This distrust level will be sent to the clusterhead, and in turn delivered to a third trusted party that revokes the attacker certificate. Unfortunately, authors did not detail the different communication steps involved, nor the overhead associated to the cluster-based implementation.

   To deal with blackholes and the selective forwarding (greyholes) procedure, some *Hybrid trust models* are also available [SS15, HRGD15]. The first solution, proposed by Sedjelmaci et al., is a two-level intrusion detection system,

the first one being based on a collaborative in-cluster detection, and the second one on a global detection processed by the RSU. The main weaknesses of this solution are the excessive time associated to clusterhead election, and the assumption of having stable clusters around fixed RSUs.

The work of Haddadou et al. [HRGD15], called DTM^2, proposes forcing nodes to be cooperative by establishing a communication cost. The latter is higher for selfish nodes, decreasing alongside with in-network collaborativity. How to choose the initial cost, and how to differentiate between selfish behavior and packet loss due propagation issues, are the mains questionable points of this work.

3. *Trust-based solutions against jamming and denial of service (DoS) attacks*

   Similarly to blackholes, jamming and DoS attacks can also prevent important information to be delivered on time, thereby disturbing VANET functionality.

   Raya et al. [RPGH08] propose a *Data-oriented trust model* for Ad-hoc ephemeral networks. This model uses different trust metrics, in addition to the *a priory* fixed entities trust (e.g. $Trust(Police\ vehicles = 1;\ ordinary\ vehicles = 0.5)$), in order to detect whether the reported events are real, or if it is just an attempt to jam bandwidth. They also propose evaluating the evidences related to the reported events using Bayesian inference. The problems of this solution are the fixed entities trust and the required training phase, which cannot be ensured in practice.

4. *Trust-based solutions against fake location and timing attacks*

   The *Data-oriented trust model* proposed by Shaikh et al. [SA14] is an intrusion-aware trust model that differs from other works by being capable of detecting fake location and timing values generated either by the event's reporter or the message forwarder. In this event-related solution, authors propose the computation of a confidence value for each message coming from a unique source. In addition, for all messages describing a same event, a trust value is calculated using the previously computed confidence information. Finally, accepting or rejecting an event message depends on its trust value. Despite the high accuracy of this approach, we find that it introduces a high waiting delay, which is not acceptable when targeting VANET safety applications.

5. *Unspecified adversarial model*

   In addition to the aforementioned trust models, in some works authors do not specify an adversarial model, nor the types of attack they support. Instead, they only address trust establishment over the inter-vehicular communication link.

   The only *Entity-oriented trust model* falling under this category was proposed by Jesudoss et al. [JRS15]. In particular, authors propose a clustering technique to reduce the communication overhead and assign a reputation weight to all nodes participating in the clusterhead election and network

control tasks by sharing their reports about exchanged traffic. Unfortunately, this scheme does not respect reference trust metrics such as direct and indirect trust. Moreover, high mobility levels can cause this scheme's performance to decrease considerably.

Works in [KC14, LLLS13, CW13, RNT+15] are examples of *Hybrid trust approaches*.

Li et al. [LLLS13] propose a reputation-based trust establishment scheme for VANETs where the messages and their senders are evaluated based on the direct trust, indirect trust and node reputations. The main drawback of this scheme is its centralized trust computing procedure through the use of an additional infrastructure Called RMC (Reputation Management Center). This RMC is responsible for all revocation decisions.

Under the assumption that all application messages are encrypted, Chen et al. [CW13] propose a beacon-based trust model for enhancing users' location privacy in VANETs. The proposed system can secure the VANET while maintaining privacy by using two kinds of messages: beacons and event-based messages. The main idea is crosschecking the plausibility of these two types of messages to decide if other messages are trusted or not. Despite preserving the privacy of far-away vehicles (at more than one hop), this scheme cannot efficiently evaluate all kinds of messages, nor can it detect attacks occurring at upper layers (routing, application, etc.). In addition, whenever an obstacle appears between two neighboring vehicles, this scheme causes those two vehicles to judge each other as being a liar and malicious.

In [Ger07] authors propose constructing a trust system based on node reputation to secure communications and preserve the location privacy of vehicles. In this solution, a belief-based trust is calculated using three metrics: the situational trust, the event-based trust, and the dispositional trust. However, there is no description of how different metrics are combined, neither the exchanged traffic and adversary model.

To ensure the privacy of nodes within dynamic groups, a trust model is proposed [TKC10]. In this scheme, only the cluster-heads are in charge of exchanging information or disseminating it to group members. Despite being able to preserve privacy, this scheme has two main shortcomings: First, a security weakness is detected when the group leader is compromised or malicious nodes launch a distributed denial of service (DDoS) attack. Second, it is hard to see how groups can be formed based on heterogeneous entities because group formation is often related to the presence of vehicles in a specific geographical area. A model similar to [TKC10] using ant colony routing is proposed in [SPBN12]. The clusters are formed around the RSUs, or around the slowest and most trusted vehicles. For each message sent by a node, the clusterhead gathers the members' opinions about that node and generates a decision about the message. The ant colony algorithm is used to choose the best path between different clusters using boundary nodes. The main weaknesses of this work are the use of a static clusterhead and the slow forwarding decision due to the opinion gathering process.

In another work [GRBB12], authors propose a trust model based on the formalization of the trust metrics' variation using a Markovian chain; this way, each vehicle has to evaluate and assign a trust weight to its neighbors based on the formalized model. Evidently, the decision process about the identities' honesty and the messages' validity is purely local, a process authors denote as 'monitoring process', meaning that each monitored vehicle will have its trust value increased, decreased, or unchanged in the monitoring registry. The main limitation of this model is the limited local knowledge of vehicles, which is easy to overcome through a betrayal behavior and different DOS attacks, especially due to the re-execution of the markovian process for each received message.

T-CLAIDS [KC14] is another work providing a trust-aware intrusion detection solution for VANETs. This solution takes into account the number of vehicles, their mobility, and their motion direction to perform an action. It also maintains a probability matrix of all actions which is updated in the iterations that follow until convergence to a particular value is achieved. This way, it offers an approximate representation of a global knowledge about the environment. Unfortunately, even if this solution shows good results in the general case where malicious behaviors are stable throughout time, it looks questionable in the case of unpredictable events or attacks. Also, convergence time may be very long in sparse cases since it will be hard to gather all the information required to have a global view.

Last but not least, Rostamzadeh et al. [RNT+15] try to divide the map into different areas, and the traffic into three categories: safety, infotainment, and third party services, such as inter-transportation vehicular communication. In this solution, called "FACT", the message source should be known by piggybacking the identities of all vehicles participating in the routing process. Meanwhile, an admission module is responsible for analyzing the messages using the traffic category and the piggybacked identities' trust. If the degree of satisfaction is high, a trusted path is selected for the message. Unfortunately, this solution adds a considerable overhead and processing delay. Moreover, authors do not provide information about its security performance.

3.4 Attacks bypassing trust management

As mentioned before, trust can be defined as the evaluation of the historical interactions among peers. The fact that trust is based on these historical interaction may affect its robustness and make it susceptible to some attacks such as the On-Off and the Newcomer attacks. In these kinds of attacks, attackers behave smartly to avoid being detected. Hence, they either alternate between legal and illegal behaviours (i.e. Betrayal and tracking-based attacks), stopping all network activity until meeting new nodes that have no previous knowledge about their behaviour (i.e. On-Off and Newcomer attacks), control a certain number of nodes having lack of security measurements and launch attacks using their identities (i.e.

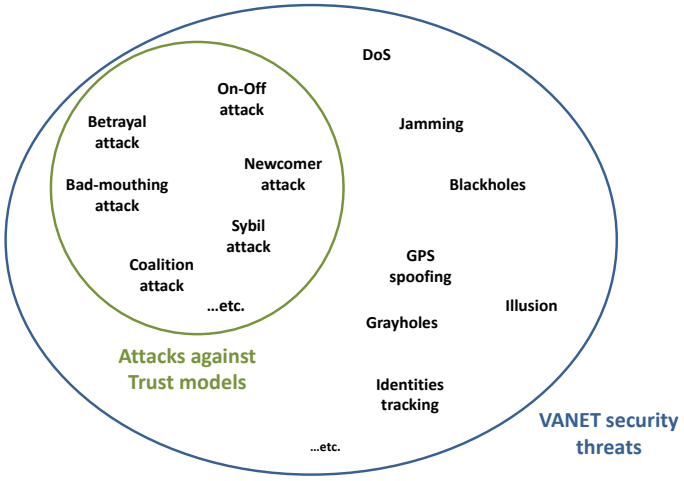


Figure 3.5: VANET security threats and attacks against trust management.

Sybil attack), or keep within a coalition or a platoon of attackers, assuring this way that only positive recommendations about each other are disseminated (i.e. Bad-mouthing, coalition, and platooning attacks).

Figure 3.5 summarizes the main VANET threats, together with those attacks that most of the existing trust models cannot overcome.

Despite the rule that a good trust strategy is the one where trust is hard to get but can be easily lost, when an inside attacker becomes aware of the game rule, both cryptography and trust are easily bypassed. Figure 3.6 shows an example of a smart attacker behaviour to avoid being detected.

Therefore, new trust models for VANETs should be able to cope with smart attackers. To this end, many techniques can be used such as the adaptive detection threshold and behaviour variation estimation. Also, the last trust evaluation can be used for the next re-keying/re-certification phases and, hence, smart attackers will be dismissed from all network operations directly after their initial attack attempt. Evaluating trust for separated time intervals can also help in detecting dishonest nodes attempting to avoid being detected.

3.5 VANET trust models' evaluation methods

The evaluation part of existing trust models for VANETs is mostly done through simulations. In particular, most of these proposals have used the NS-2 simulator [NS-a]. Moreover, some proposals have adopted other existing simulation tools such as NS-3 [NS-b], Matlab [Mat], TRMSIM-V2V [MP09], GrooveNet

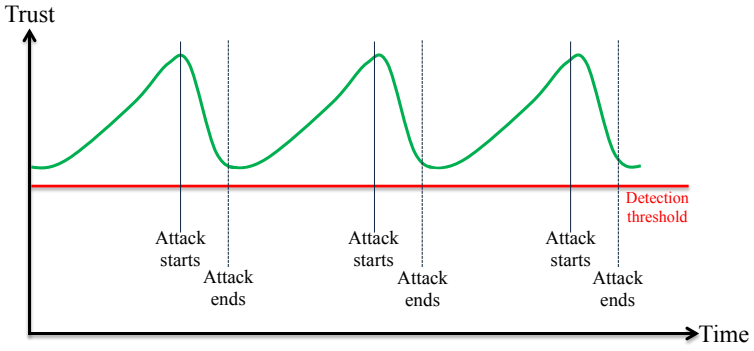


Figure 3.6: Intelligent dishonest behavior.

[MWR+06], TraNS [PRL+08], SWANS++ [SWA], and Veins [SGD11]. In addition, in some works, authors have chosen to develop their own simulator instead of using the existing simulators using either C++ or Java programming languages.

It is worth pointing out that in [SPBN12] authors did not specify which tool they used, whereas the authors of [KC14] mention that they used VanetMobisim [HFFB09] as a simulator, when the latter is in fact a mobility trace generator. Hence, further details about how authors modified this tool to consider all simulation patterns should be provided.

Besides the simulation experiments, other works only offer a theoretical analysis and discussion of their proposals. We also noticed that only one work has used Markov chains as an analytical validation method.

Figure 3.7 summarizes the existing trust models evaluation methods together with the selected simulators and environments.

A drawback found in most of the existing solutions is that they do not mention which propagation models are used for the inter-vehicular communications. Thus, it does not matter which environment is simulated (highway, freeway, or urban) if we do not use realistic propagation and mobility models that take into account all relevant factors including: signal attenuation, multi-path fading, obstacles, etc. The absence of such realistic models clearly affects any studied performance metrics.

Many works have studied and clarified the impact of the propagation models in inter-vehicular communication including [MTC+09, MFC+10]. The obtained results show that the end-to-end delay and packet delivery ratio were clearly affected when varying the attenuation scheme with obstacles, and using a real map layout compared to those when varying the attenuation scheme without obstacles and using a Manhattan layout. Both results also differ from those obtained when using the realistic attenuation scheme and varying the visibility/layout schemes.

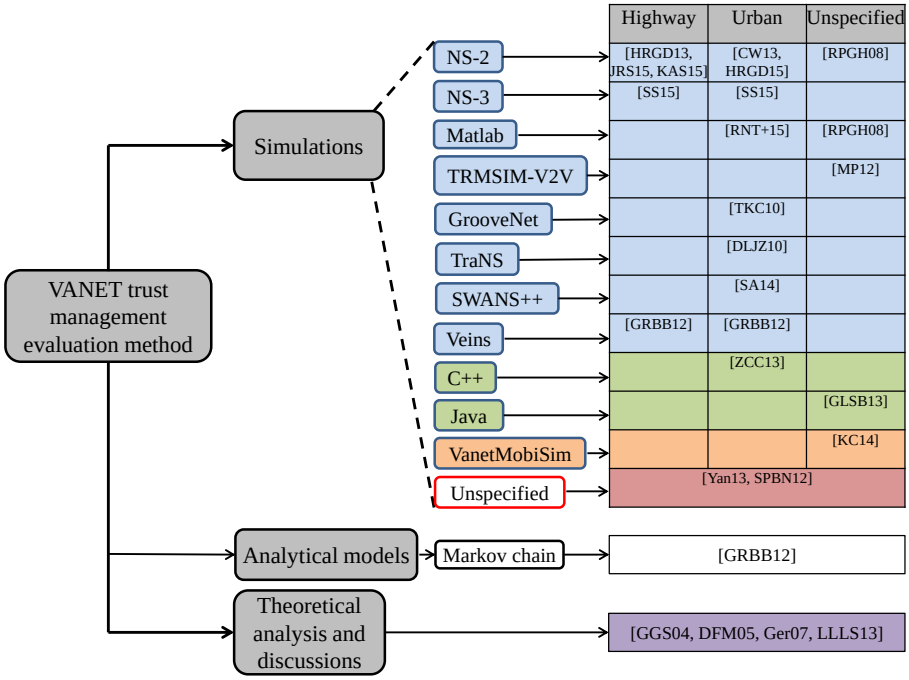


Figure 3.7: Evaluation tools of existing trust models for VANETs.

Similarly to radio propagation models, mobility models have clearly a direct impact on network performance. For instance, the work in [MFU+15] highlighted the relevance of mobility patterns when aiming at realistic vehicular mobility for VANET simulations.

We should also mention that there is no real testbed implementation of any of the existing trust models. Hence, implementing and testing the existing or the new proposals is highly recommended.

Table 3.5 summarizes the simulated solutions, together with the evaluated metrics and the used propagation and mobility models (if specified).

Table 3.5: Simulation tools and performance evaluation metrics.

Proposal	Simulator	Propagation model	Mobility model	Performance metrics
[RPGH08]	Matlab [Mat] and NS-2[NS-a]	Unspecified	Unspecified	-Decision correctness (correct reports and false reports)
[TKC10]	GrooveNet [MWR+06]	Unspecified	Sight Seeing Trip	-Trust values variation
[DLJZ10]	TraNS [PRL+08]	Unspecified	Random Waypoint [YLN03]	-Reported event correctness -Fuzzy logic enhancements
[GRBB12]	Veins [SGD11]	Unspecified	SUMO [BBEK11]	-Trust values variation -Average number of vehicle-to-vehicle interactions -Duration of vehicle-to-vehicle interactions
[SPBN12]	Unspecified	Unspecified	Unspecified	-Clusters creation time -Clusterheads selection time -Message delivery probability -Routing overhead
[ZCC13]	C++	Unspecified	Unspecified	-Number of delivered messages -Spam's propagation distance -Average number of undetected spams -Overall delivery probability -Average number of wrong decisions
[MP12]	TRMSIM-V2V [MP09]	Unspecified	Unspecified	-Percentage of selection of trusted vehicles (autonomous attackers) -Percentage of selection of trusted vehicles (attackers in collusion)
[Yan13]	Unspecified	Unspecified	Unspecified	-Trust values variation
[HRGD13]	NS-2 [NS-a]	Unspecified	Vanet Mobisim [HFFB09]	-Attackers detection ratio -Corrupted data ratio -Data delivery ratio
[CW13]	NS-2 [NS-a]	TwoRayGround	Random Trip [LBV06]	-Attackers detection ratio -Attackers detection with location privacy -Attackers detection delay
[GLSB13]	Java	Unspecified	Unspecified	-Trust values variation -Processing time
[KC14]	VanetMobisim [HFFB09]	Unspecified	VanetMobisim [HFFB09]	-Attackers detection ratio -Processing time -Number of successfully delivered packets
[SA14]	SWANS++ [SWA]	Free space	STreet RAndom Waypoint [CB05]	-Attackers detection accuracy -False positive rate

[SS15]	NS-3 [NS-b]	Unspecified	SUMO [BBEK11]	-Attackers detection ratio -False positive rate -Detection time -Communication overhead
[JRS15]	NS-2 [NS-a]	Unspecified	VanetMobisim [HFFB09]	-Trust values variation -Attackers detection probability -False negative rate -Average number of hops for data delivery -Clusters stability
[KAS15]	NS-2 [NS-a]	Unspecified	Unspecified	-Average throughput -Packet delivery ratio -End-to-end delay
[RNT+15]	Matlab [Mat]	Rician fading with shadowing [PK93]	Real traffic traces	-Packet delivery delay -Average number of packet retransmissions -Packets delivery ratio
[HRGD15]	NS-2 [NS-a]	Unspecified	VanetMobisim [HFFB09]	-Attackers detection ratio and required delay -Detection of false positives -False Message Diffusion

3.6 Open research issues

Because of the wide range of security threats seeking different network and security services, finding a single security scheme able to deal with all parameters of interest is an hard and quasi impossible task. Hence, towards this objective, we believe that all proposals should follow and enhance the major standards, projects and consortia including 3GPP/oneM2M/WAVE, 1609.2 [Com13], and ETSI ITS [ETS12] security models.

Besides, handling both location and identities privacy, while ensuring efficient and reliable safety messages' dissemination, is one of the open issues of existing trust models. In addition, dealing with smart attackers is an issue that remains mostly untackled in terms of VANET trust models since all existing models assume that their adversary has a stable and continuous malicious behaviour which facilitates the detection process.

More important than performing extensive simulations, there is a clear need to deploy real testbeds to assess the effectiveness of the different trust-based proposals in real scenarios. We also noticed that most existing solutions belong to the application layer, which means they are software-based and do not require specialized hardware or extra components. Thus, the use of smartphones seems like the easiest and less costly way to implement and test existing solutions. In fact, different researchers have already developed some prototypes supporting vehicular communications using smartphones [TPC+15, JKS+12, ZCCM11].

Among the main open issues for VANET security and trust is the human factor. Since human honesty can clearly enhance both security and safety in VANETs, this information can be extracted from online social networks through trusted third parties, as the latter are usually the only authorities able to match the vehicle identity with the driver identity, and to gather the driver's online social network profile based on the identity. To our knowledge, there is no trust-based system for VANETs that has taken the human factor into account the way we are suggesting.

Finally, advanced persistent threats in VANET contexts are also among the worthwhile research issues to improve trust management in VANETs.

3.7 Summary

Various security threats and different adversaries are faced when attempting to secure vehicular communications. In addition, other influential parameters in VANETs should be taken into account by any security system, including high mobility, open wireless medium, and the absence of trusted infrastructures in some cases, like rural environments. In this review chapter we clarified the main differences between cryptography-based and trust-based solutions for securing VANET environments. We conclude that a robust security system should include both strategies to handle all kind of threats. Such desired system should have the ability to combine or alternate between cryptography and trust, depending on the context and the probable adversary in this context.

Chapter 4

Trust Establishment Proposals for Vehicular Networks

4.1 Overview

In this chapter we detail our two main proposals for establishing trust in vehicular environments, namely TFDD and T-VNets. Both proposals are represented by modular architectures and focus on insider attackers, which are able to launch different attacks mainly addressing service availability. In addition, we also summarize our proposed opportunistic alert system dedicated to VANET safety applications.

4.2 TFDD: a Trust-based Framework for Reliable Data Delivery and DoS defense in VANETs

4.2.1 System model

In this section we detail our TFDD modular architecture, which aims at dealing with DoS and DDoS attacks, preventing the forwarding of malicious data, and revoking dishonest nodes from all network operations based on a fast and powerful evaluation of the forwarder/source, and of the nature of the transmitted data (normal, virus, spam, ...etc.). Recommendation-based solutions are generally very slow and may lead to uncertain consequences if they delay the detection of malicious nodes. Therefore, in our scheme, we try to exclude bad data/nodes from the routing operation as quickly as possible, and choose the most trusted, stable and close forwarder to the destination by introducing a new parameter that combines the Trust weight of nodes (Tr) and the Link Stability (LS) between direct forwarders. So, each node receiving a packet shall compute this parameter.

Table 4.1 details the used notations and their meanings.

To ensure an adequate and efficient message evaluation process, we have added a field $opinion_{forwarder}^{(msg)}$ to each message header which contains the last forwarder

Table 4.1: TFDD Notations

Notation	Meaning
$Tr_{i,j}$	the trust value given by 'i' to 'j'
$LS_{i,j}$	the link stability between 'i' and 'j'
$V_{i,j}$	the speed difference between 'i' and 'j'
$D_{i,j}$	the distance between 'i' and 'j'
$opinion_{forwarder}^{(msg)}$	The last forwarder opinion on the messages 'msg'
$W_{(i,j)}^{IDM}$	The honesty weight of 'i' generated by the IDM module of 'i'
$W_{(i,j,msg)}^{DB}$	The data trustiness weight computed by 'i' of the message (msg) sent by 'j'
$W_{(i,j)}^{DB}$	A weigh computed by 'i' representing the cumulative quality of data packets received from 'j'
$W_{(i,j)}^{DoS}$	DoS & DDoS detection weight
τ	Error factor
α	Peak cases avoidance factor
β	Trust penalization factor
γ	Trust increment factor
δ	Trust decrement factor

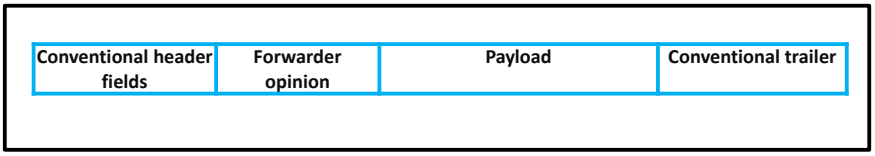


Figure 4.1: Message format

opinion concerning its forwarded message, as illustrated in Figure 4.1:

We take into consideration solely the opinion of the direct source (forwarder) of the message in order to have a fast and efficient tradeoff between these elements.

Since we only include the last forwarder identity and its opinion within the message header, we do not cause privacy problems as the forwarder identity would not be transmitted beyond one-hop neighbors. In addition, to avoid man-in-the-middle attacks, we combine the forwarder opinion with our evaluation about this forwarder's behavior.

4.2.2 Proposed modular solution

Figure 4.2 illustrates our proposed framework design, which includes the following elements: Neighboring Evaluation module, Decision Module, Communications Interface, Message Classifier, Delayed Verification module and Intrusion Detection Module (IDM).

In our scheme, every node 'i' calculates the trust value of any neighbor 'j' called Tr_ij using the following metrics: (1) the direct trust representing its evaluation about the sender (or forwarder), (2) indirect trust indicating the opinion of the last forwarder about it, (3) the weight assigned to official vehicles and; (4) the prior Delayed Verification of sender data. More details will unfold in the next sections.

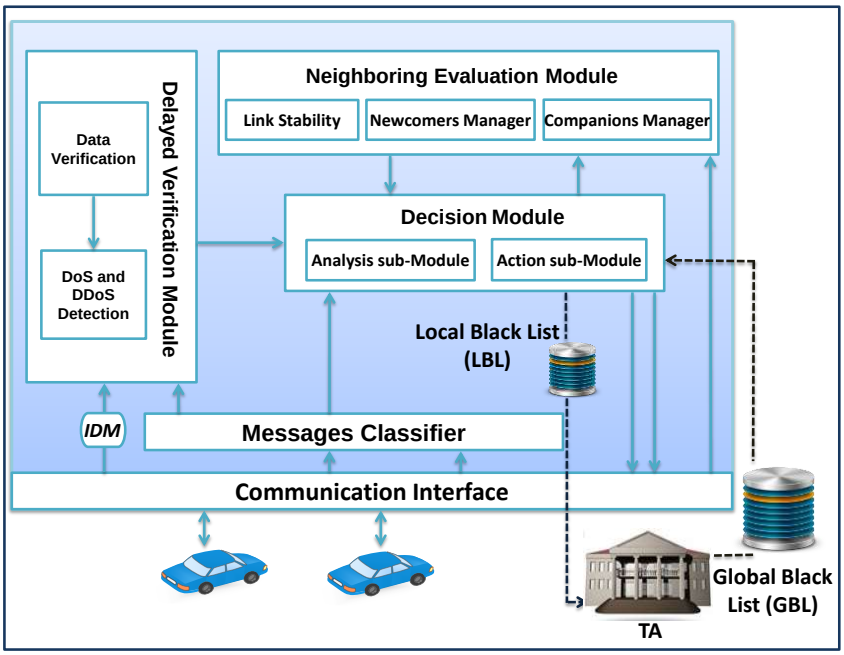


Figure 4.2: Overview of the proposed framework

4.2.2.1 Neighboring Evaluation Module

This module contains three sub-modules responsible for three tasks: (1) computing the link stability between any pair of neighbors, (2) managing newcomers within the communication range, and (3) combining trust and link stability values to generate the companions list.

Link Stability Sub-Module

We consider a link between two nodes as stable during a time t_0 (we take t_0 equal to the service channel interval defined in IEEE 1609.4 -2006- Trial Use Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operations -) if they are neighbors moving in the same direction, and with roughly the same velocity in the time interval [t, t+t_0]. The link stability between every pair of nodes must be reviewed periodically due to the nature of communications in mobile networks.

We calculate the Link Stability $LS_{i,j}$ between two nodes 'i' and 'j' as follows:

$$LS_{i,j} = \alpha \cdot LS_{i,j} + (1-\alpha) \cdot \left[\frac{1}{\frac{\Delta V_{i,j}(t+\rho)}{\Delta V_{i,j}(t)} \times \frac{D_{i,j}(t+\rho)}{D_{i,j}(t)}} \right] \tag{4.1}$$

Where α: constant used to avoid the influence of peak cases, such as unexpected braking;

V_i(t): velocity of vehicle 'i' at time t;

$\Delta\ V_{i,j}$ (t) = V_i(t) - V_j(t); 'i' and 'j' speed variation at instant t;

$D_{i,j}$(t): distance between 'i' and 'j' at time t.

Newcomers Sub-Module

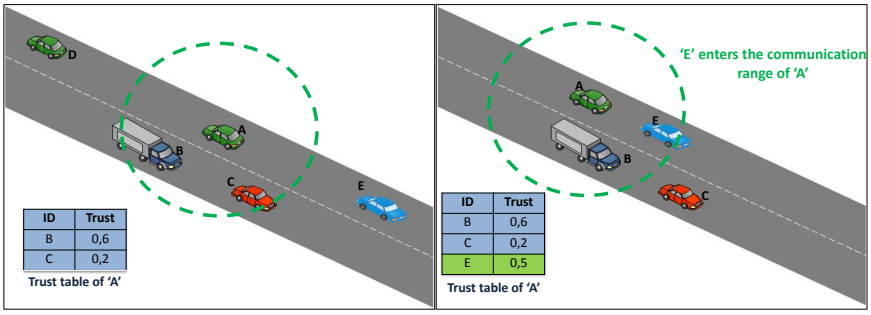
When a vehicle enters another vehicle's communication range for the first time, they assign each other an initial trust value (e.g. 0.5 for a simple vehicle, 1 for an official vehicle) (see Figure 4.3). In addition, this trust value can be increased or decreased according to the vehicles' behaviors.

To avoid resetting nodes' trust in a highly dynamic network, a vehicle must save the trust values for each node leaving its communication range in an internal list for a certain period. Therefore, if a node again enters the vehicle's vicinity, it will be associated to its last updated trust value.

Companions Manager Sub-Module

In our case, a companion is a trusted neighbor that stays within the range of a vehicle during a certain period. Hence, each node maintains a list of companions based on which the next forwarder is preferably chosen.

Algorithm 1 summarizes the three tasks of this module. Upon receiving a message, if its source or forwarder is a highly-trusted neighbor node moving similarly to another ($\geq$ TH, where TH is a trustiness and stability threshold fixed at 0.5), the latter adds its identity to the companion list. Besides, if it belongs to the old neighbors list, its last trust weight is assigned to it again, whereas new unknown nodes get an initial trust weight equal to 0.5 if it is a normal vehicle, or 1 if it is an official vehicle.



A: The trust table of vehicle 'A'

B: A's trust table update when the vehicle 'E' enters its communication range

Figure 4.3: Allocation of the initial trust value

Algorithm 1 Neighboring evaluation module's tasks

INPUTS: a node ID 'j', LS, Tr.
OUTPUTS: updated Companions list, $Tr_{i,j}$.
CNL: Current Neighbors List;
ONL: Old Neighbors List;
For each received message from a node 'j' Do
$LS_{i,j} \leftarrow$ Equation 4.1 ;
if 'j' $\in$ CNL **then**
    if ($Tr_{i,j} \geq$ TH) And ($Tr_{i,j} \geq$ TH) **then**
        Companions list $\leftarrow$ ID(j) ;
    end if
else
    CNL $\leftarrow$ ID(j) ;
    if 'j' $\in$ ONL **then**
        $Tr_{i,j} \leftarrow OldTr_{i,j}$;
    else
        if 'j' is a simple vehicle **then**
            $Tr_{i,j} \leftarrow 0.5$;
        else
            $Tr_{i,j} \leftarrow 1$;
        end if
    end if
end if

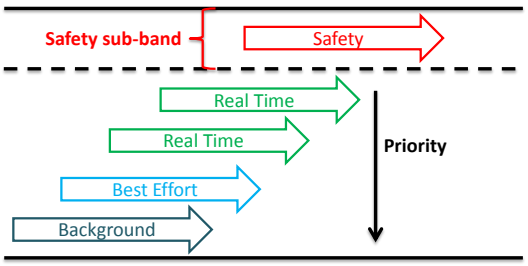


Figure 4.4: Traffic priorities defined in the WAVE standard

4.2.2.2 Messages Classifier Module

In any security or prevention system, message quality checks can be done by running a set of tests. The variety of messages and the high number of rules makes the verification procedure very slow. In this scope, dividing data traffic into classes allows to improve performance by dividing the set of rules and reducing the test time.

In this work, we use the IEEE 802.11e standard classification where data traffic is divided into four Quality of Service (QoS) categories, classified from the lowest to the highest priority as follows: background traffic (BK), best effort traffic (BE), video traffic (VI), and voice traffic (VO). Safety messages are not included in this classification since a specific band is reserved to them (see Figure 4.4). The use of this classification allows making the detection thresholds adaptive to the different situations (events) and traffic types.

4.2.2.3 Intrusion Detection Module (IDM)

Intrusion detection techniques have been traditionally classified into two categories:

- Misuse detection, which seeks for signature of known attacks in exchanged packets.
- Anomaly-based detection, where the general behavior of a node is compared to a model of typical behavior. The latter can be built in several ways, most often through artificial intelligence techniques.

In our framework, we use a new hybrid intrusion detection module that uses both misuse and anomaly detection, and allows preventing DDoS attacks by keeping statistical information about all the neighbors concerning sent (forwarded) messages, as illustrated in Figure 4.5.

Neighbor ID	Safety counter	VO counter	VI counter	BE counter	BK counter
...	...	...	...	...	...

Figure 4.5: Statistical information gathered

Algorithm 2 Intrusions' detection process

```
1: INPUTS: a node ID 'src', a message (msg) from 'src'.
2: OUTPUTS: updated W^IDM_(i,src).
3: For every message 'msg'
4: if (Attack signature detection (msg) ) then
5:     W^IDM_(i,src) ← 0 ;
6: end if
7: For every neighbor 'j' ;
8: if ∃ counter ≥ legal behavior threshold then
9:     W^IDM_(i,j) ← 0 ;
10: else
11:     if ∑ counters ≤ α * ∑ legal behavior thresholds then
12:         W^IDM_(i,j) ← W^IDM_(i,j) - δ ;
13:     end if
14: end if
```

It also allows detecting other kinds of attacks and identifying selfish nodes that drop packets or do not collaborate in message transmission similarly to the watchdog technique proposed in [TWLY10].

The IDM assigns to each node a weight representing its honesty $W^{IDM}_{(i,j)}$. Initially this weight is set to 1 for all nodes. Then, it is adjusted according each node's behavior as described in Algorithm 2.

The IDM penalizes nodes by setting their weights $W^{IDM}_{(i,j)}$ to 0 in two cases: (i) after a signature-based detection, (ii) if the amount of data sent per node surpasses a predefined threshold representing the maximum number of sent messages, for a specific type of traffic, allowed under acceptable conditions. Obviously, this threshold will depend on the type of services that the targeted node is offering. For example, we can exchange only safety messages with official vehicles, being messages associated to comfort applications (e.g. games) not expectable.

In order to avoid the selfish behavior of nodes, as well as colluding attacks (see Figure 4.6), we penalize those nodes continuously sending a high number of messages (close to the threshold) similarly to [GWZZ14] whenever they satisfy the following condition: $\sum$ counters $\leq \alpha * \sum$ thresholds; $\alpha \approx 1$. This penalty is done by reducing their $W^{IDM}_{(i,j)}$ weights by a factor δ, where $0 \leq \delta \leq 1$.

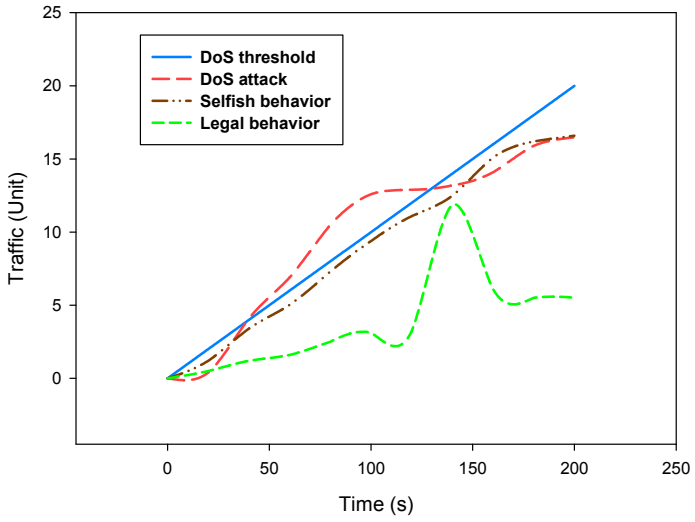


Figure 4.6: Different node behaviors in terms of traffic injected on the channel throughout time

Figure 4.6 shows an example of different behaviors in terms of traffic injected on the channel. For instance, a selfish node will always try to use the maximum bandwidth possible without exceeding the thresholds, whereas a legal one uses the bandwidth depending on its needs. As expected, an attacker tries to exceed all limits to penalize the network and its nodes.

4.2.2.4 Delayed Verification Module

Since most traffic on a VANET is delay sensitive, securing vehicular communications through data centric verification, or by including cryptographic techniques such as signatures and certificate verification, are not suitable solutions. Therefore, the challenge is to exclude malicious data/nodes in vehicular communications as quickly as possible. To this end, in addition to the trust-based evaluation when observing the historical interactions between nodes, we propose exploiting the results of data verification in a delayed manner for the following reasons: First, to avoid penalizing delay-sensitive applications; Second, to get more information about each messages' source. Third, to allow excluding nodes/data after the first exchange.

To achieve these goals, this module comprises two sub-modules: data verification and DoS&DDoS sub-modules, which are described below.

Data verification Sub-Module

Since we start with the assumption that all nodes are honest and collaborative, this sub-module is responsible for generating two weights, $W^{DB}_{(i,j,msg)}$ and $W^{DB}_{(i,j)}$, both initialized at 1. The first one relies on a data filtering application that is

used to update the node honesty in the decision module. The second represents the global data quality degree related to the same node 'j', and which is used by the DoS and DDoS sub-module to prevent attacks.

Therefore, if a node 'i' receives a message from a node 'j' that has a data-related weight $W^{DB}_{(i,j)}$=a, and the data verification sub-module assigns a weight $W^{DB}_{(i,j,msg)}$=b to this message, the new global data quality degree of each node $W^{DB}_{(i,j)}$ is updated as follows:

$$\begin{cases} W^{DB}_{(i,j,msg)} & \leftarrow & MAX(W^{DB}_{(i,j)}, W^{DB}_{(i,j,msg)}) \ if \ (a*b \geq Th_h); \\ W^{DB}_{(i,j,msg)} & \leftarrow & AVG(W^{DB}_{(i,j)}, W^{DB}_{(i,j,msg)}) \ if \ (Th_l \leq a*b \leq Th_h); \\ W^{DB}_{(i,j,msg)} & \leftarrow & MIN(W^{DB}_{(i,j)}, W^{DB}_{(i,j,msg)}) \ if \ (a*b \leq Th_l); \end{cases} \tag{4.2}$$

Where, Th_H and Th_L are two thresholds used in the same way as in multimedia and quality of service applications [JCOB02], and that define the limits separating legal from malicious messages.

If the resulting weight is higher than Th_H, the node's data quality is considered good, and the maximum of these two weights is chosen in order to avoid decreasing weights when data traffic is high. Moreover, if the computed weight is between the two thresholds, the average may be considered as a node having a suspicious behavior. However, when the result weight is less than Th_L, we take the minimum of the two weights to penalize this node.

Clearly, the decision of such filtering application will be either legal or malicious (0 or 1), but since there is always a margin of error, we modified the filtering application weight using an error factor τ that is close but less than 1, as displayed in the following equation:

$$\begin{cases} W^{DB}_{(i,j,msg)} & \leftarrow & 1-\tau; \ if \ W^{DB}_{(i,j,msg)} = 0; \\ W^{DB}_{(i,j,msg)} & \leftarrow & \tau; \ if \ W^{DB}_{(i,j,msg)} = 1; \end{cases} \tag{4.3}$$

DoS and DDoS detection Sub-Module DoS or DDoS attacks are generally launched using legal instead of malicious traffic to avoid being detected (and mitigated). This module should prevent these attacks based on the quality of messages and their frequency. Hence, the use of the data quality reports ($W^{DB}_{(i,j)}$) generated by the data verification sub-module will allow detecting data-based attacks. Moreover the IDM report about the number of received messages, from the same or different sources, can help at quickly detecting these attacks, as occurs in [WVB+06].

Consequently, the two weights $W^{DB}_{(i,j)}$ and $W^{IDM}_{(i,j)}$ will be combined to compute a new weight called $W^{DoS}_{(i,j)}$ that helps making a global decision. Therefore, for every neighbor 'j' having a global data-related behavior $W^{DB}_{(i,j)}$=a and IDM report $W^{IDM}_{(i,j)}$=b, the $W^{DoS}_{(i,j)}$ will be computed periodically in the same way as explained in the previous section:

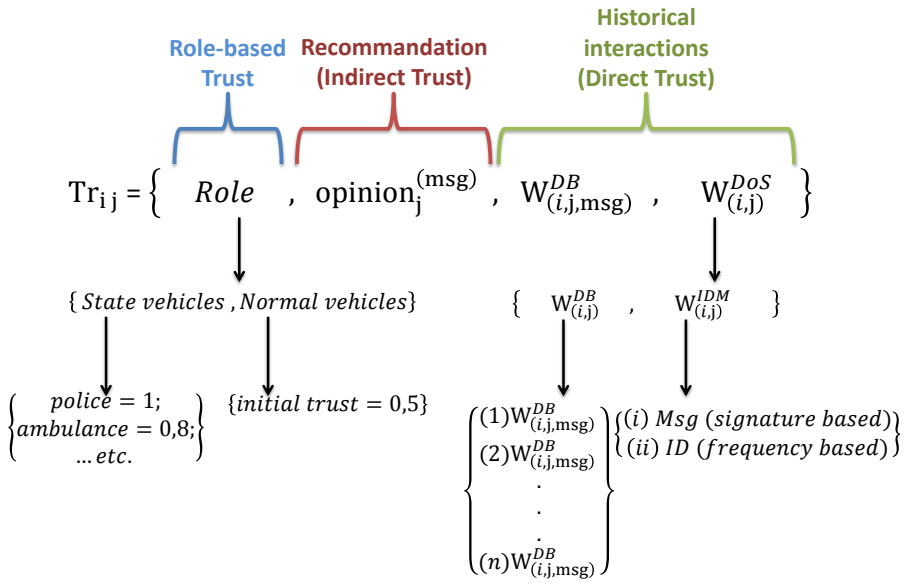


Figure 4.7: Proposed trust building scheme which combines different direct, indirect and role-based metrics

$$\begin{cases} W^{DoS}_{(i,j)} \leftarrow MAX(W^{DB}_{(i,j)}, W^{IDM}_{(i,j)}) \; if \; (a*b \geq Th_h); \\ W^{DoS}_{(i,j)} \leftarrow AVG(W^{DB}_{(i,j)}, W^{IDM}_{(i,j)}) \; if \; (Th_l \leq a*b \leq Th_h); \\ W^{DoS}_{(i,j)} \leftarrow MIN(W^{DB}_{(i,j)}, W^{IDM}_{(i,j)}) \; if \; (a*b \leq Th_l); \end{cases} \tag{4.4}$$

This weight ($W^{DoS}_{(i,j)}$) will be combined with the other weights by the analysis Sub-Module to produce as a result an efficient and reliable trust establishment scheme.

4.2.2.5 Decision Module

This module is the core of our framework. It allows combining the modules' weights (see Figure 4.7), evaluating the received messages, revoking dishonest entities locally, and managing routing decisions. The decision module comprises two sub-modules: the Analysis Sub-module and the Action Sub-module.

Analysis Sub-Module

The Analysis sub-module updates the trust value given to each neighbor by combining the weights generated by the delayed verification module ($W^{DB}_{(i,j,msg)}$, $W^{DoS}_{(i,j)}$). If both weights are higher than Th_H, then the trust assigned to a node

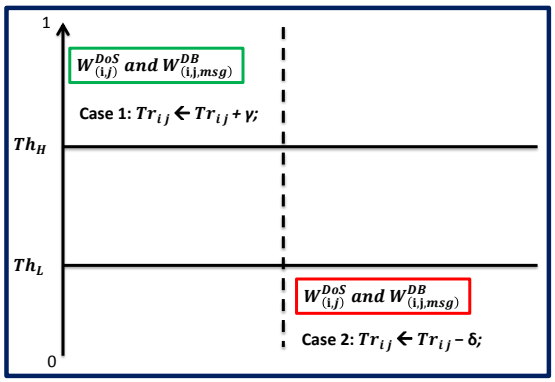


Figure 4.8: The two cases of clear behavior

can be increased by factor γ. Besides, if at least one weight is less than Th_L, the trust is decreased by a factor δ (see Figure 4.8).

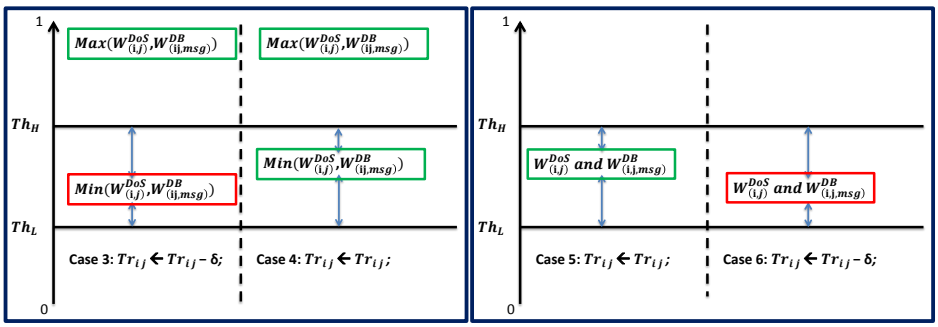
In the other cases, and as illustrated in Figure 4.9, the trust can be decreased or maintained following the difference between the two weights ($W^{DB}_{(i,j,msg)}$, $W^{DoS}_{(i,j)}$) and their closeness to Th_H and Th_L in the following manner:

If the difference between $W^{DB}_{(i,j,msg)}$ and $W^{DoS}_{(i,j)}$ exceeds the difference between the two thresholds (Th_H and Th_L), and the distance between the minimum is closer to Th_H than to Th_L, the trust will be maintained; in the case of the closeness to Th_L it will instead be decreased. On the other hand, when the difference between $W^{DB}_{(i,j,msg)}$ and $W^{DoS}_{(i,j)}$ is lower than the difference between the two thresholds (Th_H and Th_L), and the distance between the minimum is closer to Th_L than to Th_H, the trust will be decreased (or maintained in the opposite case).

At the end of the analysis procedure, we verify if the node's trust is lower than ThL and try to find the reason for this. If it is due to a DoS attack, the node's identity is blacklisted and dismissed from all network operations. If a node's identity belongs to the gray list, which contains nodes judged as probably dishonest and that can be blacklisted if another illegal behavior is detected, then, if it sends another malicious message, we add this identity to the local blacklist. The latter will be used by the trusted authority (TA) to compute the global blacklist, as proposed in [ZPU08].

It must also be remembered that, differently from other networks, DDoS attacks in VANETs are launched the same way as colluding attacks, and that every attacker sends a high number of messages because the target cannot have a high number of neighbors; also, the malicious nodes ratio generally does not exceed 30%. In addition, we assume that all DDoS attackers will send similar types of traffic because, if every attacker sends a different type of traffic, such attacks would not be considered as DDoS, being instead considered as DoS attacks.

Algorithms 3 and 4 summarize the functionality of the analysis sub-module.



A: The case of one of the weights is superior than Th_H while the other between Th_H and Th_L

B: The case of one of the weights is inferior than Th_H while the other between Th_H and Th_L

Figure 4.9: Cases of uncertain/doubtful behavior

We take $\gamma \ll \delta$ as in [Zha11] since peer trust is difficult to build up but easy to tear down. The two thresholds, Th_H and Th_L, are the same ones used in the previous sections.

Action Sub-Module

This sub-module is responsible for conditionally forwarding a message based on the previous evaluation of the message source (forwarder) and the piggybacked opinion in the message. It maintains a local blacklist, a global blacklist generated by the TA and a gray list. Therefore, upon receiving a message, the receiver node first checks its source; if it does not belong to local or global blacklists, it computes the new trust opinion that will be piggybacked on the message as shown in the following equation. The action sub-module uses the forwarder trust opinion indicated on the message '$Opinion_j^{msg}$=a', and the node's trust '$Tr_{i,j}$=b' to compute the message opinion.

$$\begin{cases} My_{Opinion} \leftarrow Tr_{i,j} \ if \ (a*b \geq Th_H); \\ My_{Opinion} \leftarrow AVG(Tr_{i,j}, Opinion_j^{msg}) \ if \ (Th_L \leq a*b \leq Th_H); \\ My_{Opinion} \leftarrow MIN(Tr_{i,j}, Opinion_j^{msg}) \ if \ (a*b \leq Th_L); \end{cases} \quad (4.5)$$

In the second step, the decision process chooses an adequate node to forward the message, preferably among the trustable neighbors. Obviously, the message will be forwarded if the generated opinion indicated on the message ($My_{Opinion}$) exceeds a trust value greater than *TrustThToSend*, which represents the lowest trust value to forward a message as used in [ZCC13]. Algorithm 5 summarizes this decision process.

In this algorithm β is a factor (≤ 1) used to penalize nodes belonging to the gray list.

The forwarding node must be the most trusted, stable and closer to the destination, which helps avoiding dishonest entities, minimizes the communication cost due to the transmission channel stability, and minimizes the number of hops

Algorithm 3 Neighbors's trust updates using the analysis sub-module

INPUTS: a node ID 'j', $W^{DB}_{(i,j,msg)}$, $W^{DoS}_{(i,j)}$.
OUTPUTS: updated $Tr_{i,j}$.
if MIN($W^{DB}_{(i,j,msg)}$,$W^{DoS}_{(i,j)}$) $\geq Th_H$ **then**
  $Tr_{i,j} \leftarrow Tr_{i,j}+\gamma$;
  if $Tr_{i,j} \geq 1$ **then**
    $Tr_{i,j} \leftarrow 1$;
  end if
  if $W^{DB}_{(i,j,msg)}$ or $W^{DoS}_{(i,j)}$) $\leq Th_L$ **then**
    $Tr_{(i,j)} \leftarrow Tr_{i,j}$-$\delta$;
    if $Tr_{i,j} \leq 0$ **then**
      $Tr_{i,j} \leftarrow 0$;
    end if
  else
    if $|(W^{DB}_{(i,j,msg)}$-$W^{DoS}_{(i,j)})| \geq Th_H$-$Th_L$ **then**
      if MIN($W^{DB}_{(i,j,msg)}$,$W^{DoS}_{(i,j)}$)-Th_L) $\geq$ (Th_H -MIN($W^{DB}_{(i,j,msg)}$,$W^{DoS}_{(i,j)}$)) **then**
        $Tr_{i,j} \leftarrow Tr_{i,j}$;
      else
        $Tr_{i,j} \leftarrow Tr_{i,j}$-$\delta$;
        if $Tr_{i,j} \leq 0$ **then**
          $Tr_{i,j} \leftarrow 0$;
        end if
      end if
    else
      if MIN($W^{DB}_{(i,j,msg)}$,$W^{DoS}_{(i,j)}$)-Th_L) $\leq$ (Th_H -MIN($W^{DB}_{(i,j,msg)}$,$W^{DoS}_{(i,j)}$)) **then**
        $Tr_{i,j} \leftarrow Tr_{i,j}$-$\delta$;
        if $Tr_{i,j} \leq 0$ **then**
          $Tr_{i,j} \leftarrow 0$;
        end if
      else
        $Tr_{i,j} \leftarrow Tr_{i,j}$;
      end if
    end if
  end if
end if

Algorithm 4 Attackers detection using the analysis sub-module

INPUTS: 'j', $Tr_{i,j}$, $W^{DoS}_{(i,j)}$.
OUTPUTS: updated LBL, Gray list.
if $Tr_{i,j} \leq Th_L$ **then**
  if $W^{DoS}_{(i,j)} \leq Th_L$ **then**
    local black list(LBL) $\leftarrow$ Add to (ID(j));
  else
    if (j $\in$ Gray list) **then**
      local black list(LBL) $\leftarrow$ Add to (ID(j));
    else
      Gray list $\leftarrow$ ID(j) ;
    end if
  end if
end if

Algorithm 5 Data delivery process

INPUTS: Message.
OUTPUTS: A decision of either relay or drop the message.
if ((Forwarder and Src) $\notin$ (GBL or LBL)) **then**
  if DstID $\neq$ MyID **then**
    Trust $\leftarrow Tr_{i,forwarder}$*$Opinion_j^{msg}$;
    if (Trust $\geq Th_H$) **then**
      $My_{Opinion} \leftarrow Tr_{i,forwarder}$
    else
      if ($Th_L \leq$ Trust $\leq Th_H$) **then**
        $My_{Opinion} \leftarrow$ AVG($Tr_{i,j}$,$Opinion_j^{msg}$);
      else
        $My_{Opinion} \leftarrow$ MIN($Tr_{i,j}$,$Opinion_j^{msg}$);
      end if
    end if
    if ((Forwarder or Src) $\in$ (Gray List)) **then**
      $My_{Opinion} \leftarrow \beta$*$My_{Opinion}$
    end if
    if ($My_{Opinion} \geq$ TrustThToSend) **then**
      if (Dst $\in$ Neighbors List) **then**
        Send (Msg, MyID, $My_{Opinion}$) To Dst;
      else
        Send (Msg, MyID, $My_{Opinion}$) To BestNextHop();
      end if
    else
      Drop (Msg);
    end if
  end if
  Delayed verification (Msg);
else
  Drop (Msg);
end if

Algorithm 6 Best next hop selection

```
1: INPUTS: Destination ID.
2: OUTPUTS: BestNexthop ID.
3: Min ← ∞;
4: For every Companion 'j' Do
5: Distance ← distance(j, destination);
6: if (Min ≤ Distance) then
7:     Min ← Distance;
8:     Next ← j;
9: end if
10: BestNextHop ← Next;
```

needed to reach the destination. Therefore, the Best Next hop should be chosen among the companion vehicles that are monitored for a long-enough period and show good behavior (see algorithm 1).

Algorithm 6 is the best next hop selection function.

4.2.3 Performances evaluation

4.2.3.1 Simulation parameters

To evaluate our proposal we relied on the NS-2 simulator modified to support the IEEE 802.11p standard, and using the RAV propagation model [MFC+10]. We chose to evaluate the trust protocol in a 10 km long highway with 2 lanes in each direction.

Vehicles are moving with speeds varying between 20 and 40 m/s. Each vehicle allows an initial trust value equal to 0.5 for all vehicles entering its communication range for the first time. However, official vehicles are considered as fully trusted nodes ($Tr_{i,j}$=1). The total number of nodes in our simulation varies from 50 to 300, and among them between 10% to 30% are dishonest. The malicious messages sending rate is set to 1 message every 3 seconds, but in the case of DoS and DDoS attacks, it can exceed 20 messages per second.

Table 4.2 summarizes the main simulation's parameters.

4.2.3.2 Results discussion

To evaluate our framework's performance, and to show the effect of each module, we chose to compare the following versions of our framework:

- *TrustGlobal* represents the framework's global model.
- $TrustDVM-$ represents the framework's model without the delayed verification module.
- $TrustRL-$ represents the framework's model without the use of role-based vehicles.

Table 4.2: TFDD simulation parameters

Parameters	Value	
Road length (km)	10	
Transmission range(m)	300	
Vehicles speed (m/s)	[20,40]	
Simulation time (s)	200	
Percentage of dishonest nodes	{10,20,30}	
Nodes Number (vehicle)	[50,300]	
State cars percentage (%)	5	
throughput (Mb/s)	18	
Malicious messages sending frequency (message/s)	1/3	
initial $Tr_{i,j}$	0.5	
Th_H	0.6	
Th_L	0.4	
TrustToSend threshold	Safety	0.3
	VO/VI	0.4
	BE	0.5
	BK	0.6
α	0.9	
β	0.95	
γ	0.01	
δ	0.10	

- $TrustIDM-$ represents the framework's model without the intrusion detection module.

To compared these alternative solutions, the following metrics are used:

1. **Dishonest nodes detection ratio**: represents the ability of our framework to exclude bad nodes from network operations. It can be defined as the ratio of number of threats detected to the total number of messages exchanged in the network.

2. **Detection speed**: represents by the average number of hops needed before deleting bad messages. In other words, it represents the lifetime of malicious messages.

3. **False positive and the false negative nodes detection ratios**: represent the error margin of our framework.

4. **DDoS Time convergence**: the necessary time for our system to revoke dishonest nodes and stop a colluding attack.

5. **Bandwidth usage ratio**: in DoS and DDoS attacks, the bandwidth usage ratio is one of the most important evaluation metrics than can give a clear idea about the abuse of network's resources.

In addition to the different variants of our solution, we provide a comparison against two other representative solutions [KC14, SS15] in terms of detection ratio.

Dishonest nodes detection

To show the impact of the delayed verification module and the presence of trustable (official) vehicles, we chose to compare the TrustDVM- and TrustRL-

solutions against our global system. In the following simulations, we chose to vary the dishonest nodes' ratio from 10 to 30%, while node density varies from 50 to 300.

Figure 4.10 shows that, for both global and TrustDVM- versions, the detection increases since both alternatives use a collaborative revocation scheme based on the exchange of opinions between direct communicating nodes. Therefore, in a dense network, the detection of dishonest nodes can be faster (see Figure 4.12). However, the global scheme achieves a higher performance compared to those obtained by TrustDVM- thanks to the use of the data centric verification sub-module that increases the detection ratio, in the worst case, by at least 26%.

Nevertheless, Figure 4.11 depicts that the presence of trustable vehicles allows increasing the detection ratio in those sparse cases where any reputation scheme fails. However, in dense networks, their effect diminishes in the favor of the delayed verification module and the collaborative mechanism.

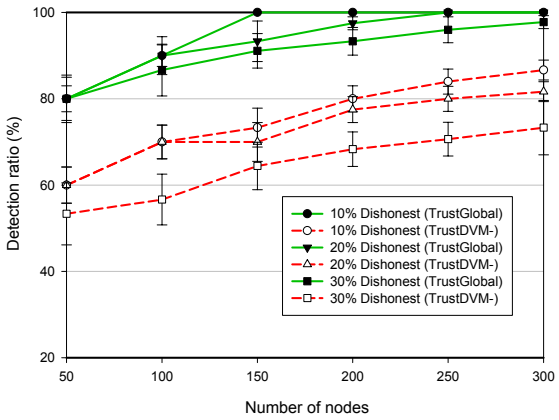


Figure 4.10: Impact of the DVM on the detection ratio of dishonest nodes

In addition, since we did not have the source code of other solutions at our disposal, we implemented T-CLAIDS [KC14] and AECFV [SS15] following the details provided by their authors in their respective papers. Figure 4.12 shows the detection ratios obtained in the presence of 30% of dishonest nodes. We can see that TFDD, despite being less effective for a low number of nodes, is able to greatly improve detection effectiveness when the number of nodes increases beyond 120, showing a consistent growth trend thanks to the collaborative detection process of our proposal.

Detection speed

To show the delayed verification module's effect on the detection speed, we compare our framework's performance against the TrustDVM- version. To this end, we assume that the dishonest nodes density is equal to 20%, and that each dishonest node generates a malicious message every three seconds.

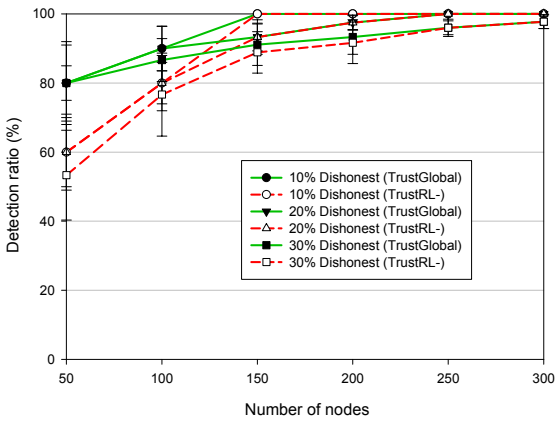


Figure 4.11: Impact of the RL (official vehicles) on the detection ratio of dishonest nodes

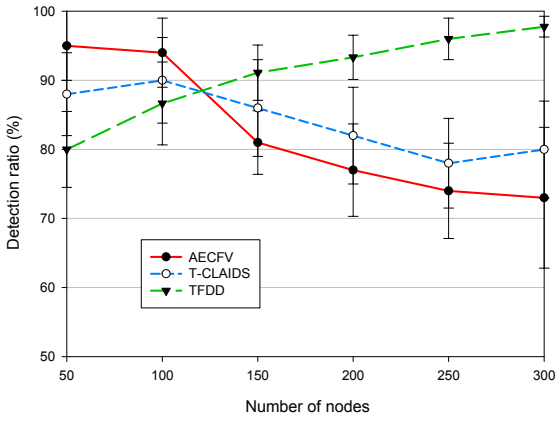


Figure 4.12: Impact of dishonest vehicles on the detection ratio

Figure 4.13 illustrates that, for both versions, a node forwards the first message of any new transmission initiated by either honest or dishonest nodes. However, a node can revoke a dishonest node after receiving the third malicious message. The Figure also illustrates that the system can converge faster and after the second exchange only when the data verification is used. This also explains the fact that a high network density can play a primordial role on any reputation system as it can enhance the overall performance (see Figures 4.14 to 4.17).

False Positives and False Negatives ratios

As in all security solutions, the false positives and false negatives ratios in the dishonest nodes detection process are essential for the evaluation phase.

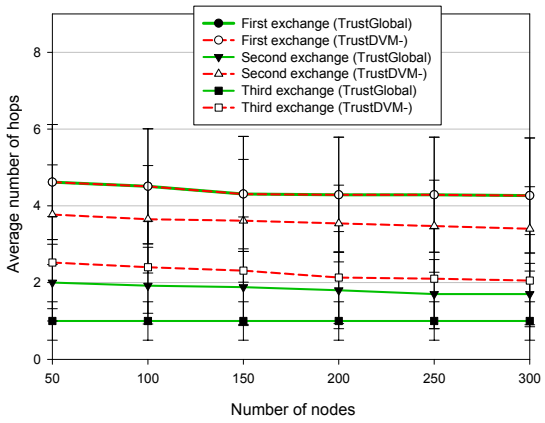


Figure 4.13: Malicious messages' lifetime (in number of hops)

The false positives ratio is evaluated by comparing the performances of the two versions (TrustDVM-, TrustRL-) against the global scheme for different densities, and for dishonest node ratios varying from 10 to 30%. Figure 4.14 illustrates that, for higher densities, the false positives ratio is low, and there are no considerable differences when the delayed verification module is deactivated due to the aforementioned cause (collaborative detection). In addition, Figure 4.15 depicts that the false positives ratio is higher in sparse environments, when new nodes launch attacks in the absence of official vehicles and fully trusted entities.

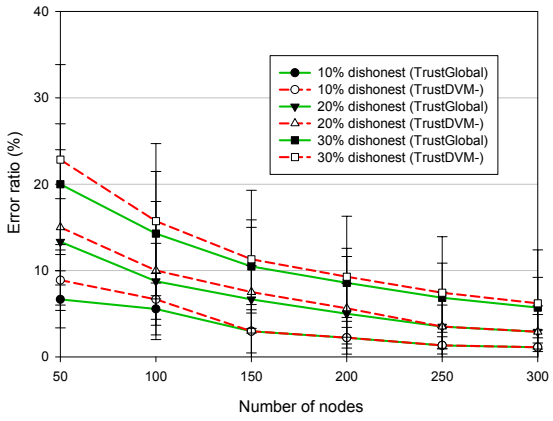


Figure 4.14: Impact of the DVM on the false positives concerning dishonest nodes detection

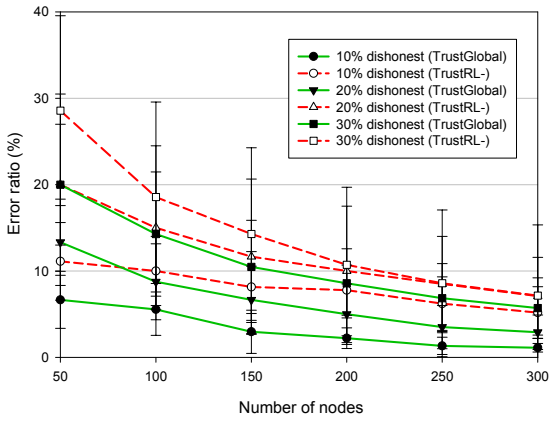


Figure 4.15: Impact of the RL (official vehicles) on the false positives concerning dishonest nodes detection

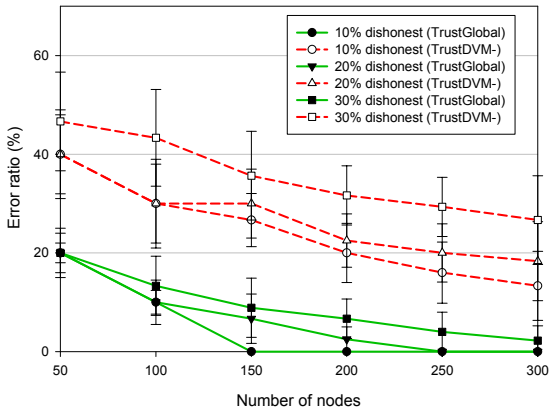


Figure 4.16: Impact of the DVM on the false negatives concerning dishonest nodes detection

For the false negatives ratio evaluation, and using the same scenarios, Figures 4.16 and 4.17 show that all the models' versions behave similarly to the false positives' case. However, the false negatives ratio is much lower, not exceeding 20% when using the data verification module that prevents honest nodes from relaying malicious data. Moreover, the false negatives for the TrustDVM- version are more considerable and can exceed 40% in the presence of a high ratio of dishonest nodes (30%), which means that the global model behaves better than the reputation-based version (TrustDVM-).

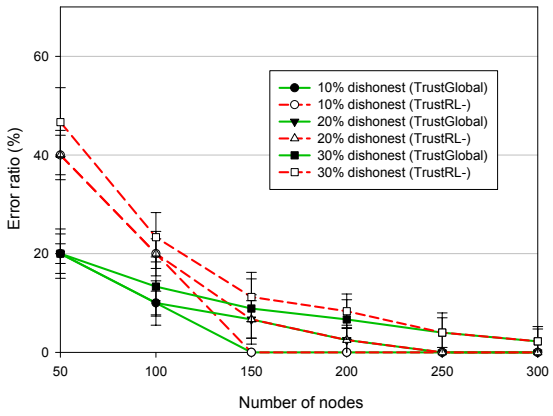


Figure 4.17: Impact of the RL (official vehicles) on the false negatives concerning dishonest nodes

In addition, Figure 4.17 shows that, except for the sparse case, the absence of role-based vehicles has no influence on false negatives because detection is performed mainly using the local knowledge and the delayed verification.

Thus, by analyzing the results of Figures 4.14 to 4.17, we can conclude that the dishonest nodes detection and the malicious messages' filtering are based on the delayed verification module, whereas the importance of dishonest vehicles becomes more significant in the sparse case, where the collaborative detection lacks efficiency.

DoS and DDoS detection evaluation

- **Time convergence of DDoS attacks detection**: To evaluate our framework's performance against DDoS attacks, we chose to study a worst-case scenario where a set of trusted nodes launches a colluding attack against a specific target. To this end, we set the number of nodes in the network to 200, with a dishonest nodes' ratio varying between 10 and 30%. We also consider that dishonest nodes are initially "fully trusted" (Tr =1). As mentioned before, we evaluate the reaction of the framework against DDoS attacks in terms of the time needed to decrease the attackers' trust and exclude them.

  Figure 4.18 shows the attackers' average trust allowed by honest nodes, after launching the attack. We notice from the curves that our system converges faster in the case of a higher ratio of attackers; this can be justified by the fact that these attackers have sent a high number of messages in a short period, and that the frequency-based detection of the IDM allows detecting them quickly. However, a lower ratio of attackers may require more time depending on the attackers' distribution in the network.

  We also note that the average trust of attackers does not reach a value of zero in the best case due to the nature of vehicular networks, where the trust

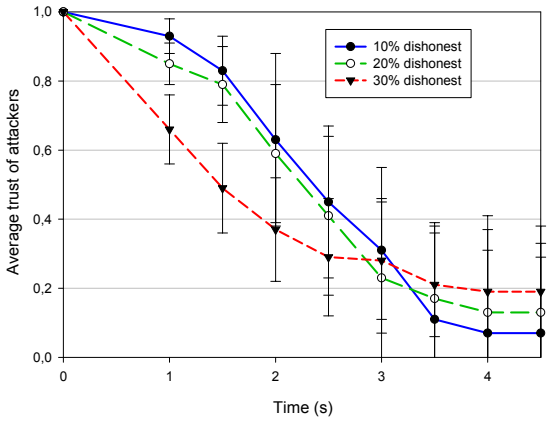


Figure 4.18: Evolution of the average trust of attackers

affecting nodes is varying from one node to another. Therefore, any trusted node may launch a DDoS attack, as a bot, at any time when controlled by a master, meaning that a node can consider these nodes as fully-trusted when leaving its range since their misbehavior only starts later-on.

- **Bandwidth usage under DDoS attacks**:

  In the MAC sub-layer, the maximum frame size is generally set to 1500 bytes using the same frame size and a bandwidth capacity of up to 18 Mb/s [Pap10], we compare the performances of the global model against the TrustIDM- version (Global model with deactivation of IDM module), in terms of bandwidth usage ratio during a colluding attack.

  Figure 4.19 illustrates that, when the IDM module is activated, our scheme can detect and stop the attack by blocking traffic very quickly, which proves the efficiency of the frequency-based detection. It is worth noting that many thresholds are defined to prevent excluding nodes sending high flows of legal data (e.g. streaming multimedia).

  In the other case, when the IDM module is deactivated, the bandwidth usage ratio is maintained at a high value ($\simeq 100\%$), proving that the misuse-based detection is not enough to prevent DDoS attacks. Figure 4.19 also shows that, when different paths are used to forward packets, the convergence of the system is affected, which explains the second peak in the curves.

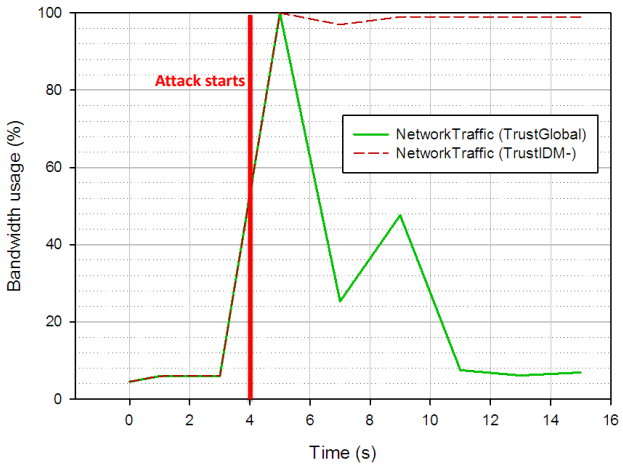


Figure 4.19: Bandwidth usage ratio in the case of a DDoS attack

4.3 T-VNets: a novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS

4.3.1 T-VNets architecture

In this section we detail our proposal called 'T-VNets', a solution that provides trust establishment over vehicular networks using ETSI ITS messaging services. Specifically, based on the information carried by the periodical *Cooperative Awareness Messages* (CAM) and the event-triggered *Decentralized Environmental Notification Messages* (DENM), T-VNets can provide an efficient and continuous evaluation of traffic, as well as the distribution of dishonest nodes within the network.

Figure 4.20 shows the trust establishment architecture defined by T-VNets. Based on the different pieces of information collected, global trust relations are built. We distinguish between two main kinds of trust: inter-vehicles trust, and RSUs-to-vehicles trust.

Nodes within the network can compute a trust value about the honesty level associated to the different interactions. Moreover, RSUs can be considered as a trusted third authority from which nodes can receive both instant and historical behavior evaluations. The latter are called in-segment and historical RSU evaluations, and together are used to build trust between RSUs and vehicles. Our solution takes advantage of the existing message format introduced by the ETSI standard to estimate the events' credibility, as well as the level of traffic on the roads and the distribution of dishonest nodes. Finally, the aforementioned fea-

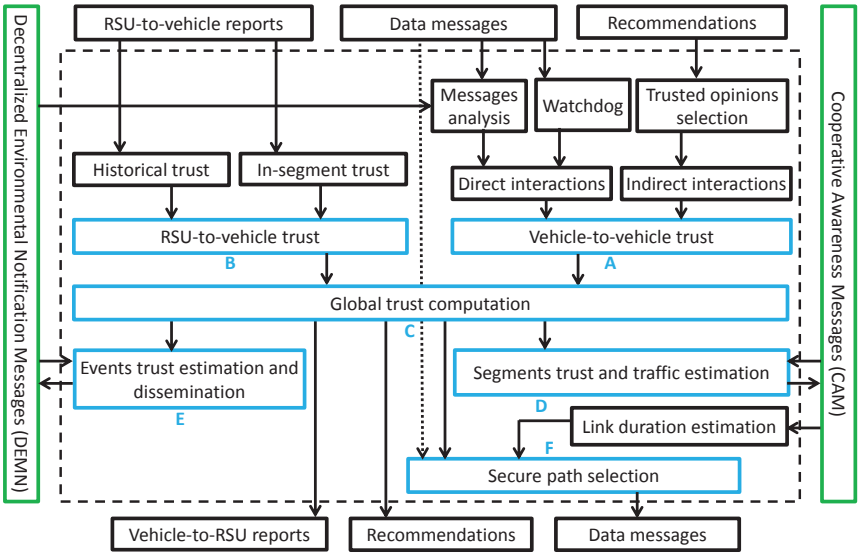


Figure 4.20: Proposed trust establishment architecture.

tures allow our framework to choose the most reliable, secure and shortest path to deliver legal data messages.

T-VNets trust establishment process is based on different modules, as shown in figure 4.20. It starts by evaluating the direct interactions between vehicles. This phase involves two modules: (1) the message analysis module, which accounts for both the received messages' quality and the reported events' effectiveness, and (2) the watchdog module, which generates reports about the direct neighbours collaboration in the different network operations. Simultaneously, whenever a vehicle 'i' observes a behaviour change regarding another vehicle 'j', it broadcasts either a positive or a negative recommendation about vehicle 'j' taking as reference a previously defined honesty threshold, which means that recommendations are not requested, but instead are automatically broadcasted whenever a vehicle notices a positive or a negative behaviour change. The gathered recommendations about a vehicle 'j' will later be combined in order to compute an indirect trust evaluation for vehicle 'j'.

In parallel with the previous vehicle-to-vehicle trust evaluation, whenever a vehicle 'i' encounters an RSU it delivers a report about its neighbours' behaviour, thus allowing the RSU to have a quasi-global view about all vehicles; this way, the RSU will generate evaluations about both recent and historical behaviours of vehicles called RSU-to-vehicle trust evaluation.

Afterward, both vehicle-to-vehicle and RSU-to-vehicle trusts are combined to compute a global trust evaluation for every neighbor 'j'. Such value will be carried by CAM messages, and used later on to enhance both data and event message

delivery while respecting DENM message specifications.

In sections that follow, we start by detailing how trust among vehicles can be updated depending on both local knowledge and vehicle-to-vehicle recommendations. The module responsible for this task is the one associated with label 'A' in figure 4.20. The second part will be dedicated to explaining how the presence of an RSU within communication range can enhance the trust computation and prevent both coalition and platooning attacks, which is the task of module 'B'. Third, we detail how global trust evaluation is computed using the two previous processes (module 'C'). In the fourth and fifth sections, which refer to modules 'D' and 'E', we explain how T-VNets takes advantage of ETSI ITS standardized CAM and DENM messages to enhance the inter-vehicle trust establishment. Finally, module 'F' is the one responsible for the trusted path selection and data delivery.

4.3.1.1 Trust metrics

T-VNets employs different trust metrics like direct, indirect, event-related and RSU-based trust. Moreover, to take advantage of this variety of trust metrics, we propose a message forwarding scheme that is effective both in the presence and in the absence of RSUs, thereby providing a more flexible solution that is adaptive to different types of environments. In the following, the 8 used metrics are listed with the same order of use.

- *Qmsg(i, j)*: quality of messages; it is the data centric evaluation of a node i about messages sent by another node j during a period of time.
- *ETR(E, j)*: event's trust; it can be defined as the degree of belief associated to an event 'E' as reported by a node j.
- *WDR(i, j)*: watchdog continuous evaluation, where every node participates in surveying the network by analyzing the sending frequency of neighboring messages .
- *DTR(i, j)*: the direct trust evaluation upon an interaction between a pair of nodes (i, j). This metric is computed based on every node's local knowledge without external feedback.
- *ITR(i, j)*: unlike the direct trust evaluation, a node 'i' computes the indirect trust for another node 'j' based on the opinions of network nodes about this node 'j', instead of i's local knowledge.
- *SRSU(j)*: in-segment RSU evaluation is the evaluation of a roadside unit about the behavior of a vehicle j within its current segment.
- *HRSU(j)*: historical RSU evaluation, represents a global view about a the trust of a vehicle 'j' generated by the RSU using j's different in-segments evaluations.
- *GTR(i, j)*: the global trust evaluation given by a node i to another j based on its overall behavior. This metric is the combination of all used metrics.

4.3.1.2 Adversary model

In general, reputation and trust-based systems are susceptible to different types of attacks [RH05, WBH+08]. However, in this solution, we focus on the active attacks listed below:

- False alert: this occurs when a selfish or dishonest vehicle triggers an alert about an nonexistent event.
- Message dropping attack: when a node does not collaborate in the message transmission process and behaves as a blackhole.
- Denial of service attack (DoS): we consider a resource exhaustion attack by sending messages at a high frequency.
- Coalition and platooning attacks: where a set of dishonest nodes (or a set of nodes controlled by a dishonest node) are moving together in order to avoid being detected, and to gain trust by providing similar reports about nonexistent events.

This means that our adversary can be: (i) A sender of malicious messages or regular messages injected at a high rate; (ii) A relay node that can act as a blackhole or camouflages its illegal behavior by relaying packets through an untrusted path; or (iii) A coalition of senders and relays having illegal purposes.

4.3.2 Proposal details

For the sake of clarity, our proposal will be divided into five main parts, and it employs the notations listed in table 4.3. In addition, we will be using Figure 4.21 as reference since it summarizes our adversary model and the different elements of our proposal.

In subsections 4.3.2.1 and 4.3.2.2 we describe how direct and indirect inter-vehicles trust (DTR, ITR) can be computed, as well as the calculation for in-segment and historical RSU-to-vehicles trust (SRSU, HRSU) and then, how these metrics are combined to compute the global trust evaluation (GTR).

4.3.2.1 Vehicle-to-vehicle trust

Trust can be defined as a relation amoung entities based on the observation of historical interactions or recommendations [Ger07]. Hence, the two main trust metrics are the direct interaction between every pair on nodes (i, j), and the recommendations coming to i about j. In the subsections below we describe how our solution maintains and updates the direct trust $DTR(i, j)$ and the indirect trust $ITR(i, j)$.

Figure 4.22 illustrates the used modules in this phase.

Direct trust (DTR)

In our case, DTR is the combination of the exchanged messages' quality (Qmsg) and a continuous report about the neighbors' degree of cooperation within the network using a watchdog technique (WDR), where every node remains in promiscuous mode and evaluates neighbor cooperation regarding network operations.

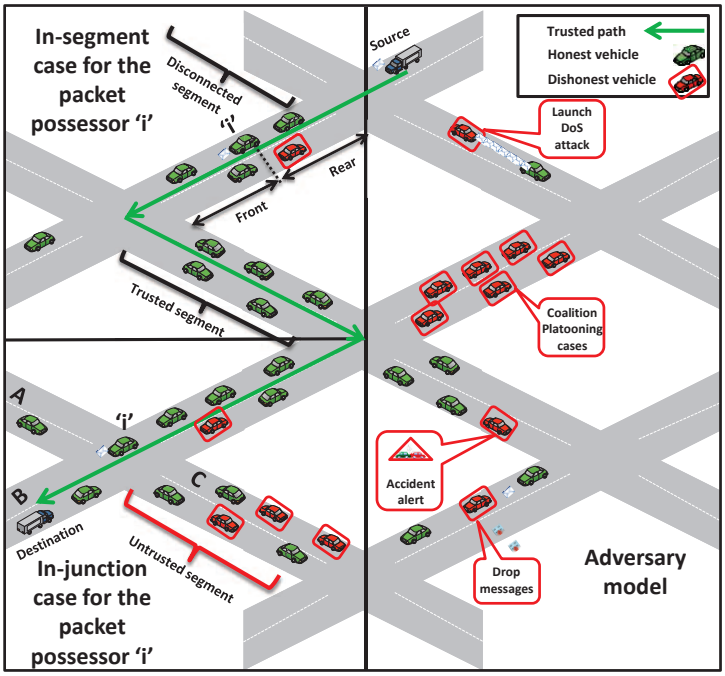


Figure 4.21: Adversary model, best path selection and routing different cases.

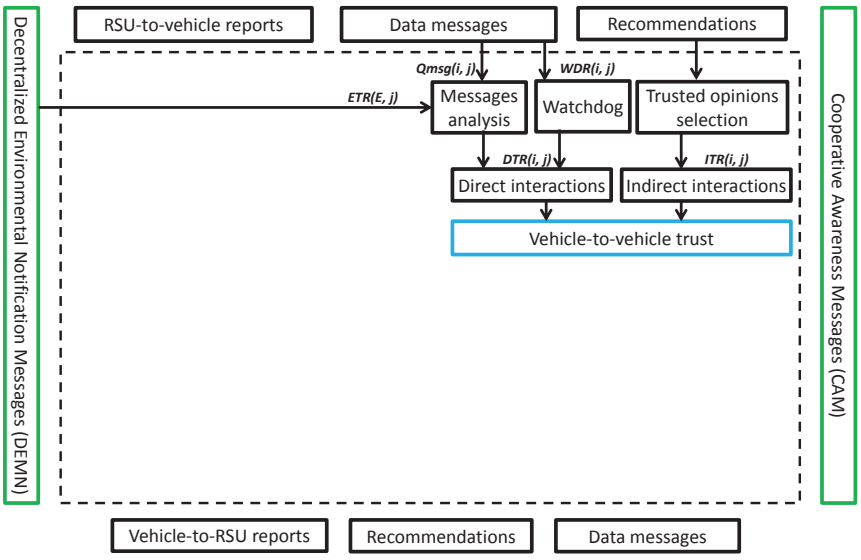


Figure 4.22: Vehicle-to-vehicle trust modules.

Table 4.3: T-VNets Notations.

Notation	Meaning
$GTR(i,j)$	Global TRust Evaluation given by i to j
$DTR(i,j)$	Direct interactions' TRust given by i to j
$ITR(i,j)$	Indirect (recommendation-based) TRust given by i to j
$HRSU(j)$	RSU's Historical trust evaluation of j
$SRSU(j)$	RSU's in-Segment trust evaluation of j
$ETR(E,j)$	TRust of the Event E reported by j
$Qmsg(i,j)$	Quality of the messages sent by j to i
$WDR(i,j)$	i's WatchDog Report about j's cooperation behavior
α	Honesty factor
β	Dishonesty factor
δ	Trust increment factor
μ	Trust decrement factor
RL	Role playing factor
ρ	Message credibility factor

Similarly to all other trust metrics used, the intial 'DTR' value assigned by a node i to another node j is equal to 0.5, and it can vary from 0 to 1 depending on j's behavior according to equation 4.6.

$$DTR(i,j) = AVG\big[DTR(i,j), [(\beta \cdot Qmsg(i,j)) + (\alpha \cdot WDR(i,j))]\big] \tag{4.6}$$

α and β are two factors where $(\alpha + \beta = 1)$ and $(\beta > \alpha)$. They are used to give more importance to directly exchanged messages in a period of time compared to network collaborativity since we are evaluating the direct trust.

Moreover, every node evaluates its neighborhood and stores, for every neighbor, some information such as the Packet Drop Ratio (PDR) and the Packet Sending Ratio (PSR). In order to decide whether an ongoing attack is taking place, we define both a high (TH_h) and low (TH_l) traffic threshold. Then, we compare the PDR and the PSR against these thresholds, updating the watchdog report $WDR(i,j)$ according to algorithm 7:

Algorithm 7 Vehicles cooperation evaluation

INPUTS: PDR, PSR of a node j during a period of time.
OUTPUTS: Watchdog report updated.
if ($PDR(j) \geq TH_h$) **then** (DoS attack detected)
    $WDR(i, j) \leftarrow 0$;
else
    if ($PDR(j)/PSR(j) \leq TH_l$) **then** (blackhole attack detected)
        $WDR(i, j) \leftarrow WDR(i, j)\text{-}\mu$;
    end if
end if
End

In this algorithm notice that μ is the trust decrement factor.

For $Qmsg(i, j)$, since it is a direct interaction, all messages can be decrypted and analysed. Hence, a data trustiness value can be obtained. The global messages' trustiness in a period of time will be updated by i upon receiving a message from j using equation 4.7:

$$Qmsg(i,j) = AVG\Big[Qmsg(i,j), \frac{RL + \alpha \cdot \sum j's\_legal\_messages}{\beta \cdot \sum j's\_malicious\_messages + \alpha \cdot \sum j's\_legal\_messages}\Big] \tag{4.7}$$

'RL' is an aditional factor ($0 \leq RL \leq 0.5$) assigned to vehicles playing a specific role (police, ambulance, etc.); otherwise, $RL = 0$.

Dishonest behaviors (malicious messages) will cause the trust level to be multiplied by a factor β higher than the legal behavior factor α (legal messages), because one of the main features of trustfulness is being hard to gain but easy to lose ($\beta > \alpha$).

Indirect trust (ITR)

Indirect trust among vehicles is computed by gathering the vehicles' recommendations about each other. Usually, voting-based techniques have a bad impact on bandwidth usage. To avoid this unwelcome situation, all one-hop neighbor recommendations will take into account only in the initial step; once the trust metrics are updated (after a small period of time), only trusted neighbor recommendations will be taken into consideration for indirect trust computation.

The indirect trust (ITR) given by a node i to another node j will be continuously updated following equation 4.8:

$$ITR(i,j) = \frac{\alpha \cdot \sum P\_recommendations\_about\_j}{\beta \cdot \sum N\_recommendations\_about\_j + \alpha \cdot \sum P\_recommendations\_about\_j} \tag{4.8}$$

Similarly to the previous cases, dishonest behaviors (negative recommendation) will cause the trust value computed to be multiplied by a factor β that is higher than the legal behavior factor α (positive recommendation), where ($\beta > \alpha$).

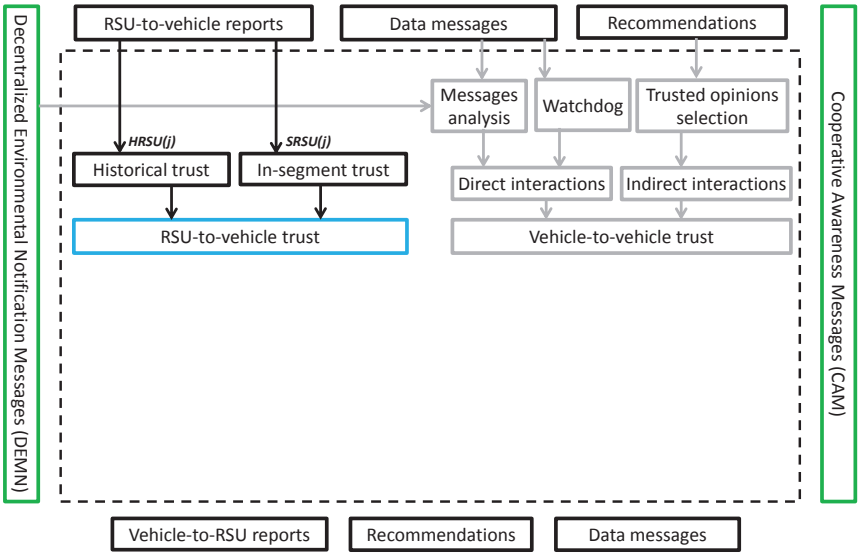


Figure 4.23: RSU-to-vehicle trust modules.

4.3.2.2 RSU-to-vehicle trust

RSU deployment is considered a complex task under both freeway and urban scenarios since RSU coverage is often affected by the presence of obstacles. However, when communication is feasible, the RSU's quasi global view about the network can significantly enhance the trust establishment among vehicles.

Based on the periodic vehicle reports, an RSU can match the vehicles pseudo identity with their real identity since it can contact the certification authority. Hence, the RSUs can generate and forward some reports about the vehicles' historical behavior using their current pseudo-identities. In our case, we distinguish between two types of RSU reports: (i) RSU trust evaluation for the current road segment, and (ii) RSU trust evaluation for the global historical data. The main aim of this distinction is preventing coalition and platooning attacks. If we have a global idea about the past behavior of a node, we can combine it with information about its behavior within the current segment, and readily detect if it is participating in a coalition attack, or if it is part of a platoon composed of dishonest members sending positive reports about each other.

Figure 4.23 illustrates the used modules to compute both recent and historical RSU evaluations.

After filtering out reports coming from dishonest nodes, an RSU can compute a value representing the behavior of node j within its current road segment (SRSU(j)), and considering the time spent by the vehicle within that road segment. This time can be estimated using the segment's length and the vehicles' average speed, in addition to the traffic light waiting time. Equation 4.9 represents how

the SRSU updates its information about a node j based on received reports about j:

$$SRSU(j) = \frac{\alpha \cdot \sum P\_reports\_about\_j}{\beta \cdot \sum N\_reports\_about\_j + \alpha \cdot \sum P\_reports\_about\_j} \tag{4.9}$$

In addition, based on the different in-segment trust evaluation reports received, an RSU can compute a global historical trust value concerning all nodes since it is usually connected to other RSUs. This global historical trust for a node j ($HRSU(j)$) is updated as follows:

$$HRSU(j) = AVG\Big[HRSU(j), \frac{\alpha \cdot \sum P\_SRSUs\_about\_j}{\beta \cdot \sum N\_SRSUs\_about\_j + \alpha \cdot \sum P\_SRSUs\_about\_j}\Big] \tag{4.10}$$

Factors α and β are also used in both equations 4.9 and 4.10 for the same purpose as in the previous equations. In addition, when an RSU is available, every node i sends a list containing the identities j of nodes assumed to be dishonest ($\forall$ j /$GTR(i,j) \leq danger\_value$). Otherwise, it broadcasts a positive or negative recommendation about j based on its trust value $GTR(i,j)$.

4.3.2.3 Global trust computation

The global trust evaluation uses both vehicle-to-vehicle and RSU-to-vehicle to evaluate a node j as illustrated in figure 4.24

Every node i can build a global trust view about any other node j in the presence, as well as in the absence, of an RSU within its communication range. We call this global trust evaluation $GTR(i,j)$, and it will be updated periodically, although following a different procedure depending on whether nodes are in the presence of an RSU or not. The procedures are the following:

When located within an RSU's communication range, vehicles periodically receive both the historical (HRSU) and the in-segment (SRSU) behavioral trust of all nodes within the same segment. This allows every vehicle to have a clear idea about its direct and indirect neighborhood in order to prevent any kind of dishonesty. Equation 4.11 shows the global vehicle-to-vehicle trust updating process in the presence of an RSU:

$$GTR(i,j) = \beta \cdot \big[AVG[DTR(i,j),\ SRSU(j)]\big] + \alpha \cdot \big[AVG[ITR(i,j),\ HRSU(j)]\big] \tag{4.11}$$

To benefit from the global view provided by the RSU, we give more importance to the instant direct (DTR) and in-segment trust (SRSU) evaluations, instead of recommendations (ITR) and historical behaviour (HRSU). To this end, similarly to equation 4.6, we employ factors α and β, with (α + β=1) and ($\beta > \alpha$).

Similarly, in the case of vehicles outside the communication range of an RSU, they can evaluate each other based on the direct and indirect interactions, as well as on the last historical report of the RSU. The latter will be taken more or less into account depending on its freshness. In other words, we use the report's reception

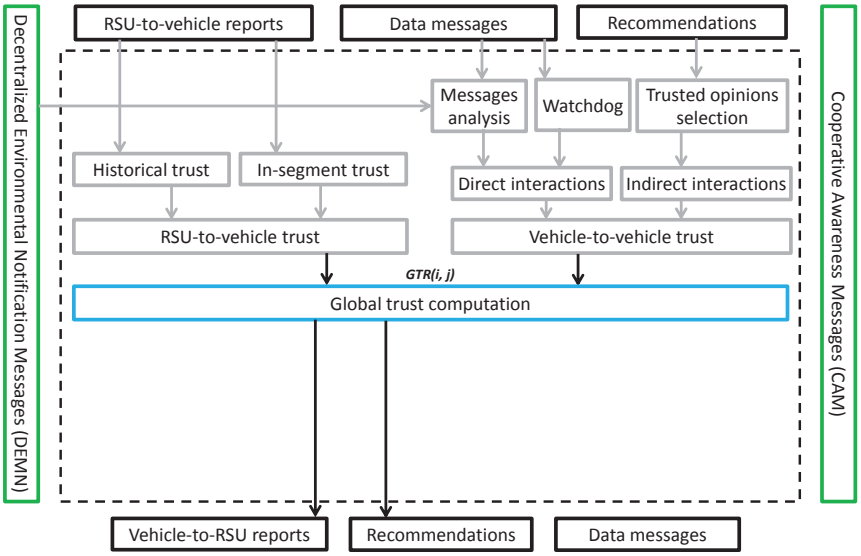


Figure 4.24: Global trust computation.

time (T0) with the current time (T) to compute its importance factor $\frac{T_0}{T}$. Then, the global trust evaluation (GTR) given by a node i to another node j is updated using equation 4.12:

$$GTR(i,j) = (1-\frac{T_0}{T})\cdot\big[(\beta\cdot DTR(i,j))+(\alpha\cdot ITR(i,j))\big]+(\frac{T_0}{T})\cdot\big[HRSU(j)\big] \quad (4.12)$$

In addition, if the new global trust evaluation $GTR(i,j)$ increases compared to its previous value, a positive recommendation about the node j is automatically broadcasted. In the other hand, if $GTR(i,j)$ decreases bellow a predefined threshold a negative recommendation is broadcasted.

4.3.2.4 ETSI-based trust establishment

In the facilities layer defined in the ETSI standard, the main components are the CAM and DENM basic services.

Cooperative awareness within road traffic means that road users and the roadside infrastructure are informed about each other's position, dynamics and attributes. Cooperative Awareness Messages (CAMs) are exchanged in the ITS network between ITS-Ss (Intelligent Transportation System-Stations) to create and maintain awareness of each other, and to support cooperative performance in the road network [CAM14]. In addition, ETSI ITS has defined a "Basic Set of Applications" where the Road Hazard Warning (RHW) application is composed of

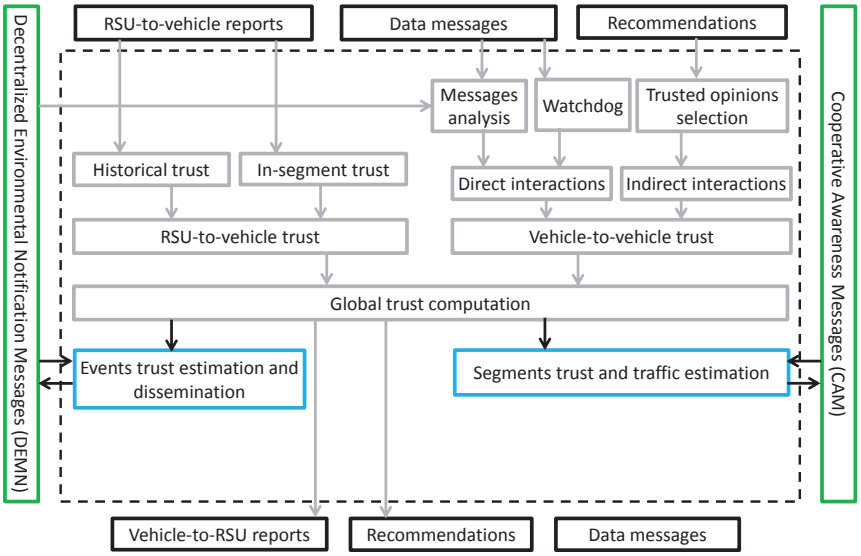


Figure 4.25: Events' trust, segments' trust, and traffic estimation modules.

multiple use cases. Those applications are supported by the decentralized environmental notification (DENM) basic service [DEN14].

In this work we take advantage of these messages (CAMs and DENMs) to continuously, and in a distributed manner, estimate the traffic density, the existence of dishonest nodes within road segments, and the trust-level associated to different events and their dissemination.

Involved modules in this phase are shown in figure 4.25

Segments' trust and traffic estimation

To estimate the degree of trust and the traffic density between two road junctions in a collaborative and distributed manner, we use three information sources: the total Number of Front and Rear Nodes (NFN, NRN), the rate of Trusted Front and Rear Nodes (TFN/TRN), and the Minimum Trust of Nodes in the Front and Rear (Min(TFN)/Min(TRN)).

We used the trusted nodes rate (TFN and TRN) in addition to the total number of nodes (NFN and NRN) to have a clear idea about the traffic density. Furthermore, in the message forwarding process, untrusted vehicles will be avoided because they behave as blackholes dropping messages.

The Minimum trust values (Min(TFN), Min(TRN)) are used to know the dishonest nodes distribution within the road segments.

Figure 4.26 represents a numerical example of such information carried by a vehicle labeled as A.

For fields Min(TFN) and Min(TRN), a value of 1 would only take place if all vehicles in a specific segment have a special role (e.g. police, ambulance), but this

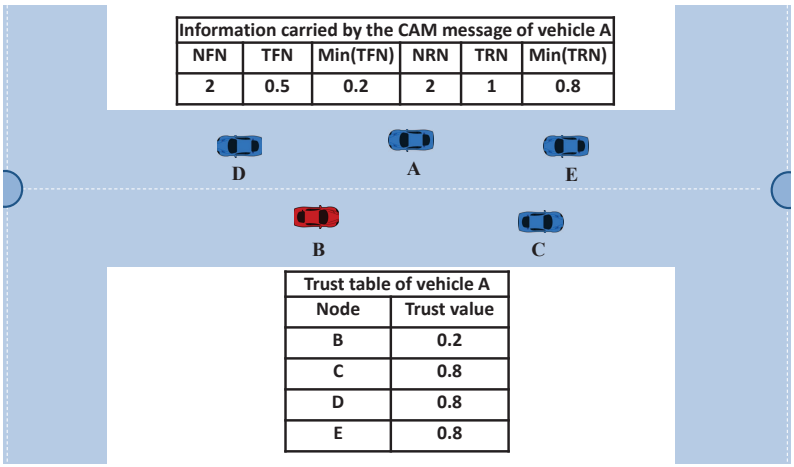


Figure 4.26: An example of traffic density and segment's trust information.

situation is not realistic, and so a value of 1 will never be reached (minimum trust will always be less than 1). A similar value can be achieved if all nodes within a segment consider each other trusted vehicles (*trusted vehicles ratio* = 1). In addition, every node i associates the previously computed trust value *GTR(i, j)* to each neighbor (see section 4.3.2.3).

We chose to take advantage of CAM messages [CAM14] by adding our security-related fields. This allows us to estimate the trust, the traffic density, and the dishonest nodes distribution within a road segment. More specifically, we extend the high frequency container since information within this container is continuously updated, which is also the case for traffic density and the trust values of nodes. The new format contains the previously mentioned information: Total Number of Front and Rear nodes (NFN, NRN), the Ratio of Trusted Front and Rear nodes (TFN/TRN), and the Minimum Trust at Front and Rear (Min(TFN)/Min(TRN)), as illustrated in figure 4.27.

In particular, to optimize the length of our fields, we represent the float information (TFN, TRN, Min(TFN), Min(TRN)) using only one byte for each. For example, if the Trusted Nodes Rate in the rear (TRN) is 0.99, carried value in TRN will be $(99)_2$.

Nodes maintain local information about their one-hop neighbors to perform trust and traffic density estimations. For the traffic estimation, the maintained fields are: (i) 'MyNFN' and 'MyNRN', which store the total number of one hop front/rear neighbors; (ii) 'MyTFN' and 'MyTRN', that store the ratio of trusted one hop front/rear neighbors; and (iii) 'Min(TFN)' and 'Min(TRN)', for the minimum trust in one hop front/rear neighbors.

Upon receiving a CAM message from the front or rear sides, the vehicles compare it with their own neighborhood information. The goal of this comparison is

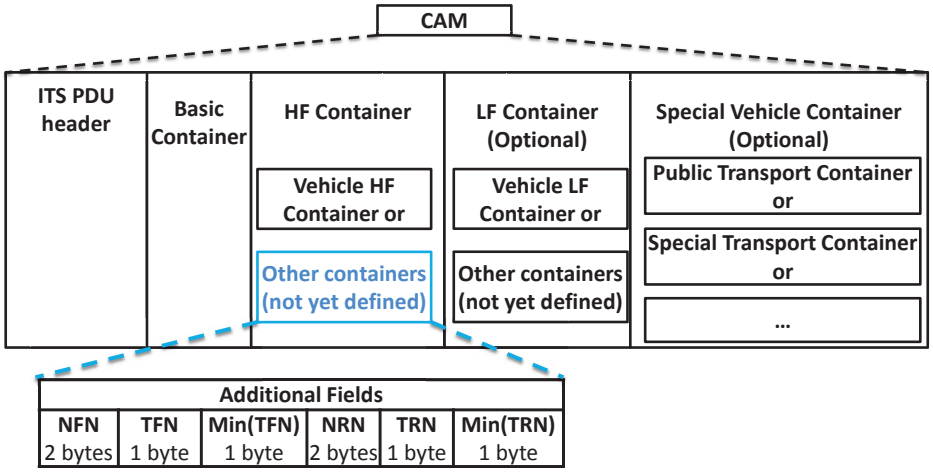


Figure 4.27: Additional Fields.

to gather accurate and precise information about the segment, meaning that this information will be used later on by vehicles located at junctions to choose the best segment, and by in-segment vehicles to choose the most adequate next hop for unicast data messages.

For more accuracy, every node i only takes into account messages coming from its farthest trusted neighbor j both at front and rear to select the most accurate and fresh information, updating its current security metrics following algorithm 8.

When a vehicle 'i' located within a road segment receives a CAM message broadcasted by another node 'j' located at its front/rear, it computes: the number of front/rear vehicles, the front/rear trusted vehicles ratio, and the minimum trust value of front/rear vehicles. Since we take into account just CAMs coming from trusted nodes 'j', these last can be located near to the receiver node 'i'. Hence, to avoid re-counting common neighbors we used the 'cardinal' function.

In the other hand, if the vehicle 'i' is located within a junction, it associates a weight called SW ("Segment Weight") for every segment 'k', this weight is computed using the received traffic and trust information from vehicles located in segment 'k', and it will be used later on to choose the most adequate path in the message routing process.

Algorithm 8 Segments' trust and traffic estimation

INPUTS: CAM messages broadcasted by j and received by i.
OUTPUTS: updated CAM for i; segments' weights computed.
Upon receiving the estimation fields from j by i;
if (i is located within a road segment) **then** (see figure 4.21 in-segment part)
    if (j in front of i) **then**
        NFN(i) ← MyNFN + NFN(j) - [Card(one hop Front Neighbors of $i \cap$ Front Neighbors of j)];
        TFN(i) ← MyTFN + TFN(j) - [Card (one hop Trusted Front Neighbors of $i \cap$ Trusted Front Neighbors of j)];
        Min(TFN) ← Min [MyMin(TFN), Min(TFN)(j)];
    else (j in rear of i)
        NRN(i) ← MyNRN + NRN(j) - [Card(one hop Rear Neighbors of $i \cap$ Rear Neighbors of j)];
        TRN(i) ← MyTRN + TRN(j) - [Card (one hop Trusted Rear Neighbors of $i \cap$ Trusted Rear Neighbors of j)];
        Min(TRN) ← Min [MyMin(TRN), Min(TRN)(j)];
    end if
else (i is located within a junction, see figure 4.21 in-junction part)
    $\forall$ k $\in$ { A, B, C}
    if (The vehicle in 'k' is entering the junction) **then**
        $SW_k \leftarrow NFN_{V_k} \cdot TFN_{V_k} \cdot Min(TFN)_{V_k}$;
    else (The vehicle in 'k' is leaving the junction)
        $SW_k \leftarrow NRN_{V_k} \cdot TRN_{V_k} \cdot Min(TRN)_{V_k}$;
    end if
end if
End

Event trust and trusted alert dissemination

DENM messages are mainly used by cooperative Road Hazard Warning (RHW) applications in order to alert road users about the events detected. A cooperative RHW application is an event-based application composed of five containers, where two of them are mandatory (ITS PDU header and Management Container), and the other three are optional (Situation Container, Location Container, and Alacarte container). For more details about these containers, please refer to [DEN14].

In addition to the ITS PDU Header container, in this work we focus on the management, and the situation containers (see Figure 4.28).

In the Management container, some event-related information is defined including the traffic direction, the validity duration and the relevance distance representing the maximum distance beyond which DENMs should not be disseminated. This important information will be used in the dissemination part in addition to the computation of DENM similarities.

For the situation container, the application layer provides an information quality value varying from 0 to 7 representing the event's message effectiveness. A classification of events, along with a set of 99 event-related causes, are also avail-

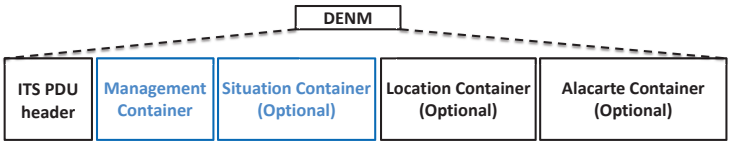


Figure 4.28: DENM format.

able in the standard, which can improve the similarity evaluation [DEN14].

Generally, the trust given to a specific event is related to the level of honesty associated to the event report originator. In addition, some context-based information may be used to ensure reliable event report dissemination. For example, we can decide not to accept notifications about ice on the road when having a temperature superior to 20^{o}, or that a road is congested from midnight to 6 a.m in normal situations. To this end, DENM messages contain fields describing the reported event in a clear and precise manner.

Operations that can be done on these messages are three: triggering, updating and termination of the event. While the first two are a task of the originator node, the third one includes cancelation and negation, and it can be done by any intermediate node.

Unlike nodes' trust, the event's trust (ETR) is a value computed on the fly for a specific event. In our case, this value is computed using the originator global trust (GTR) and the event credibility through the received information quality (from the situation container). Then, if the event's trust is higher than a predefined threshold, a validity test is done on the DENM before rebroadcasting it; otherwise, it is dropped. In addition, if node i decides to rebroadcast node j's event messages, it increases its message quality $Qmsg(i, j)$, decreasing it otherwise since this communication is considered a direct interaction. Algorithm 9 describes the proposed trust-based DENM dissemination process.

Algorithm 9 Trust-aware DEN messages dissemination process

INPUTS: Alert of an event 'E' sent by a node j (DENM message).
OUTPUTS: Direct interaction evaluation; relay or drop the alert.
Upon receiving a DENM;
$ETR(E,j) \leftarrow \rho \cdot InfoQuality(E) + (1-\rho) \cdot GTR(i,j)$;
if $(ETR(E,j) \geq$ TrustToSend) **then**
    $Qmsg(i,j) \leftarrow Qmsg(i,j) + \delta$;
    if (Relevance distance and Validity duration) $\leq$ limits) **then**
        Broadcast (DENM);
    else
        Cancel (DENM);
    end if
else
    $Qmsg(i,j) \leftarrow Qmsg(i,j) - \mu$;
end if
End

In the case of DENM messages, and since we focus on safety situations, we give more importance to the event information quality than to its originator's trust. This is achieved by multiplying it by the message credibility factor (ρ), which is in the range $0.7 \leq \rho \leq 1$, thereby insuring that message credibility has always a higher impact. The event information quality ($InfoQuality(E)$) is a field included within every generated DENM representing the credibility of the reported event E; for more details please refer to [DEN14].

In addition, we consider DENM's information as a vector A of n elements. Every element represents the value of specific information parameters. For instance: A[1] = event latitude, A[2] = event longitude, A[3] = validity duration, etc. Then, for every pair of sources *(Vj, Vk)*, we perform an offline computation of the similarities between DENMs describing the same event, but coming from different sources *Vj*. Finally, common sources in all inadequate similarities have their trust level decreased. By comparing information carried by periodical CAM messages to the RSU, the latter will be able to detect whether trusted nodes within a road segment are more or less numerous than malicious ones. Based on this information, it decreased the RSU historical trust (HRSU) of vehicles with low similarity values. Algorithm 10 summarizes this process.

Algorithm 10 Events reporters honesty using DENMs similarity

INPUTS: A set of nodes Vi reporting a same event.
OUTPUTS: Historical RSU-to-vehicle trust updated.
For every pair of event reporters *(Vj, Vk)* do;
Similarity*(Vj, Vk)* $\leftarrow \frac{1}{\sum_{i=0}^{n}(A_{Vj}[i]-A_{Vk}[i])^2}$;
if *Vj* and *Vk* reports are not similar **then**
    Increment (Counter of *Vj* low similarities);
    Increment (Counter of *Vk* low similarities);
end if
if TFN|TRN $\geq$ NFN|NRN/2 **then** (there are more trusted than dishonest nodes)
    if (*Vj* appearance frequency $\geq$ NFN|NRN/2) **then**
        HRSU(j)$\leftarrow$ *HRSU(j)*-μ;
    end if
else (there are more dishonest nodes than trusted ones)
    if (*Vj* appearance frequency $\leq$ NFN|NRN/2) **then**
        HRSU(j)$\leftarrow$ *HRSU(j)*-μ;
    end if
end if
End

A_{Vj} and A_{Vk} are the vectors representing the DENM's information of vehicles j and 'k', respectively.

4.3.3 Trusted communication and data routing

In addition to the continuous trust and traffic estimation, our additional fields carried by CAM messages allows in-junction and in-segment nodes to collaborate with each other to choose the most suitable path to the destination whenever data must be delivered (see figure 4.21).

Involved modules in this last phase are shown in figure 4.29

Upon receiving a data message, node i checks the source's trustfulness GTR(i, source). If it is lower than the predefined 'TrustToSend' threshold, the message will be dropped; otherwise, the forwarding process continues. Then, if vehicle i is the destination, it performs data verification on the received message. This verification allows evaluating the senders' behavior based on the quality of its message. If node i is just an intermediate node, we distinguish two cases:

- In-segment case: if the position of i is within a segment, it has to select as the next hop the most trusted, stable and close to the destination/junction node among its neighbors.
- In-junction case: if the position of i is within a junction, it has to select the most trusted and close segment to the destination to forward the message through it.

Algorithm 11 summarizes the data delivery process.

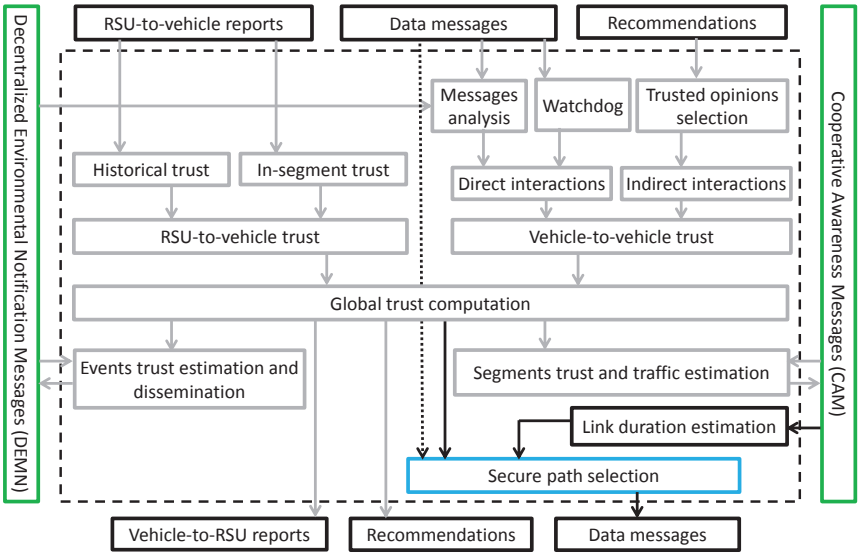


Figure 4.29: Trusted communication and data routing modules.

Algorithm 11 Trust-aware inter-vehicular communication

INPUTS: Data message sent/forwarded by j to i.
OUTPUTS: Data message accepted/dropped; Direct trust updated; Best path selected.
When a data message from 'source' is received by i;
if ($GTR(i, Source) \geq$ TrustToSend) **then**
  if (End destination is i) **then**
    Data verification (msg);
    if (legal (msg)) **then**
      $Qmsg(i, Source) \leftarrow Qmsg(i, Source)+\delta$;
    else
      $Qmsg(i, Source) \leftarrow Qmsg(i, Source)-\mu$;
    end if
  else
    if (Destination is a neighbor of i) **then**
      Deliver ('msg' to destination);
    else (i is an intermediate node)
      if (i is an In-segment node) **then**
        For every neighbor 'k' of i
        if (Destination in segment) **then**
          Score(k) $\leftarrow \frac{GTR(i,k) \cdot LD(i,k)}{Distance(k,destination)}$;
        else (Destination out of segment)
          Score(k) $\leftarrow \frac{GTR(i,k) \cdot LD(i,k)}{Distance(k,nextjunction)}$;
        end if
        Transfer ('msg' to 'k' having max score);
      else (i is an In-junction node)
        For every segment 'k';
        Score(k) $\leftarrow \frac{SW(k)}{Distance(junction,destination) through' k'}$;
        Transfer ('msg' through 'k' having max score);
      end if
    end if
  end if
else (low trust $GTR(i, source)$)
  Drop (msg);
end if

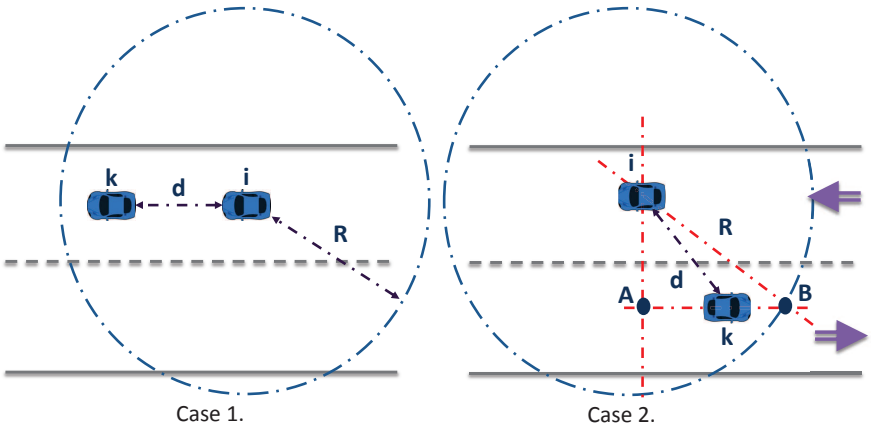


Figure 4.30: Link duration estimation.

δ, μ are the trust increment and decrement factors. We take $\delta \ll \mu$ since peer trust is difficult to build up but easy to tear down.

'SW' is the segment weight computed in the continuous trust and traffic estimation presented in the previous section. $LD(i,k)$ is an estimation of the link duration between the two nodes i and k, and it is computed as follows:

- In the case of two vehicles moving with similar directions:

  $$LD(i,k) = \begin{cases} \frac{R+d}{|V(i)-V(k)|} & V(i) \geq V(k) \\ \frac{R-d}{|V(i)-V(k)|} & V(i) < V(k) \end{cases}$$

  Where $V(i)$ is the velocity of i, R is the communication range, and d is the distance between i and k.

- In the case of two vehicles moving in opposite directions:

  $$LD(i,k) = \frac{|L+X|}{|V(i)-V(k)|}$$

  Where $L = \sqrt{R^2 - (y_i - y_k)^2}$; $X = x_i - x_k$; $L = distance(A,B)$ and $X = Distance(A,k)$ (see figure 4.30).

4.3.4 Performance evaluation

To evaluate our Trust establishment scheme we relied on the NS-2 simulator [IH11]. The generated vehicular traffic is based on the Citymob mobility model [MCCM08], which uses SUMO [BBEK11] to create mobility traces based on real maps extracted from OpenStreetMap. In our case we used a map from the downtown area of Valencia, Spain (see figure 4.31).

Table 4.4 summarizes the main simulation parameters:

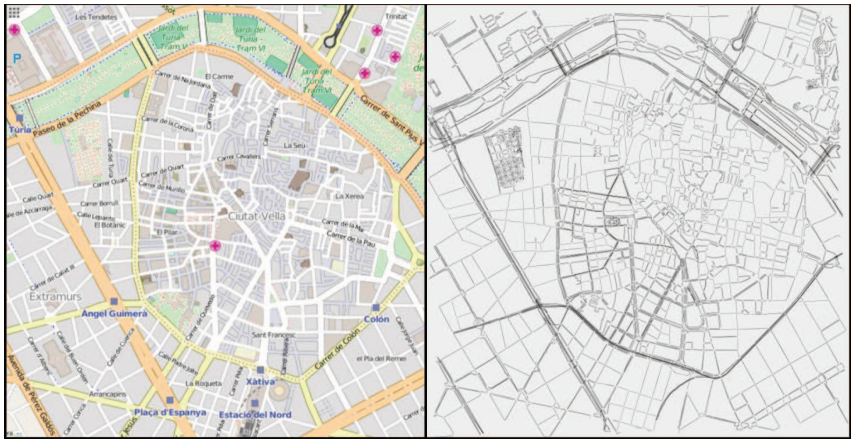


Figure 4.31: Simulated scenario of Valencia city, Spain.

Table 4.4: T-VNets simulation parameters.

Parameters	Value
Simulation area (km×km)	2×2
Transmission range (m)	300
Permissible lane speed (km/h)	[0,80]
Number of vehicles	[0,400]
State cars percentage (fully trusted) (%)	2
All trust metrics initial values	0.5
α	0.4
β	0.6
δ	0.01
μ	0.1
RL	0.2
ρ	0.7

Trust increment and decrement factors (δ, μ) are the same as in [ZCC13], while the values of α, β, RL and ρ are chosen in such a way so as to achieve the best possible performance based on a large set of experiments.

In addition, we assume that we have 6 RSUs randomly distributed. 10 events occur at random simulation times. Moreover, vehicles can exchange unicast data messages. To avoid consuming too many resources, and considering that trust variations do not require a higher refresh rate, we have adopted a frequency of

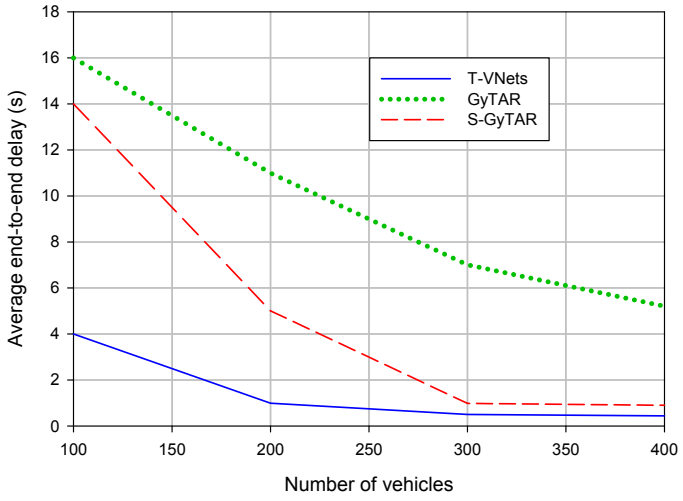


Figure 4.32: Average end-to-end delay of unicast data messages.

0.5 Hz for our extended CAM messages, possibly extending only 1 message every 2 seconds with trust information, while CAM messages are transmitted at the typical 10 Hz rate.

We divide our performance evaluation section into two parts: (i) Impact on network performance when compared to an insecure routing protocol; and (ii) Security performance, describing the achieved security results when compared to other existing works.

4.3.4.1 Network performance

In this part we discuss the impact of establishing trust on the network resources in terms of: average end-to-end delay, packet delivery ratio, and network overhead. We compare our proposal against both secure and insecure versions of the GyTAR routing protocol [JSRGD09, BAS14], in the presence of 20% of nodes acting as blackholes.

Figure 4.32 shows that our proposal performs better than both GyTAR versions, delivering packets to their end destinations with a reduced delay, typically not exceeding a second if the number of vehicles is higher than 200.

Similarly to the Average end-to-end delay, our solution can ensure a high efficiency in terms of packet delivery ratio, approaching optimal values whenever a fully connected network is available (see figure 4.33).

In terms of additional overhead, figure 4.34 shows that our solution is injecting an acceptable load into the network, being lower than the one introduced by the GyTAR protocol. Notice that, since our solution is based on the standard, it does not add a significant amount of overhead or additional messages. This means that the overhead introduced is mainly due to RSU reports and trusted nodes recommendations.

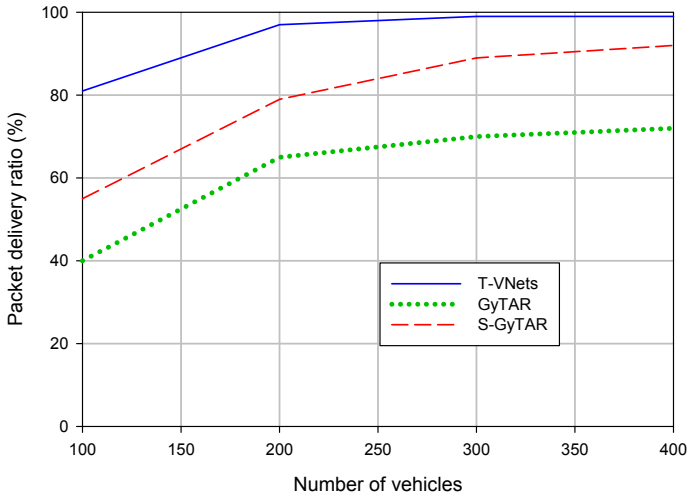


Figure 4.33: Packet delivery ratio.

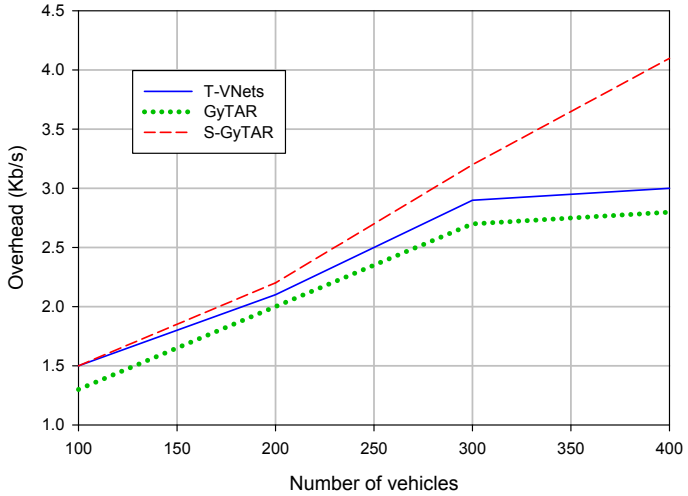


Figure 4.34: Generated Overhead.

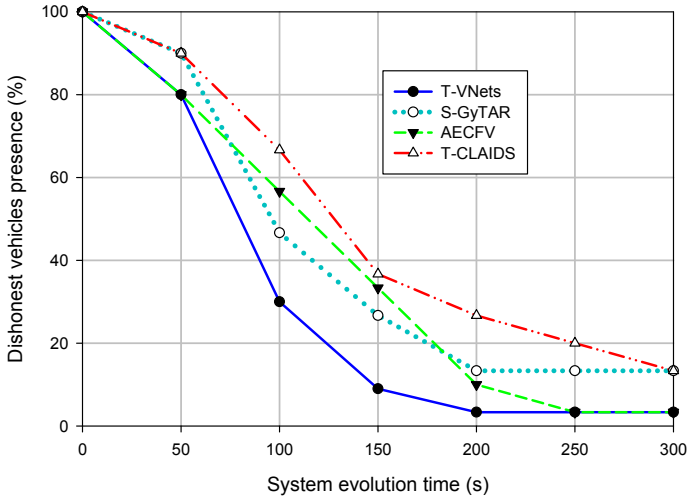


Figure 4.35: Dishonest nodes detection ability during 300s of simulation time.

4.3.4.2 Security performance

In this part we study the achieved security results of our proposal when compared to the T-CLAIDS [KC14] and the AECFV [SS15] trust establishment schemes, in addition to the secure version of the GyTAR protocol (S-GyTAR) [BAS14]. The comparison will be in terms of dishonest vehicles detection ratios and percentage of wrong decisions. Moreover, we analyse the impact of deactivating some elements of our security architecture on performance results.

4.3.4.3 Dishonest nodes detection efficiency

In this part we discuss the ability of our proposal to detect dishonest nodes compared to other existing solutions. To this purpose we fix the number of nodes within the network at 300, and configure 30% of them to behave maliciously.

Figure 4.35 shows that our system has detected nearly 97% of the existing dishonest nodes in about 200s, while AECFV requires 25% additional time to achieve the same results. This is due to the variety of trust metrics used, and to the ability to estimate the distribution of dishonest nodes in our system. Concerning the S-GyTAR and T-CLAIDS protocols, they achieve poorer performance levels.

In the second scenario we study the system scalability. With this purpose we vary the number of nodes within the network from 100 to 400 nodes, where 30% of them have a malicious behavior (33% keep sending messages at a high rate, 33% drop all received packets, and 33% send false alerts). In addition, dishonest nodes broadcast only positive reports about each other.

Similarly to the dishonest nodes detection results (see figure 4.35), T-VNets is able to maintain its resilience even in the presence of a high number of nodes, offering performance results comparable to those of the AECFV protocol, and performing much better than the two other solutions (see figure 4.36). This detec-

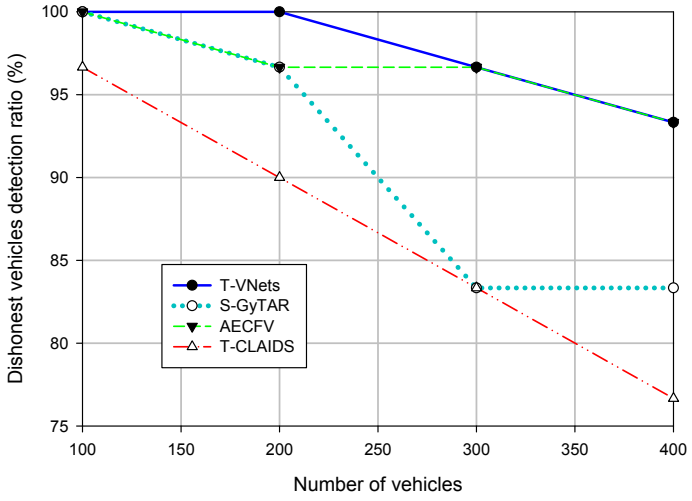


Figure 4.36: Dishonest nodes detection for different densities.

tion stability is mainly due to the cooperation among nodes, which means more information is handled to the RSUs and, therefore, more accurate decisions can be made.

The last scenario analysed measures the resilience of our proposal when varying the dishonest nodes' ratio. Figure 4.37 shows that our solution improves upon AECFV in the presence of a high ratio of dishonest nodes. This is mostly due to the fact that AECFV has no previous estimation about the ratio of dishonest nodes and their distribution within the network, contrarily to our proposal.

Dishonest nodes detection accuracy

Similarly to any security system for mobile and distributed networks, the existing solutions are prone to trigger some false positives when detecting dishonest nodes.

To evaluate the impact of this problem we varied the dishonest nodes ratio over a total of 300 nodes, studying how many honest nodes are wrongly considered dishonest at the end of the simulation.

Figure 4.38 shows that, in the detection process, T-VNets generates about 4.7% of false positives when half of the nodes are dishonest; this is generally due to their presence in a zone containing a high ratio of dishonest nodes, or because they have relayed some malicious messages coming from these dishonest nodes. This is prone to occur right at the beginning of an experiment, when no previous interactions have occurred. However, T-VNets is able to clearly provide improvements compared to the three other solutions (see figure 4.38).

Trust metrics impact

Finally, we discuss the impact of the different trust metrics used. We vary the number of node used from 50 to 400, with 30% of them behaving maliciously, and compare our protocol against other three slimmed-down versions of itself:

- *T-VNets*: this version shows the performance of our full proposal.

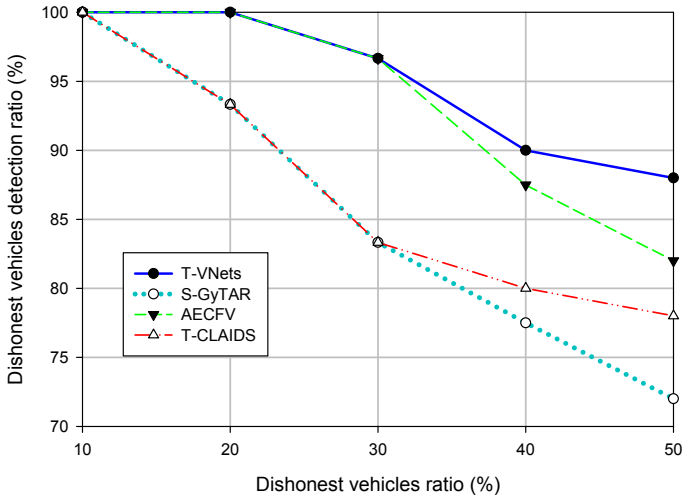


Figure 4.37: Dishonest nodes detection effectiveness when varying their number.

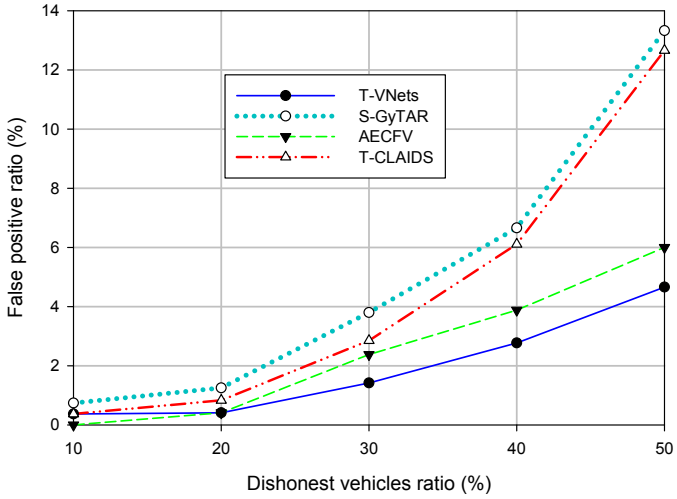


Figure 4.38: Generated false positive.

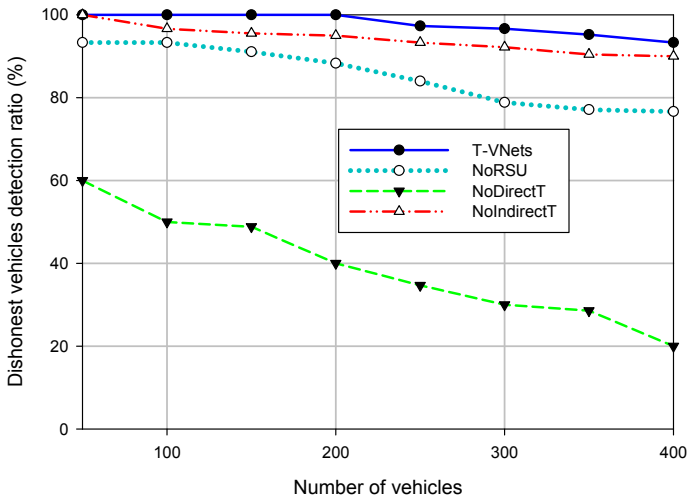


Figure 4.39: The different trust metrics' impacts.

- *NoRSU*: it shows the performance of T-VNets when no RSUs are available.
- *NoDirectT*: it shows the performance achieved when direct trust metrics are not used. Unlike the other versions, this one is computed after 100s of simulation time since trust will never be updated if there are no interactions among nodes.
- *NoIndirectT*: it shows the performance achieved when no recommendations are exchanged among nodes.

Figure 4.39 shows that the key element in T-VNets is the use of direct trust metrics, which are much more relevant than the other elements (RSU and Indirect trust). As a result, we find that it is possible to reduce the generated overhead (see figure 4.40) by reducing the number of recommendations since the impact of the latter is reduced compared to the other metrics.

4.4 Trusted opportunistic alerting system

In this section we explain our trust-aware dissemination mechanism for VANET safety applications that takes advantage of ETSI ITS standardized messaging services, more specifically of the Decentralized Environmental Notification Messages (DENM) [DEN14], to carry the required information for establishing trust among vehicles. These messages are mainly designed to support cooperative Road Hazard Warning (RHW) applications, which allow alerting road users about the events detected. Our solution becomes easy to deploy by being ETSI ITS standard-based, completely distributed, and software-oriented. In addition to these advantages, it can also ensure a trusted dissemination of alerts without causing a broadcast storm problem. This is achieved by using the trust information among vehicles to

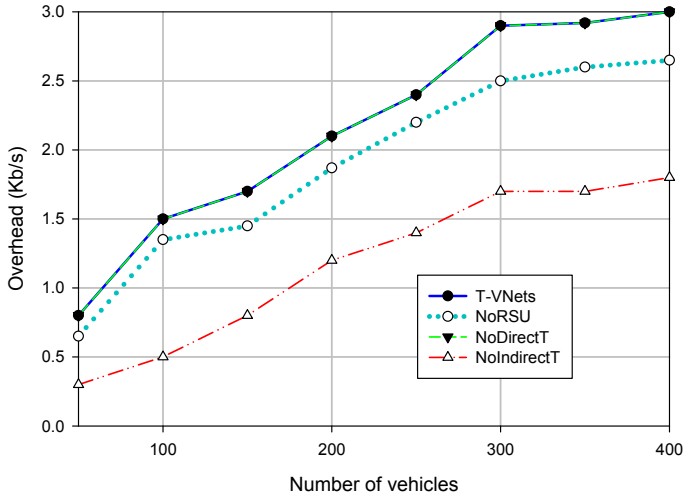


Figure 4.40: Generated Overhead by T-VNets in different versions.

select the most trusted vehicles as next broadcasters of DENMs, and by punishing vehicles sending false alerts and acting as blackholes.

Our proposal is mainly based on the information carried by DENM messages about a specific event. It uses the trust among vehicles to ensure a wide, trusted, and non-redundant dissemination of DENM messages. Figure 4.41 illustrates how we propose to extend the classical protocol stack in order to support such opportunistic broadcasting. Our proposal can be divided into two main components: (i) trust establishment module, and (ii) opportunistic broadcasting module.

Concerning the trust establishment module, it is responsible for evaluating direct interactions between vehicles, as well as their degree of collaboration in different network operations. Thus, honesty indexes called 'Trust' are computed by every vehicle concerning its neighbors; this trust value will be carried by DENM messages, and will then be combined with the generated event messages' quality to compute a belief degree about the validity of the reported event. Finally, the opportunistic broadcasting module is responsible for selecting the best next broadcaster of the reported event. The latter's identity is also piggybacked onto the DENM message.

As shown in figure 4.42, in order to take advantage of these DENM messages, we added two other fields: (i) 'Next broadcaster' in the management container, which will contain the selected next broadcaster in the DENM's opportunistic broadcasting process; and (ii) 'Belief degree (BD)' in the situation container, which represents the last broadcaster's belief about the veracity of the reported event.

4.4.1 Inter-vehicular trust establishment

Trust establishment usually includes two main factors: direct, and indirect trust. Direct trust is the evaluation of the direct interactions among vehicles represented

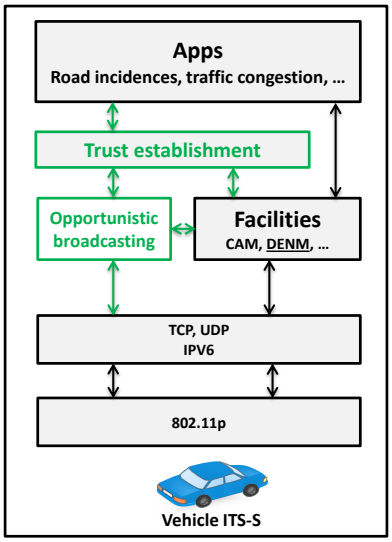


Figure 4.41: The proposed protocol stack.

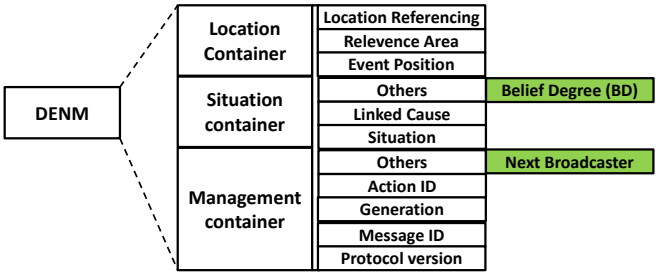


Figure 4.42: Proposed DENM extension.

in this solution by $MsgQ(i,j)$, which means the quality of messages sent from j to i. Instead, indirect trust is usually based on the exchanged recommendations among vehicles. However, in the safety context, exchanging recommendations is not always the best solution since it introduces a significant overhead in addition to bandwidth requirements. In our case, every vehicle remains in promiscuous mode, and it will evaluate its neighbors based on the dropped/broadcasted ratio for safety messages whenever a neighbor is selected as the next broadcaster. We call this evaluation result $NetC(i,j)$ for the network collaboration of j from the perspective of i.

Equation 4.13 represents the trust value $Trust(i,j)$ of a vehicle j from the perspective of i, which is a combination of old evaluations of the current messages quality' $MsgQ(i,j)$ and the in-network collaboration $NetC(i,j)$ of a vehicle j. Its initial value is 0.5, and is then updated accordingly.

$$Trust(i,j) = \sqrt{Trust(i,j) \cdot \sqrt{NetC(i,j) \cdot MsgQ(i,j)}} \tag{4.13}$$

As mentioned before, the network collaboration of a neighbor vehicle j computed by i ($NetC(i,j)$) is the ratio of the broadcasted messages $\#B(i,j)$ compared to the total number of both brodcasted $\#B(i,j)$ and dropped $\#D(i,j)$ messages. Equation 4.14 describes the $NetC(i,j)$ calculation.

$$NetC(i,j) = \frac{\#B(i,j)}{\#D(i,j) + \#B(i,j)} \tag{4.14}$$

Concerning the $MsgQ(i,j)$ value, it will be increased or decreased depending on the received messages' quality, which will be included in algorithm 12. Moreover, same as $Trust(i,j)$, the messages' quality $MsgQ(i,j)$ is initially equal to 0.5.

Whenever a vehicle receive a DENM message, it computes a belief degree about the message $BD(i,DENM)$ based on its broadcaster B trust evaluation $Trust(i,B)$. The two pieces of information included within the DENM message are: (i) the belief degree of the broadcaster $BD(B,DENM)$ and (ii) the information quality of the described event $InfoQ(Event)$. As mentioned in the previous section, $InfoQ(Event)$ varies from 0 (for the lowest quality) to 7 (for the highest one). In our case, we use this information as 8 values varying from 0 to 1 (0.125, 0.25, 0.375, ..., 1). Equation 4.15 shows how the belief degree is computed.

$$BD(i,DENM) = \sqrt{Trust(i,B) \cdot \sqrt{BD(B,DENM) \cdot InfoQ(Event)}} \tag{4.15}$$

This value will be used later on in algorithm 12 to decide either to: (i) consider the DENM as true report, and thereby increase the reporter's messages quality $MsgQ(i,j)$ and broadcast the DENM again if still valid, or (ii) consider the DENM as a false alert, hence decreasing the reporter's messages quality $MsgQ(i,j)$ and dropping the DENM messages.

4.4.2 Opportunistic alerts dissemination

To avoid the broadcast storm problem while informing the maximum possible number of vehicles in the surrounding area about any event, we select the best next broadcaster on every single hop. The selected next broadcaster is the farthest trusted neighbor to insure coverage of the maximum additional area [LHL+07, VBT10]. Equation 4.17 shows the selection of the next broadcaster j among the neighbors of a vehicle i based on a pre-computed score for every neighbor (see equation 4.16):

$$Score(i,j) = \frac{Trust(i,j)}{Distance(i,j)} \tag{4.16}$$

$$NextB = j \ / \ Score(i,j) = Max\{Score(i,j),\ \forall\ j \in Neighbors\ of\ i\} \tag{4.17}$$

Once the re-broadcasting is done, vehicles receiving the same DENM can again drop it and remove the saved version of this DENM as well. Moreover, in the case of a broadcasting failure, one of the informed vehicles should take the broadcasting decision. In addition, two or more neighbors of a vehicle 'i' are not always neighbors of each other. Hence, even if the next broadcaster selected broadcasts the DENM, we can still have some neighbors that remain uninformed about this action. The latter should rebroadcast the DENM to cover other non-informed zones.

In this case, upon receiving a DENM, every neighbor j triggers a timer following the distance to the safety message's source i and the communication range. If it does not receive another valid copy of the DENM during a computed waiting time, it rebroadcasts the DENM message again.

Equation 4.18 describes how this waiting time can be computed:

$$WaitingTime = DistanceT(i,j) + TT + PT + PRT \tag{4.18}$$

where $DistanceT(i,j)$ is the distance-based waiting time as proposed in [BL02, BK06, DJ07], used in such a way that the farthest neighbor will have the shortest waiting time. TT, PT and PRT correspond to the maximum Transmission, Propagation, and message PRocessing Times, respectively.

Algorithm 12 summarizes the DENMs' multi-hop dissemination procedure. When vehicle i receives such a message sent by another vehicle j, it checks the belief degree $BD(i, DENM)$ computed using equation 4.15. If this degree is lower than a predefined threshold, the DENM will be dropped and the message quality of j will be decreased by β. Otherwise, the broadcasting process should continue, and the message quality of j will be increased by α. We chose $\beta \gg \alpha$ to satisfy the main trust feature, which is: *"trust must be hard to win and easy to lose"*.

Afterward, if i finds its identity included within the DENM, this means that it is the one selected as next-hop broadcaster. In addition, if the included identity is not even part of i's neighbors list, it verifies the DENM's validity, selects the next broadcaster, and rebroadcasts the DENM once its waiting time has expired. However, if the DENM's validity expires, the latter will be logically canceled. Otherwise, if i is not the selected vehicle for rebroadcasting the DENM, and if its waiting time has expired without receiving another copy of the DENM, it selects

a new next broadcaster and broadcasts the DENM. This last case means that the selected broadcaster is among the neighbors of i, but he did not broadcast the DENM.

Algorithm 12 DENM multi-hop dissemination

```
1: Upon receiving a DENM from i broadcasted by j;
2: if (BD(i, DENM) ≥ TrustThreshold) then
3:     MsgQ(i,j)← MsgQ(i,j)+ α
4:     if ('i' is the next broadcaster OR next broadcaster ∉ neighbors list of 'i'
   ) then
5:         if NotExpired(DENM, relevance distance, validity duration) then
6:             NextB ← Select next broadcaster (Equation 4.17);
7:             Broadcast(DENM, BD(i, DENM), NextB);
8:         else
9:             Cancel (DENM);
10:        end if
11:    else
12:        WaitingTime ← Compute waiting time (Equation 4.18);
13:        if Expired(WaitingTime) AND NotRreceived(DENM, NextB) then
14:            NextB ← Select next broadcaster (Equation 4.17);
15:            Broadcast(DENM, BD(i, DENM), NextB);
16:        end if
17:    end if
18: else
19:    Drop(DENM);
20:    MsgQ(i,j)← MsgQ(i,j)-β
21: end if
22: End
```

4.4.3 Simulation results

To evaluate our proposal we relied on the NS-2 simulator modified to support the IEEE 802.11p standard and using the RAV propagation model [MFC+10]. The generated vehicular traffic is based on the Citymob mobility model [MCCM08], which uses SUMO [BBEK11] to create mobility traces based on real maps extracted from OpenStreetMap using the Krauss Mobility model [KHRW02]. In our case we used a map from the downtown area of Laghouat, Algeria (see figure 4.43).

Table 4.5 summarizes the main simulation parameters:

Figure 4.43: Simulated scenario of Laghouat city, Algeria.

Table 4.5: Simulation parameters.

Parameters	Value
Simulation area (km×km)	2×2
Simulation time (s)	300
Transmission range (m)	300
Permissible lane speed (km/h)	[0,80]
Number of vehicles	{100, 200, 300, 400}
Dishonest vehicles presence (%)	{0, 15, 25}
TrustThreshold	0.5
α	0.01
β	0.1

To evaluate our proposal's performance we assume that 15 % and then 25% of the vehicles are dishonest vehicles injecting false alerts, and acting as blackholes. We also assume that an event occurs every 10 seconds. We note that Φ represents the dishonest vehicles ratio within the network.

Figure 4.44 shows the detection effectiveness of our proposal when varying the vehicle density for Φ=15% and Φ=25%. In our case, an attacker is detected whenever its trust decreases below the predefined trust threshold (TrustThreshold) which we fixed at 0.5 in these tests. Figure 4.44 also evidences that our proposal can offer high detection ratios exceeding 91% in presence of 25% of attackers, whereas the detection performances are almost optimal for more realistic scenarios of Φ=15% or less.

Same as any security system, a certain margin of error should exist. However, some network features such as vehicle density, MAC layer collision problems, and

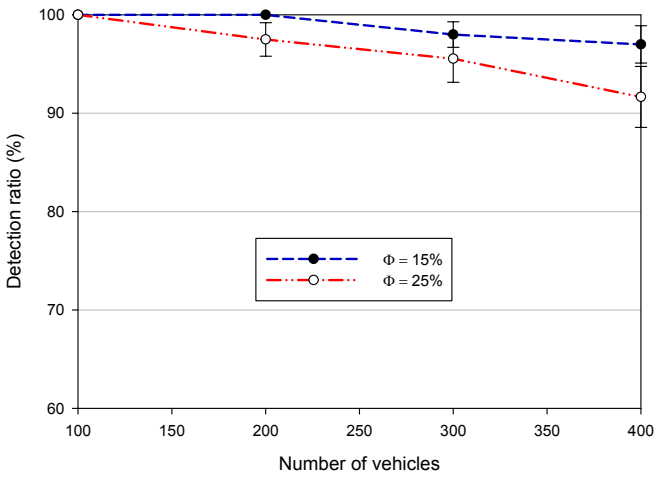


Figure 4.44: Detection performances for different vehicular densities when 15% or 25% the vehicles are dishonest.

the roadmap itself can directly influence how large this margin of error is.

Figure 4.45 represents the alert messages' loss ratio for different vehicle densities. Unlike the previous scenario, we also simulated the case of an ideal network that is free of attackers (Φ=0), in addition to the cases where Φ=15% and Φ=25%. Figure 4.45 shows that, except for the case of low density ($\leq$100 vehicles) our proposal causes less than 10% alert losses (including the network-related issues). Hence, more than 90% of the generated alerts about real events are canceled when the relevance area is reached, or the validity has expired, and not because alerts are dropped by an attacker. This behaviour is achieved thanks to the efficient next broadcaster selection procedure used in our proposal. In addition, alert loss ratios have grown for the high density case ($\geq$400 vehicles) mainly because of collision problems.

Moreover, some false alerts have been broadcasted since the initial trust value allows all vehicles to participate in all network operations. However, once the initial trust is updated according to the vehicles' behaviour, dishonest nodes are automatically dismissed. Figure 4.46 shows how the wrong decisions ratio varies with vehicular density in the presence of 15% and 25% of the nodes acting maliciously. Resulting curves clarify that, even in the presence of a high ratio of attackers (Φ=25%) and a high density of vehicles (400 vehicles), more than 90% of the broadcasting decisions where correct. We also notice that most the wrong decisions occurred at the beginning of experiments. In addition, for the case where Φ=15%, wrong decisions ratios are reduced, and do not exceed 4.2% in the worst case.

Finally, to show the importance of keeping vehicles in promiscuous mode after receiving a first copy of an alert, we compare the detection performances and the

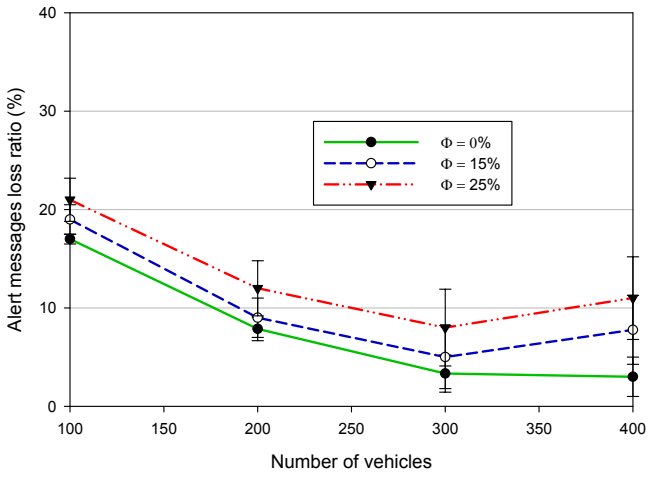


Figure 4.45: Alert messages loss ratio for different densities when 0%, 15% and 25% of the vehicles are dishonest.

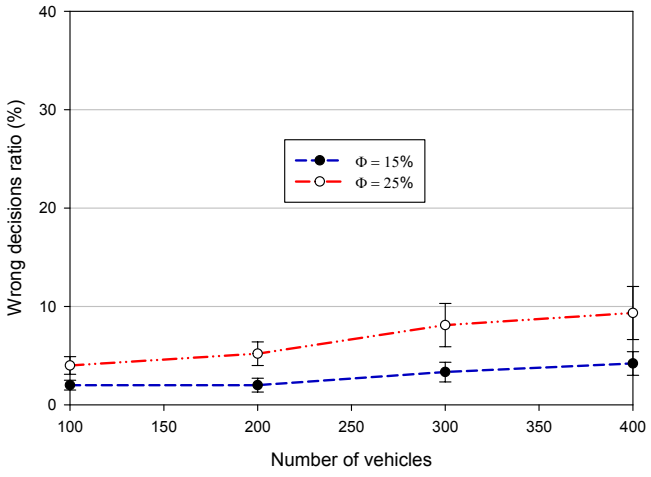


Figure 4.46: Wrong decisions ratio for different densities when 15% and 25% of the vehicles are dishonest.

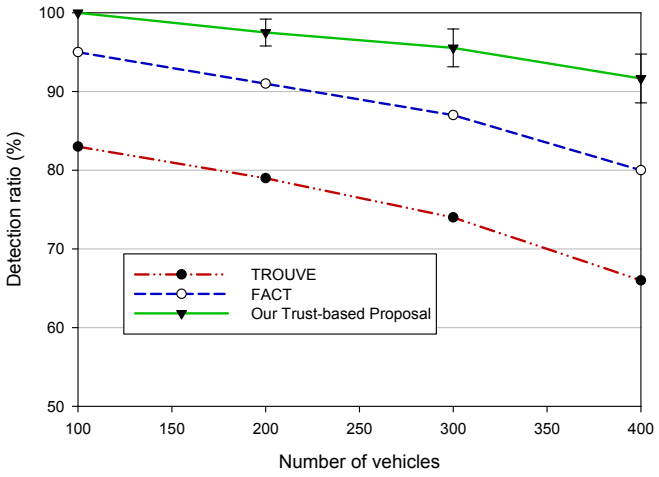


Figure 4.47: Detection performances compared to TROUVE and FACT proposals for different vehicle densities (Φ=25%).

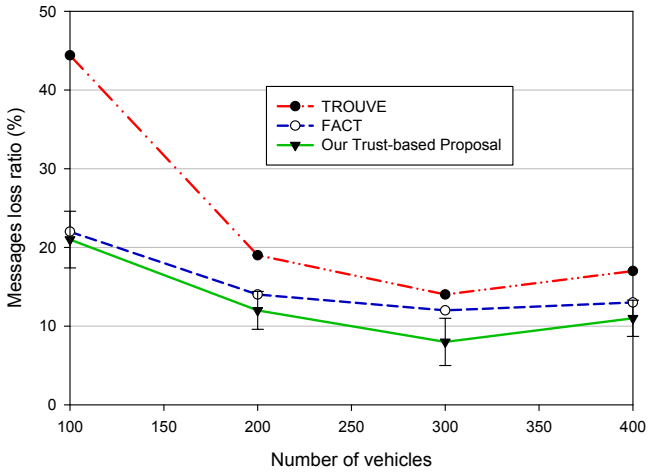


Figure 4.48: Message loss ratio when compared to TROUVE and FACT proposals for different vehicle densities (Φ=25%).

message loss ratios for our proposal when compared to the *TROUVE* [KLCL15] trusted routing protocol. In the latter solution there is a risk of selecting a vehicle acting as blackhole as the next forwarder, and also of losing messages because of any obstacle or temporal communication failures. Our proposal is also compared against *FACT* [RNT+15], a trust-based dissemination protocol which implements a time-based rebroadcasting strategy.

Figure 4.47 shows the detection effectiveness of our proposal when varying the vehicle density. We find that it outperforms both *TROUVE* and *FACT* solutions, showing an average efficiency that is 8% greater than these two proposals thanks to the continuous neighborhood evaluation technique that is adopted. Moreover, Figure 4.48 shows that, after a pre-specified waiting time (see equation 4.18), and compared to the *TROUVE* protocol, our proposed broadcasting strategy is able to reduce the message loss ratio by more than 20% in the sparse case, and by about 6% in the dense case. Compared to *FACT*, our proposal shows nearly the same behaviour, with 2% to 3% less messages lost.

4.5 Summary

In this chapter we described our two main proposals for establishing trust in vehicular networks, together with an opportunistic dissemination scheme for alert messages. Both TFDD and T-VNets are based on a modular architecture respecting all trust features by accounting for the evaluation of direct interactions and also by considering recommendations. Both proposals deal mainly with attacks seeking the availability service such as DoS, jamming, and blackhole attacks. However, similarly to other existing solutions, neither TFDD nor T-VNets can face intelligent attacks. Since trust is based on the historical evaluation of interactions, an attacker can alternate between legal and malicious behaviour to skip the deployed detection mechanisms. In the next chapter we detailed how, by introducing a risk estimation metric, we were able to strengthen the trust detection performance, and enable the detection of attackers deploying both standard and intelligent attacks.

Chapter 5

Enhancing VANET trust to address detection avoidance strategies

5.1 Overview

In this chapter we focus mainly on the problem where vehicles can become effective at achieving network disruption by alternating between legal behavior and malicious attack periods (*"anti-trust management"* strategies). Figure 5.1 illustrates this time-varying behaviour, which is similar to the On-Off attack in wireless sensors networks (WSN) [PLH06], and is also known as betrayal attack in VANETs [RH05]. While trust management is generally based on an evaluation of historical interactions, detecting these short-term attacks is a complex task. In addition, the *bad mouthing attack* [CZLF12], which can be also seen as an anti-trust management strategy, occurs when no precautions are taken against selfish vehicles generating only bad reports about other vehicles.

When hovering upon the existing solutions in the literature, it becomes clear that the adversarial models adopted assume a consistent dishonest behaviour throughout time. In addition, none of the existing works has studied the case of specific attacks against trust models themselves.

In addition, the assumption of many works about creating a global knowledge of the network [GGS04, RPGH08, LLLS13, KC14] can be effective in MANETs or similar environments that are less dynamic than VANETs. Moreover, relying on RSU deployment for trust establishment [KLCL15, SS15, LLLS13] can also become a handicap since (i) they are not always present, and (ii) the trust relationship is mostly related to direct peer-to-peer interactions rather than peer-to-authority interactions.

Furthermore, many trust-based security solutions for VANETs [MP12, HRGD13, Yan13, SA14, KLCL15] focus on improving the unicast and routing data exchange. However, critical VANET applications such as safety and service discovery are

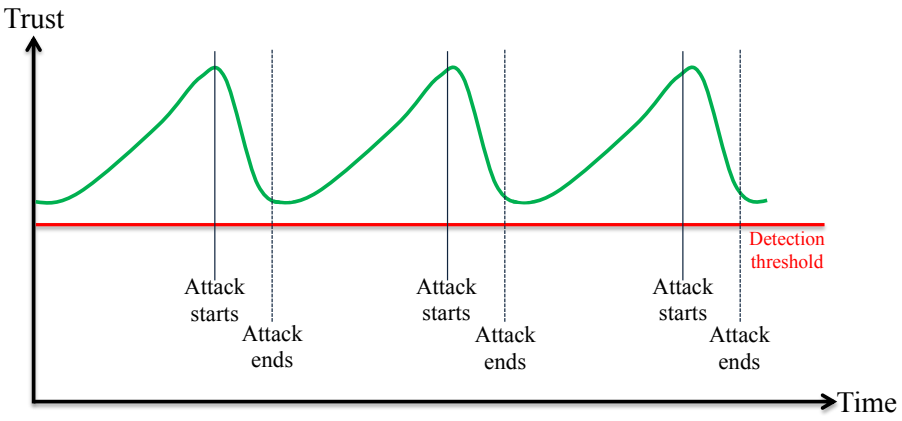


Figure 5.1: Intelligent dishonest behavior.

based on broadcast and multi-hop communication instead.

Below we detail our trust establishment technique for collaborative multi-hop communications called *RITA*. We enhance the trust computation by relying on risk estimation to deal with *"anti-trust management"* attacks. Hence, our proposal can deal with both regular and intelligent attacks against classical trust-based solutions.

5.2 RITA Overview

The overall architecture of our proposal, called RIsk-aware Trust-based Architecture for collaborative multi-hop vehicular communications (*RITA*), is illustrated in Figure 5.2. *RITA* can be divided into different modules responsible for: (a) computing inter-vehicular trust, (b) estimating risk, and (c) selecting the most adequate next forwarder/broadcaster vehicles for multi-hop messages. In addition, a database that stores the different recommendations and trust variations is used to enhance trust and risk computation.

The architecture of *RITA* takes advantage of the information carried by beacon, safety, and data messages to evaluate interactions among vehicles, which can be either direct or indirect interactions. Based on these interactions among nodes, the direct and indirect trusts are first computed and then combined to form an inter-vehicular trust evaluation (a). Simultaneously, the risk of a probably launched intelligent attack -i.e., periods with normal behaviour combined with periods with dishonest behaviour- is estimated using the variation of the local knowledge-based and recommendations-based evaluation of the messages' sources

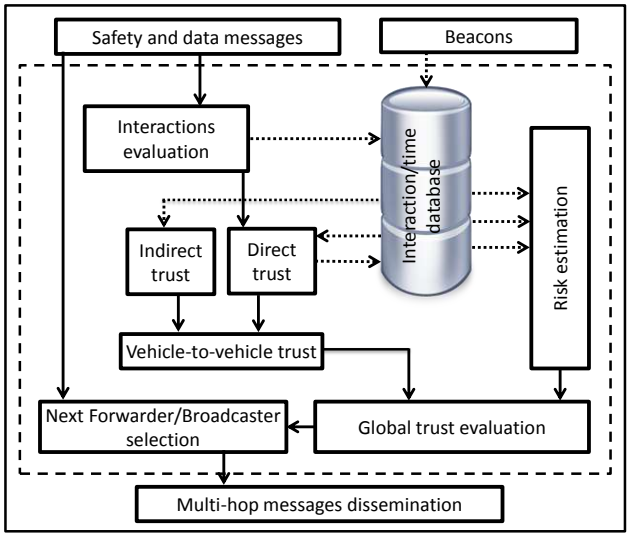


Figure 5.2: Proposed risk-aware modular trust establishment architecture ensuring reliable message dissemination.

(b). A trade-off between the inter-vehicular trust and the risk estimation is then computed. This final value called 'Global trust evaluation' can help in detecting both classical and intelligent attacks. Moreover, we use the trust evaluation in next forwarder/broadcaster selection procedure (c). Hence, the per-hop broadcasters are selected among the most trusted vehicles ensuring short delays and high delivery ratios.

Furthermore, it is clear that, for direct interactions, all messages (even those initially encrypted) can be decrypted and analyzed by the end destination. Hence, a decision about whether the interaction is legal (L) or malicious (M) can be made using an interaction evaluation module.

Instead of updating trust values after each interaction, we propose defining small time intervals and evaluating nodes' trust on each time interval to allow quickly detecting any change in the behavior pattern. Notice that adopting long observation periods is prone to include outdated information, which has a negative impact on the trust information accuracy. Thus, we propose considering only those interactions among vehicles taking place in the most recent period T. In addition, we proposed to divide this period (T) into n time slots of the same duration, updating the trust among vehicles for every time slot t_x, where '$1 \leq x \leq n$ '. On each new time slot we discard the oldest slot assessments - similarly to a 'First In First Out (FIFO)' mechanism -, thus creating a sliding window [CHDV03]. The actual size of this window and its time slots will be based on different experimental values that will be discussed in section 5.5. Hence, if a node behaves legally for a long time and then starts an attack, the behaviour observed during the last slot

t_x weights more than the behaviour observed in previous slots, in addition to the trust variation during these previous slots. The global trust evaluation denoted as GT, assigned by a vehicle i to another vehicle j, combines both inter-vehicular trust $Trust(i,j)$ and the risk estimation $Risk(i,j)$, as defined in equation 5.1.

$$GT(i,j) = \alpha \cdot Trust(i,j) + (1-\alpha) \cdot (1 - Risk(i,j)) \tag{5.1}$$

In this equation α is a tuning factor used to adjust the trade-off between the inter-vehicles trust computation and the risk estimation when computing the global trust value. Notice that, since the risk estimation presents a greater error margin compared to trust estimations, it is better to choose $\alpha \geq 0.5$ to give more weight to the latter parameter; the global trust evaluation will be anyway enhanced due to the introduction of the risk estimation factor. In section 5.5 we assign different values to the α parameter in order to choose the most adequate value for our experiments. However, it is worth mentioning that this value should be adapted to the different situations and traffic scenarios to maximize performance. The details about how the inter-vehicular trust and risk are computed is provided in the following section.

5.3 RITA details: Trust and risk estimation

In this section we provide formal details about both trust and risk estimation. Section 5.3.1 clarifies how vehicles can compute a trust evaluation about each other based on both local knowledge-based and recommendation-based information. Then, section 5.3.2 is dedicated to risk computation based on behaviour changing estimations, the honesty of broadcasted recommendations, and the reported events validity.

5.3.1 Vehicle-to-vehicle trust computation

When focusing on inter-vehicular trust we generally distinguish between two metrics: direct trust and indirect trust. Direct trust can be defined as the local knowledge-based evaluation of the direct interactions among vehicles, while indirect trust is the evaluation of the direct interactions between two vehicles based on the opinions of other vehicles about the honesty of the two participant vehicles. Since direct trust is more relevant than indirect (recommendation-based) trust when the number of interactions ($\#int$) increases, our vehicle-to-vehicle trust levels are adapted using the following relevance factor: $\frac{1}{\#int+1}$; this way, if we have more interactions, we assign more weight to direct trust than to indirect trust, and vice versa. Equation 5.2 describes how trust among vehicles is computed:

$$Trust(i,j) = \left[\left(1 - \frac{1}{\#int+1}\right) \cdot DT(i,j)\right] + \left[\frac{1}{\#int+1} \cdot IT(i,j)\right] \tag{5.2}$$

$DT(i,j)$ and $IT(i,j)$ refer to the direct and indirect trust evaluation, respectively, calculated by a vehicle i concerning another vehicle j. The computation details of $DT(i,j)$ and $IT(i,j)$ are provided in the following sections.

5.3.1.1 Direct trust computation

Before computing the direct trust evaluation, we denote by $H^{t_x}_{(i,j)}$ the honesty report generated by vehicle i about vehicle j using the number of legal (L) and malicious (M) interactions during a period of time t_x, where $1 \leq x \leq n$. $H^{t_x}_{(i,j)}$ is computed following equation 5.3:

$$H^{t_x}_{(i,j)} = \frac{L^{t_x}_{(i,j)}}{M^{t_x}_{(i,j)} + L^{t_x}_{(i,j)}} \cdot \left[1 - \frac{1}{L^{t_x}_{(i,j)} + 1}\right] \tag{5.3}$$

where $L^{t_x}_{(i,j)}$ and $M^{t_x}_{(i,j)}$ represent the number of legal and malicious interactions, respectively, between i and j from the perspective of node i. $\frac{L^{t_x}_{(i,j)}}{M^{t_x}_{(i,j)}+L^{t_x}_{(i,j)}}$ represents the percentage of legal interactions compared to the total number of interactions, and $1 - \frac{1}{L^{t_x}_{(i,j)}+1}$ is a factor that approaches 1 as the number of legal interactions increases. Hence, many legal interactions are required for a vehicle to increase its honesty index.

The direct trust computation uses the different honesty values along a period of time T by giving more importance to the last short period 't_n'. This behaviour allows $RITA$ to quickly detect misbehavior in neighboring vehicles. Equation 5.4 shows how the direct trust is updated:

$$DT(i,j) = \frac{\beta \cdot \left[\frac{\sum_{x=1}^{n-1} H^{t_x}_{(i,j)}}{n-1}\right] + H^{t_n}_{(i,j)}}{\beta + 1} \tag{5.4}$$

Factor β, whose value ranges between 0 and 1, is a reduction factor used to give more weight to the recent behavior of vehicles, while also taking into account their past behavior. In addition, this process is executed only for periods of time where there is at least one interaction between i and j; otherwise, the value of $DT(i,j)$ will remain unchanged.

5.3.1.2 Indirect trust computation

Indirect trust is calculated based on recommendations coming from one-hop neighbors about other vehicles. Most of the existing solutions suggest creating a new message type called *recommendation*, and they choose either a cluster-based technique or an aggregation method to reduce the additional overhead involved. To avoid affecting the communications bandwidth, we propose modifying the format of the periodically exchanged beacon messages by adding only two fields: (i) the neighbor identity, encoded in 1 byte, and (ii) the opinion of the beacon sender about that neighbor, also encoded in 1 byte. For example: if a node i considers that a vehicle j is untrusted, it will put the vehicle j's identity within the next beacon along with an opinion which can be < 0.5 (untrusted node) or ≥ 0.5 (trusted node). This opinion correspond to the global trust evaluation of the recommender about the recommended node $GT(i,j)$. This procedure is repeated until the entire neighbor list is included. Figure 5.3 illustrates the new beacon format.

Figure 5.3: Proposed beacon format extension.

Upon receiving neighbor beacons, a vehicle i computes, for every neighbor j, an indirect trust value $IT_{(i,j)}^{t_x}$ in a period of time t_x by combining the positive and negative opinions coming from other neighbors throughout that time period.

To avoid the negative influence of dishonest vehicles' opinions, a vehicle i computes the trade-off between the different recommenders' trust and their opinions. Hence, the higher is the level of trust on a neighbor, the more is its opinion taken into account. Equation 5.5 shows how the indirect trust is computed by a vehicle i about another vehicle j during a period t_x.

$$IT_{(i,j)}^{t_x} = \Big[\prod_{N}\Big(DT(i,k)\cdot Opinion(k,j)\Big)^{\frac{1}{2}}\Big]^{\frac{1}{N}} \; during\ t_x, \forall k \in \{trusted\ direct\ neighbors\ of\ i\} \tag{5.5}$$

In this equation N refers to the number of recommenders, $IT_{(i,j)}^{t_x}$ is a combination of the recommenders' (k) direct trust DT and their opinions about the vehicle j during a period t_x. In addition, we consider a neighbor vehicle as a trusted vehicle if its global trust $GT_{(i,j)}$ is higher than a predefined threshold; this threshold can be adapted depending on the security requirements and the traffic type.

Similarly to direct trust, we assign a higher weight to the latest recommendations without forgetting the overall recommendations received. This is achieved through equation 5.6:

$$IT(i,j) = \frac{\beta \cdot \Big[\frac{\sum_{x=1}^{n-1} IT_{(i,j)}^{t_x}}{n-1}\Big] + IT_{(i,j)}^{t_n}}{\beta + 1} \tag{5.6}$$

Notice that β is the same factor used in equation 5.4. It is clear that, if node i does not have any direct neighbor, or if it has only malicious neighbors, the indirect trust (IT) will remain unchanged.

5.3.2 Risk estimation

Trust establishment in highly dynamic networks suffers mainly from instant behavior changes since trust is based on the accumulative historical interactions. Thus, it is hard to quickly detect changing behaviors, especially if the attackers are aware of the shortcomings associated to trust-aware mechanisms, and make an effort to achieve high reputation values prior to launching their attack. In this context, risk estimation can be an effective solution to solve the aforementioned problem. Our *RITA* approach allows every vehicle i to estimate a risk value for a neighboring vehicle j by combining three different factors: (i) direct trust variability (DTV) along consecutive time slots in order to detect the betrayal behavior; (ii) event-related reports (ER) represented by the ratio of fake event reports to the total number of events reports in order to punish nodes sending reports about non-existent events; and finally (iii) evaluations of recommendations (RC) to detect bad mouthing attacks, which also relies on the ratio of negative recommendations to the total number of recommendations. Equation 5.7 clarifies how the risk among vehicles is estimated:

$$Risk(i,j) = \frac{DTV(i,j)^2 + ER(i,j)^2 + RC(i,j)^2}{DTV(i,j) + ER(i,j) + RC(i,j)} \tag{5.7}$$

In this equation $DTV_{(i,j)}$ represents the maximum negative variation in direct trust given by a vehicle i to another vehicle j along different time slots, and it is calculated as follows (equation 5.8):

$$DTV(i,j) = \mid Min(DT_{(i,j)}^{t_x} - DT_{(i,j)}^{t_{x+1}}) \mid \forall x \in \{1, ..., n-1\} \tag{5.8}$$

A negative variation means that $DT_{(i,j)}^{t_{x+1}}$ is lower than $DT_{(i,j)}^{t_x}$. Hence, $DT_{(i,j)}^{t_x} - DT_{(i,j)}^{t_{x+1}}$ is a negative value and, as a consequence, the maximum direct trust variation is the absolute value of $Min(DT_{(i,j)}^{t_x} - DT_{(i,j)}^{t_{x+1}})$ for the different time slots t_x.

$ER_{(i,j)}$ is the event-related honesty, and it represents the rate of non-existent events reported by j to the total number of events reported by that same node in a period of time t. Since j is a direct neighbor of i, we assume that i can verify, after a short period, if vehicle j has broadcasted a real or a fake event report. Equation 5.10 shows how $ER(i,j)$ is computed based on the different periods evaluated (equation 5.9):

$$ER_{(i,j)}^{t_x} = \Big[\frac{\sum j's\ \#fake\ events}{\sum j's\ \#events}\Big]^{t_x} \tag{5.9}$$

$$ER(i,j) = \frac{\beta \cdot \Big[\frac{\sum_{x=1}^{n-1} ER_{(i,j)}^{t_x}}{n-1}\Big] + ER_{(i,j)}^{t_n}}{\beta + 1} \tag{5.10}$$

Finally, $RC_{(i,j)}$ is the evaluation of i about the recommendations (RC) that j has broadcasted within its beacons. If the number of negative recommendations is excessive (e.g., more than 50% of the generated recommendations), this event

will be considered as an attempt to perform a bad mouthing attack. $RC_{(i,j)}$ will be equal to the number of negative recommendations (< 0.5) divided by the total number of recommendations. Equation 5.11 summarizes the recommendations evaluation:

$$RC(i,j) = \frac{\sum j's\ \#negative\ rc}{\sum j's\ \#rc} = \frac{Card\{Opinion(j,k) < 0.5\}}{Card\{Opinion(j,k)\}} \forall k \tag{5.11}$$

In addition, to improve the risk evaluation procedure, we associate to each parameter (DTV, ER, RC) in equation 5.7 a factor representing the influence of every report compared to the two other parameters. For example, if a node launches a betrayal attack, its DTV will be much higher than ER and RC, and, therefore, the DTV report should have more weight than the other reports. To this end, in equation 5.7, DTV is multiplied by $\frac{DTV}{DTV+ER+RC}$, ER by $\frac{ER}{DTV+ER+RC}$, and RC by $\frac{RC}{DTV+ER+RC}$.

5.4 Multi-hop information dissemination using RITA

Multi-hop dissemination is used mainly for alerting vehicles and authorities on the road about a safety event. However, multi-hop dissemination is also used for data message propagation.

Using the global trust evaluation, any vehicle i can judge any neighbor j and, hence, accept or reject interactions with this neighbor. As mentioned above, a trust threshold can be chosen according to the system security requirements or context-based information; for instance, in safety cases this threshold should be low since it is a critical case. Thus, a decision about a vehicle 'j' can be made following equation 5.12:

$$\begin{cases} j\ is\ a\ trusted\ neighbor & If\ GT(i,j) \geq TrustThreshold \\ j\ is\ an\ untrusted\ neighbor & Otherwise \end{cases} \tag{5.12}$$

Since most VANET applications, such as Internet access, electronic payment, service discovery, and parking place booking, rely on Road Side Units (RSU) for communications [OW09], the aim of multi-hop data message dissemination in these intelligent transportation systems services (ITS-s) is to reach the closest RSU in a reduced period of time. Thus, we distinguish between two dissemination types: (i) safety messages dissemination, and (ii) data messages dissemination, in order to ensure a fast delivery of safety messages, and a high efficiency with low packet loss in infotainment scenarios.

5.4.1 Multi-hop dissemination of safety messages

Same as beacons, we propose to extend safety messages with an additional field containing a pre-selected next broadcaster of the safety message, this way we avoid broadcast storms, as well as network resource exhaustion (see figure 5.4).

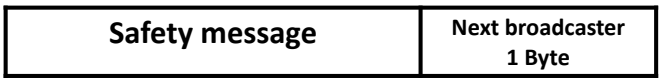


Figure 5.4: Safety message extension.

The next broadcaster in every hop is selected in a way so that it is the farthest trusted neighbor, thereby maximizing the additional coverage area [LHL+07, VBT10]. For every neighbor j the vehicle i associate a score $Score(i,j)$ representing a balance between the global trust $GT(i,j)$ and the distance $Distance(i,j)$ between i and j as shown in equation 5.13

$$Score(i,j) = \frac{GT(i,j)}{Distance(i,j)} \tag{5.13}$$

Equation 5.14 shows the selection procedure of a next broadcaster j among the neighbors of a vehicle i:

$$NextB = j \ / \ Score(i,j) = Max\{Score(i,j),\ \forall\ j \in Neighbors\ of\ i\} \tag{5.14}$$

Where {k, ..., N} are the current neighbor identities for vehicle i.

Once the re-broadcasting is done, vehicles receiving the same safety message can again drop it and remove the saved version of this safety message as well. Moreover, in the case of a broadcasting failure including both link-related and threat-related reasons, one of the informed vehicles should take the broadcasting decision. In addition, the neighbors of a vehicle 'i' are not necessarily neighbors of each other. Hence, even if the next broadcaster selected (green car with rectangle in figure 5.5) broadcasts the safety message, we can still have some neighbors that remain uninformed about this action. The latter should rebroadcast safety messages to cover other non-informed zones once its waiting time has expired without receiving another copy of the safety message. To this end, upon receiving a safety message, every neighbor j sets a timer according to the distance to the safety message's source i and accounting for the communication range.

Equation 5.15 describes how this waiting time can be computed:

$$WaitingTime = DistanceT(i,j) + TT + PT + PRT \tag{5.15}$$

In this equation $DistanceT(i,j)$ refers to the distance-based waiting time, such as in [BL02, BK06, DJ07], and it is used in such a way that the farthest neighbor

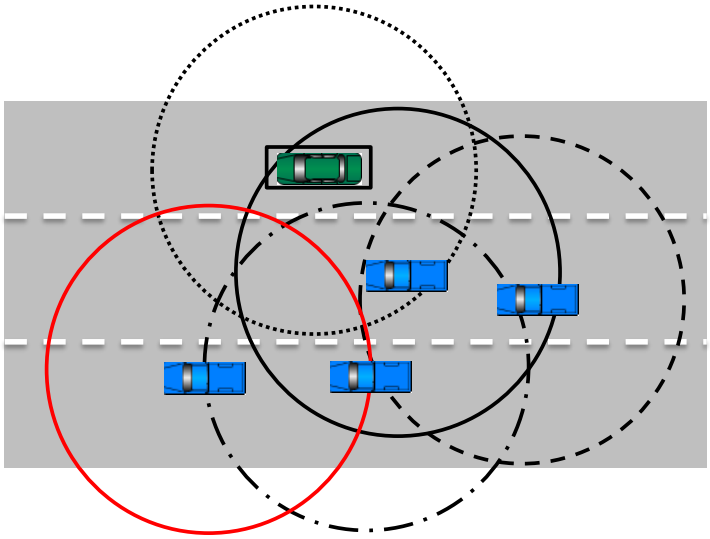


Figure 5.5: Per-vehicle dissemination areas.

will have the shortest waiting time. TT, PT, and PRT correspond to the maximum Transmission, Propagation, and message PRocessing Times, respectively.

Algorithm 13 summarizes the safety messages' multi-hop dissemination procedure. When vehicle i receives a safety message sent by another vehicle j, it checks the global trust $GT(i,j)$. If it is lower than a predefined threshold, the safety message will be dropped because j is considered to be an untrusted vehicle. Otherwise, the broadcasting process should continue since 'j' is considered to be a trusted neighbor.

Afterward, if i finds its identity piggybacked within the safety message, this means that it is the one selected as next-hop broadcaster. In addition, if the piggybacked identity is not even part of i's neighbors list, it verifies the safety event validity, selects the next broadcaster, and rebroadcasts the safety message. However, if the safety event's validity expires, the latter will be logically canceled. Otherwise, if i is not the selected vehicle for rebroadcasting the safety message, and if its waiting time has expired without receiving another copy of the safety message, it selects a new next broadcaster to broadcast the safety message.

Algorithm 13 Safety messages multi-hop dissemination using RITA

```
1: Upon receiving a safety message by i sent by j;
2: if (GT(i,j) ≥ TrustThreshold) then
3:     if ('i' is the next broadcaster OR next broadcaster ∉ neighbors list of 'i') then
4:         if NotExpired(safety message, relevance distance, validity duration) then
5:             NextB ← Select next broadcaster (Equation 5.14);
6:             Broadcast(safety message, NextB);
7:         else
8:             Cancel (safety message);
9:         end if
10:    else
11:        WaitingTime ← Compute waiting time (Equation 5.15);
12:        if Expired(WaitingTime) AND NotReceived(safety message, NextB) then
13:            NextB ← Select next broadcaster (Equation 5.14);
14:            Broadcast(safety message, NextB);
15:        end if
16:    end if
17: else
18:    Drop(safety message);
19: end if
20: End
```

5.4.2 Multi-hop dissemination of data messages

Disseminating data messages among vehicles is a procedure adopted by many VANET applications like delivering ads, restaurant menus, and short-term offers

to passing-by vehicles. However, to have a sure and permanent broadcasting of this information, the use of road side units is mandatory. Hence, to preserve the communications bandwidth, vehicle-to-vehicle broadcasting is used only to reach the RSU.

RITA assumes that vehicles are equipped with a Global Positioning System (GPS), so they can locate vehicles and RSUs within the network. Similarly to safety messages, we assume that we have an additional field containing the selected next forwarder identity as illustrated in figure 3, but with data messages instead of safety messages.

Unlike the safety messages (see equation 5.14) where the main concern is the delay, the next forwarder for data messages (NextF) is selected using the link duration estimation and distance in addition to the trust between peers in order to minimize both propagation delay and packet loss ratios. For every neighbor j the vehicle i associates a score $Score(i,j)$ representing a balance between the trust $GT(i,j)$, the link duration $LinkD(i,j)$, the distance $Distance(i,j)$ separating i and j, and the distance separating j from the closest RSU $Distance(j,RSU)$ as shown in equation 5.16

$$Score(i,j) = \frac{GT(i,j) + LinkD(i,j) + Distance(i,j)}{Distance(j,RSU)} \tag{5.16}$$

Equation 5.17 represents the next forwarder selection based on the different neighbors' scores:

$$NextF = j \ / \ Score(i,j) = Max\{Score(i,j),\ \forall\ j \in Neighbors\ of\ i\} \tag{5.17}$$

where {k, ..., N} is the set of neighbors for vehicle i. RSU is the closest roadside unit in the neighborhood which can be easily found using the GPS.

The sum of the global trust given by i to j, the distance between i and j, and the link duration between i and j, is divided by the distance between the neighbor j and the closest RSU, in order to get the closest, trusted and stable path to the RSU, as shown in equation 5.17.

$LinkD(i,k)$ is the link duration estimation between vehicle i and its neighbor k, and it is computed according to equation 5.18.

$$LinkD(i,j) = \begin{cases} \frac{R+Distance(i,j)}{|V(i)-V(k)|} & If\ V(i) \geq V(k) \\ \frac{R-Distance(i,j)}{|V(i)-V(k)|} & Else \end{cases} \tag{5.18}$$

In this equation R refers to the communication ratio, and $V(i)$ is the speed of vehicle i. Algorithm 14 summarizes the data messages forwarding process.

When a node i receives a data message forwarded by another node, it first checks whether it was selected as the next forwarder for that message. If so, it continues the forwarding process. Otherwise, the processing that follows depends on the application type, thus being outside the scope of this paper. Afterward, if the data message sender had a higher trust than the predefined threshold, the current node tries to reach the RSU if it is within communication range. Otherwise, it selects the next forwarder and then it forwards again the data message. Obviously, the message will be dropped if i considers j to be untrusted.

Algorithm 14 Data messages multi-hop dissemination using RITA

```
Upon receiving a data message from j by i;
if (i is the next forwarder) then
    if (GT(i, j) ≥ TrustThreshold) then
        if ∃ RSU ∈ neighbors of i then
            Forward(msg) to RSU;
        else
            NextF ← Select next forwarder (Equation 5.17);
            Forward(msg, NextF);
        end if
    else
        Drop(msg);
    end if
end if
End
```

5.5 Performance evaluation

To evaluate our *RITA* architecture we relied on the NS-2 simulator [IH11] modified to consider the IEEE 802.11p standard. The generated vehicular traffic is based on the Citymob mobility model [MCCM08], which uses SUMO [BBEK11] to create mobility traces based on real maps extracted from OpenStreetMap using the Krauss Mobility model [KHRW02]. In our case we used a map from the downtown area of Laghouat, Algeria (see figure 5.6).

Table 5.1 summarizes the main simulation parameters:

Table 5.1: RITA simulation parameters.

Parameters	Value
Simulation area (km×km)	2×2
Simulation time (s)	300
Transmission range (m)	300
Permissible lane speed (km/h)	[0,80]
Number of vehicles	{100, 200, 300, 400}
Dishonest vehicles presence (%)	{15, 25, 35, 45}
TrustThreshold	0.5
W (s)	100
P (s)	2
β	0.7

We divide our experiments into three parts: first, we address the optimal selection of our time window and its time slots, as well as the trade-off between trust and risk information. Second, we compare the performance of our proposal against

Figure 5.6: Simulated scenario of Laghouat city, Algeria.

two other existing proposals - T-CLAIDS [KC14] and the AECFV [SS15] - in different scenarios. While the AECFV proposal is dealing mainly with blackholes, the authors of T-CLAIDS did not detail their adversarial model, only assuming the attacker to have a stable continuous malicious behaviour. Finally, in the third part we discuss our proposed messages dissemination technique effectiveness taking end-to-end delay and packet loss ratio as the target metrics.

In our scenario, we assume that beacons are exchanged every half a second, while an event (i.e. safety message) occurs every 10 seconds.

5.5.1 Determining the optimal parameter settings

In this section we will determine the optimal values for the α factor representing the trade-off between the inter-vehicular trust and the risk estimation, allowing to defend against both standard and intelligent attacks. In addition, we discuss the choices for the W and P which refers respectively to the window size and the slots duration parameters. Initially, we assume that factor $\alpha = 0.6$, and that 25% of the vehicles within the network are dishonest and behave as blackholes.

Figure 5.7 represents the dishonest nodes detection ration with respect to the number of interactions (safety and data messages + the recommendations piggybacked to the received beacons), we note that the detection ratio increases until we reach approximately 100 interactions when it then offers almost a stable values. Therefore, our solution can converge to its optimal detection ratios after approximately 100 interactions.

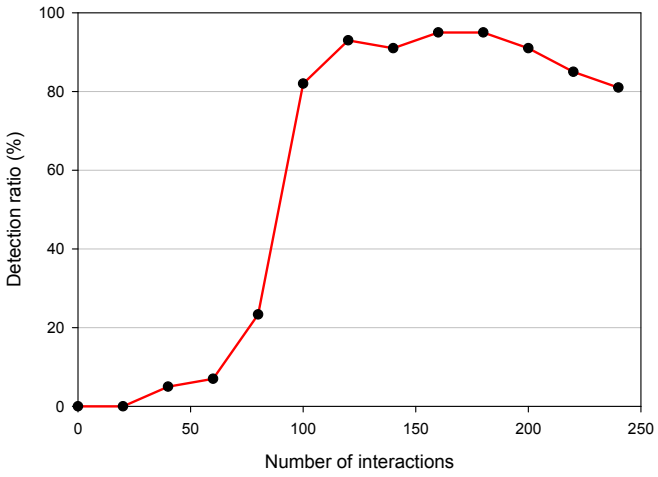


Figure 5.7: Required number of interaction for an efficient trust establishment.

In addition, while varying the number of vehicles within the network, figure 5.8 shows that the average number of direct neighbors is also an important factor in the detection process, and that it is logically related to the amount of inter-vehicle interactions shown in figure 5.7. Furthermore, figure 5.8 also shows that the average number of direct neighbors should not be below 2, otherwise, our proposal would not perform as good as expected.

As result, the size of W and P can be selected dynamically based of the number of interactions if we assume that all vehicles can chose different standards, with different beaconing frequency, or based on a combined value (number of direct neighbors, synchronization delay). Hence, we will have an interactions-based or a neighbors-based selection of values for W and P.

Moreover, many other factors can be taken into account such as: vehicle density, the simulated map (urban or freeway), as well as the communication range. Thus, artificial intelligence solutions such as neural networks can be used to estimate the best values of W and P dynamically.

For the experiments that follow, we pick the best settings, resulting in $W = 100s$ and $P = 20s$. These values are achieved for a beacon frequency equal to 2 Hz (i.e, 2 beacons per second), and considering that a data message is sent by every vehicle each $10s$.

As discussed is section 5.3, factor α represents the trade-off between the inter-vehicular trust and the risk estimation, and so it can take different values to achieve different trade-offs. Figure 5.9 represents the detection ratios while varying α parameter. The resulting histograms for different values of α refers to the detection performances of RITA againt the intelligent attack, the bad mouting attack, and the blackholes attack. It becomes clear from the histograms that the best trade-off in terms of detection of the three suggested attacks - betrayal, bad mouthing and

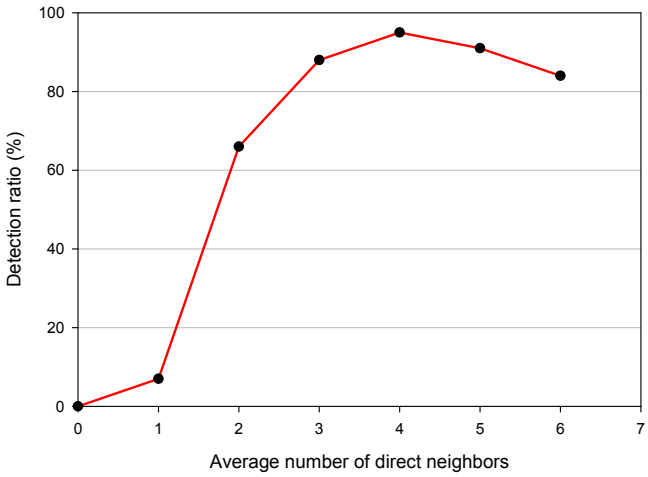


Figure 5.8: Required number of neighbors for an efficient trust establishment.

blackholes - is achieved for $\alpha = 0.6$.

Furthermore, our system alternates between $\alpha = 0.6$ (combined trust and risk) if one of the risk estimation parameters is higher than a predefined threshold TH and $\alpha = 1$ (trust without risk) if there is no behaviour changing by an intelligent attacker (the risk estimation parameters are lower than a predefined threshold TH) as described in equation 5.19:

$$\alpha = \begin{cases} 0.6 & If\ (DTV\ Or\ ER\ Or\ RC) \geq\ TH \\ 1 & Otherwise \end{cases} \tag{5.19}$$

Same as $TrustThreshold$ of equation 5.12, the TH threshold can be chosen according to the system security requirements. Hence, for both event related (ER) and direct trust variation (DTV), this threshold should be low (e.g, 0.3) since it is refers to a safety critical case or a detection skip tentative. Higher values of TH can be acceptable for the case of false recommendations (RC) since we give more importance to the direct trust evaluation than the indirect one.

5.5.2 RITA attackers detection performance

In this section we show $RITA$'s dishonest vehicles detection performances in the case of intelligent attackers that behave according to figure 5.1. Afterward, under a continuous dishonest behaviour, we compare our $RITA$ proposal against two existing proposals: T-CLAIDS and AECFV.

Figure 5.10 represents the detection ratios of $RITA$ with respect to the number of nodes. It shows that, when varying the number of vehicles in the network, our proposal can offer good detection ratios mostly exceeding the 90%. In fact, even for extremely high ratios of attackers (45%), the detection ratio remains above

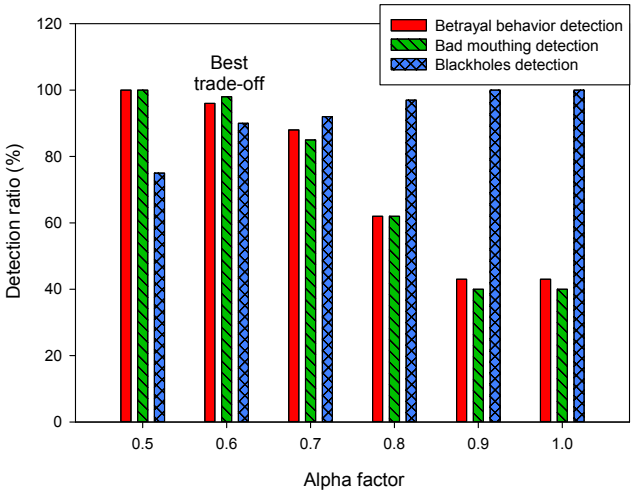


Figure 5.9: α factor selection.

82%. The performance levels for more realistic attacker ratios ($\leq$ 15%) are nearly 100%, despite all of them perform intelligent attacks thanks to the risk estimation that allows to *RITA* detecting such behaviour.

In addition, we compared our solution against other proposals such as AECFV and T-CLAIDS. It should be noted that the latter are only able to detect blackhole attacks, being unable to deal with attackers endowed with trust establishment awareness, and able to launch intelligent attacks, which raises the detection complexity. Thus, we have simplified the adversarial model to blackhole attacks alone, meaning that attackers will merely send negative recommendations about its direct neighbors. Figure 5.11 represents the detection ratios for different densities of vehicles. It shows that our proposal clearly outperforms T-CLAIDS and AECFV by more than 4% for a density higher that 300 vehicles. Here, since non of the risk estimation parameter have a high value exceeding the threshold TH discussed in the previous section, the α parameter is equal to 1. Hence, the risk estimation margin of error is avoided.

Figure 5.12 represents the detection ratios for different attacker ratios when the number of vehicles is set to 400. Similarly to figure 5.11, figure 5.12 shows that, when varying the ratio of dishonest vehicles in the scenario, *RITA* is able to perform better than both AECFV and T-CLAIDS, ensuring high detection ratios (>90%) even if almost half (45%) of the vehicles are dishonest.

5.5.3 RITA messages delivery performance

We now study the effectiveness of the proposed dissemination technique in the presence of dishonest vehicles in the network. Since the message delivery process attempts to reach an RSU in the shortest possible time, we also assess the impact

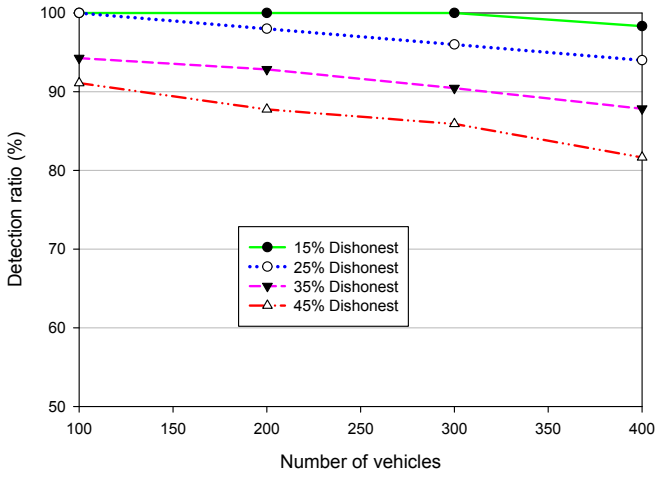


Figure 5.10: *RITA* detection performance for different vehicular densities in the presence of intelligent attackers.

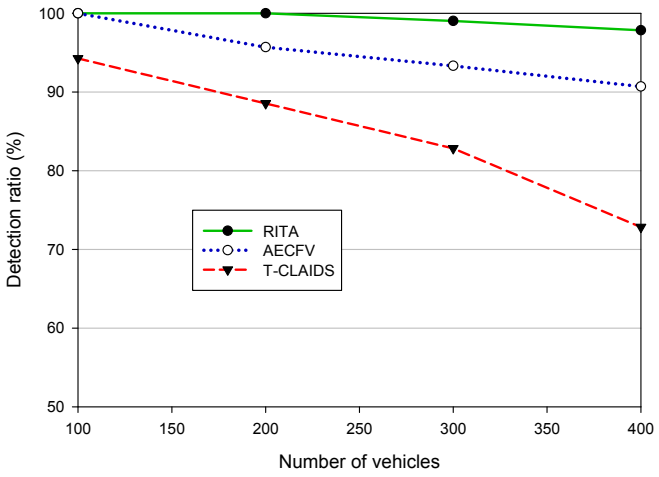


Figure 5.11: Detection performances compared to AECFV and T-CLAIDS for different densities (35% dishonest vehicles).

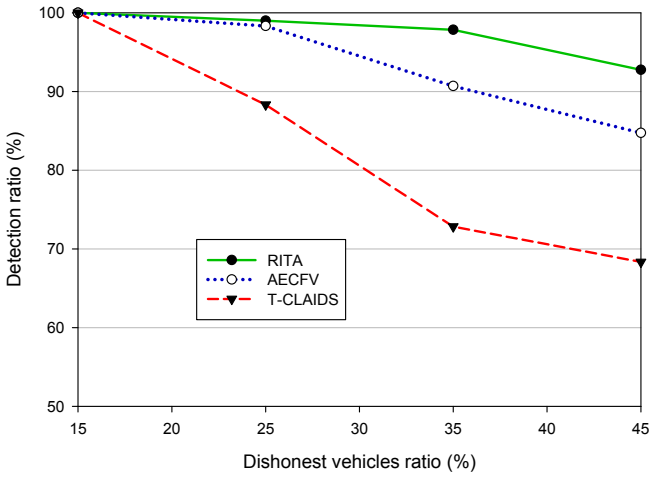


Figure 5.12: Detection performances compared to AECFV and T-CLAIDS for different dishonest vehicles ratios (400 vehicles scenario).

of varying the RSUs density among: (a) 3 RSUs, (b) 6 RSUs, (c) 9 RSUs, and (d) 12 RSUs as illustrated in figure 5.13.

Figure 5.14 represents the average end-to-end delay required for packets to reach an RSU when varying the number of vehicles and RSUs in the network. The resulting histogram shows that, except for the case of low vehicle and RSU densities (less than 200 vehicles and less than 6 RSUs), our proposed technique is able to provide low delays to the message delivery process ($\leq$ 1 *second*) despite the high attackers ratio (35%). For lower attacker ratios, results are even better.

Concerning the packet loss ratio, figure 5.15 shows that -similarly to the average end-to-end delay- and thanks to the best forwarder/broadcaster selection, our solution can overcome the high ratio of attackers (35%) and ensure low packet loss ratios, especially under high levels of connectivity (number of vehicles higher than 200) and the presence of a significant number of RSUs (6 or more), and can reach quasi optimal values (less than 3%) for a dense network of both vehicles and RSUs (respectively more than 300 vehicle and 12 RSU).

5.6 Summary

In this chapter we addressed the detection avoidance problem introduced by smart attackers, and proposed a slotted trust evaluation technique to detect such attempts. By endowing our proposal with risk assessment capabilities, *RITA* also becomes able to face additional attacks like badmouthing and fake event alerts.

In the next chapter, we detail our idea of giving a new social dimension to vehicular networks that differs from the classical vehicular social networks paradigm. Through this new dimension we introduce the human honesty factor to strengthen

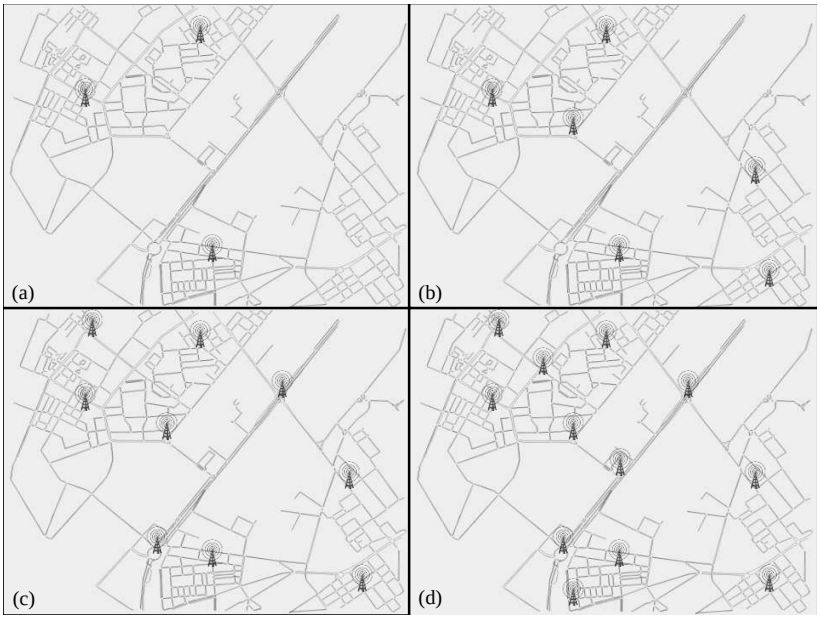


Figure 5.13: RSUs distribution in the simulated scenario of Laghouat city, Algeria.

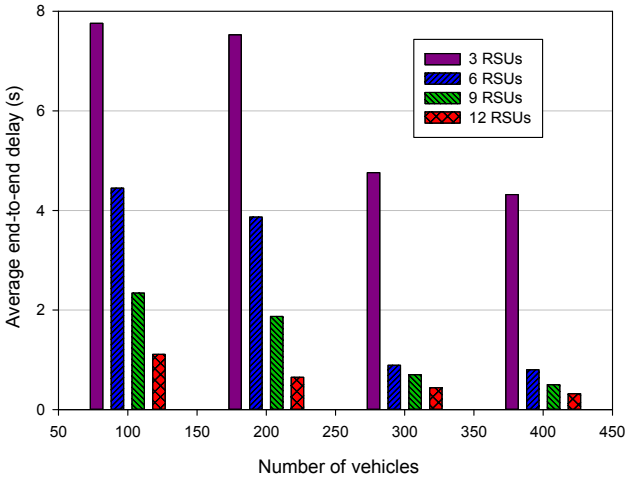


Figure 5.14: Average end-to-end delay required to reach an RSU for different vehicle and RSU densities (35% of dishonest vehicles).

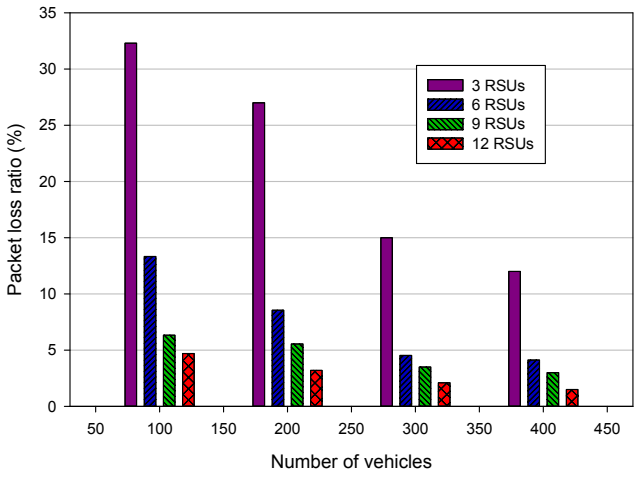


Figure 5.15: Packets loss ratio for different vehicle and RSU densities (35% of dishonest vehicles).

VANET security, as well as novel safety systems using online social networks.

Chapter 6

Future Trust models for VANET: Design and discussion

6.1 Overview

Security in vehicular networks involves four main elements, which are: vehicles, roadside units, third trusted parties, and also the drivers. However, as we mentioned in chapter 3, the fourth element represented by humans has not been well investigated, neither taken into account by security and safety researchers, despite the fact that human factor can be seen as the most relevant factor affecting VANET operation. At the same time, social networks are getting increasing interest, and starting to have an impact on the different research areas.

Trusted authorities can match the vehicles' real identities with the used pseudonyms, and they are also the only ones allowed to trace/track driver identities, matching them with the vehicles' identities. Thus, we start by first explaining our three-level evaluation proposal that takes into account the trusted authorities global view. Then, we present how our proposal can be extended to consider drivers' honesty using online social networks. Finally, we discuss how estimated driver honesty can be used to enhance existing trust models.

6.2 Hierarchical Adaptive Trust Establishment Solution for Vehicular Networks

In general, inter-vehicular trust results from combining evaluations resulting from direct interactions with recommendations coming from other peers. Hereafter, we describe the proposed data design which piggybacks recommendations to data messages instead of overloading the network with an additional type of message. Afterward, we clarify how the inter-vehicular trust is computed.

6.2.1 Data design

To ensure an adequate and efficient message evaluation process, we have added two fields to each message header that contain: (i) the identity of the last forwarder 'id', and (ii) the 'opin', which is the last forwarder opinion concerning the message's source, as illustrated in Figure 6.1.

Since we only include the last forwarder's identity and its opinion within the message header, we do not cause privacy problems as the forwarder identity would not be transmitted beyond one-hop neighbors.

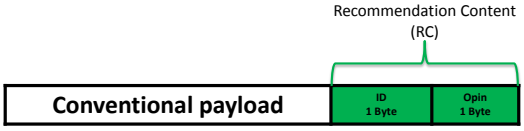


Figure 6.1: Piggybacking of recommendation contents.

6.2.2 Inter-vehicular trust computation

To establish trust among vehicles, every vehicle i computes, for every neighbor j, an honesty weight $Tr(i,j)$. The latter is a combination of local evaluation (direct trust $DT(i,j)$), recommendations from other vehicles ($RCV(i,j)$), and recommendations from both roadside units ($RCR(RSU,j)$) and trusted authorities ($RCT(TA,j)$). However, the use of these recommendations is dependent on the presence of RSUs within the vehicles' communication range, and the feasibility of meeting delay requirements. Hence, for critical cases requiring fast decisions to be taken, waiting for recommendations coming from roadside units (RSUs) and trusted authorities (TAs) is not the best solution.

As described in equation 6.1, we differentiate three cases: (i) there is no RSU, and the exchanged information is delay-sensitive, (ii) there is an RSU, and the exchanged information is partially delay-tolerant, and (iii) there is an RSU, and the exchanged information is delay-tolerant. In this work, we use the IEEE 802.11e classification where data traffic is divided into four QoS-based (Quality of Service) categories, classified from the lowest to the highest priority as follows: background traffic (BK), best effort traffic (BE), video traffic (VI), and voice traffic (VO). Moreover, a specific band is reserved for safety out of the four access categories.

In our case, we consider voice and video traffic as a single category called 'Real-time' (see Figure 6.2). Hence, (i) delay sensitive information encompasses both safety and real-time, (ii) partially-delay-tolerant information is mapped to the best effort category, and (iii) delay-tolerant information are those coming with background priority.

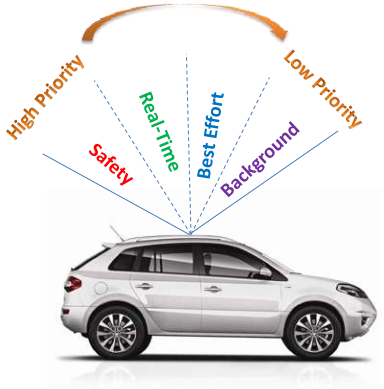


Figure 6.2: Traffic priorities defined in the WAVE standard (also known as Access Categories).

$$Tr(i,j) = \begin{cases} \left[DT(i,j) \cdot RCV(i,j)\right]^{\frac{1}{2}} & If\ No\ RSU\ Or\ Delay\ sensitive\ packet \\ \left[DT(i,j) \cdot RCR(RSU,j)\right]^{\frac{1}{2}} & If\ there\ is\ an\ RSU\ And\ Partially\ Delay\ tolerant\ packet \\ RCT(TA,j) & If\ there\ is\ an\ RSU\ And\ Delay\ tolerant\ packet \end{cases} \tag{6.1}$$

For the first case, the on-the-go trust evaluation will be the combination of the direct trust evaluation and the recommendations coming from other direct neighbors. Furthermore, when an a RSU is present, its recommendation will be considered as well in the on-the-go trust evaluation;

finally, when there are no delay limits in the presence of an RSU, our trust evaluation relies on the trusted authority's recommendation representing the global knowledge about all participant vehicles. Figure 6.3 represents an overview of our hierarchical adaptive trust establishment solution.

Thus, whenever an intermediate node 'i' receives a packet, the forwarding decision is either forwarding or dropping the packet based on the computed trust evaluation as follows:

$$\begin{cases} Forward_{Packet}(ID = Next, Opin = Tr(i,j)) & If\ Tr(i,j) \geq DangerTh \\ Drop_{Packet} & Otherwise \end{cases} \tag{6.2}$$

In the following sections we will explain how the direct trust ($DT(i,j)$), the vehicles recommendations ($RCV(i,j)$), the RSUs recommendations ($RCR(RSU,j)$) and the TA recommendations ($RCT(TA,j)$) are computed.

6.2.2.1 Direct trust computation

The Direct trust evaluation of vehicle j computed by i ($DT(i,j)$) is the ratio of the legal actions $\#L(i,j)$ compared to the total number of both legal $\#L(i,j)$ and malicious $\#M(i,j)$ actions. Equation 6.3 describes the $DT(i,j)$ calculation:

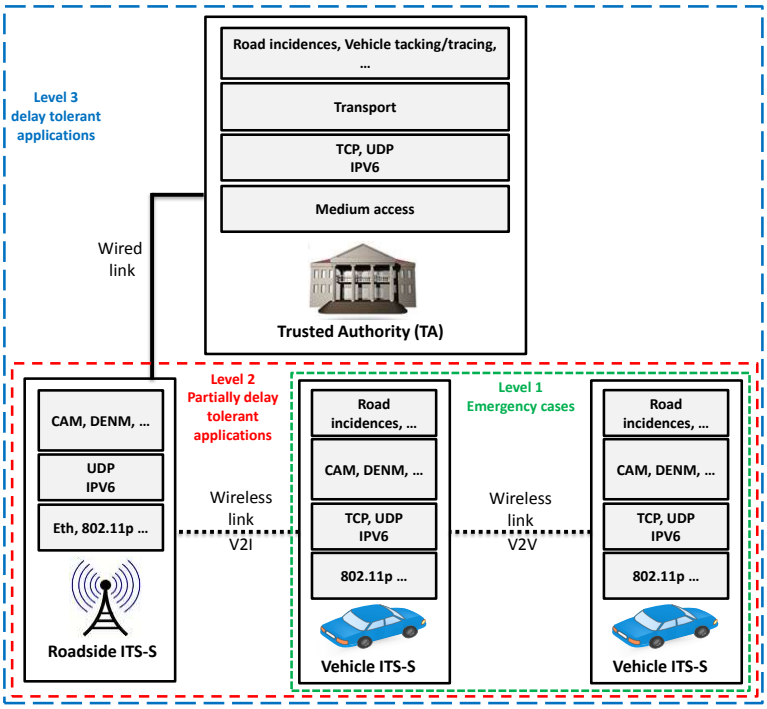


Figure 6.3: Proposed architecture.

$$DT(i,j) = \frac{\#L(i,j)}{\#M(i,j) + \#L(i,j)} \cdot \Big[1 - \frac{1}{L(i,j)+1}\Big] \tag{6.3}$$

where $1 - \frac{1}{L(i,j)+1}$ is a factor that approaches 1 as the number of legal actions increases. Hence, many legal actions are required for a vehicle to increase its direct trust.

6.2.2.2 Vehicles recommendations combination

As explained above, recommendations among vehicles are piggybacked within the exchanged messages. To give more weight to recommendations coming from highly trusted vehicles, every vehicle i combines the received opinion (recommendation) from a vehicles k about another vehicle j ($RCV_k(i,j)$) with the trust associated to this recommender k following equation 6.4:

$$RCV_k(i,j) = \big[DT(i,k) \cdot Opin(k,j)\big]^{\frac{1}{2}} \tag{6.4}$$

Then, the different vehicles' recommendation about vehicle j are combined together to find the global vehicles' recommendation value for that vehicle $RCV(i,j)$ following equation 6.5:

$$RCV(i,j) = \big[\prod_n RCV_k(i,j)\big]^{\frac{1}{n}} \tag{6.5}$$

6.2.2.3 Roadside unit recommendation computation

On every interaction with a roadside unit, vehicles send their neighbor trust evaluation list. This information allows roadside units to have a quasi global view about vehicle behaviour within their respective region.

Equation 6.6 shows how an RSU computes its recommendation towards a vehicle j using the other vehicles' trust evaluation:

$$RCR(RSU,j) = \big[\prod_n Tr(i,j)\big]^{\frac{1}{n}} \tag{6.6}$$

where n is the number of vehicles i having a trust value regarding vehicle j.

In addition to the RSU computed recommendation, the received reports can also be used to detect and blacklist attackers within the network. Figure 6.4 shows an example of the bad mouthing attack detection using the received vehicles' reports. This attack occurs when an attacker considers all vehicles as dishonest for selfish purposes.

For instance, equation 6.7 generates a black list containing the identities of the vehicles launching a bad mouthing attack.

$$RSUBlacklist \leftarrow \forall j,$$

$$\frac{Card(Tr \rightarrow ID = j \;\&\; Tr \rightarrow value \leq 0.5)}{Card(RC \rightarrow ID = j)} \geq DetectTH \tag{6.7}$$

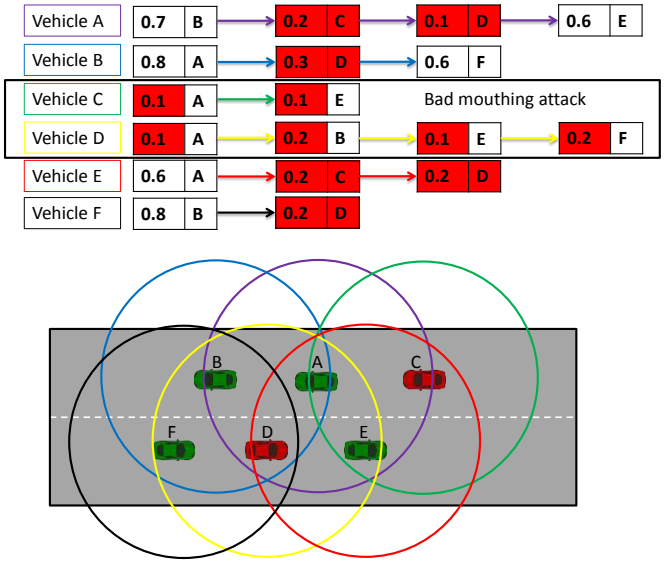


Figure 6.4: Example of dishonest nodes detection.

In this equation $DetectTH$ is the detection threshold, which is compared to the ratio between the number of vehicles considering vehicle j as dishonest and the total number of reporting vehicles.

6.2.2.4 Trusted authority recommendation computation

Assuming that trusted authorities are always in contact with RSUs through a wired connection, they can easily compute a global evaluation $RCT(TA, j)$ for all vehicles j within the network. However, such a global view generation may take longer than the inter-vehicles or the RSU-to-vehicles evaluation. Hence, the trusted authority evaluation is used only for delay-tolerant cases, and it is taken as is without the combination of any other evaluation since it logically involves all the previously computed evaluations.

Equation 6.8 represents the calculation of the trusted authority recommendations. Similarly to RSU recommendations, a trusted authority uses the different RSU evaluations $RCR(RSU, j)$ about a vehicle j to compute a final global evaluation $RCT(TA, j)$:

$$RCT(TA, j) = [\prod_{n} RCR(RSU, j)]^{\frac{1}{n}} \tag{6.8}$$

where n is the number of reporting RSUs having previously evaluated the behaviour of vehicle j.

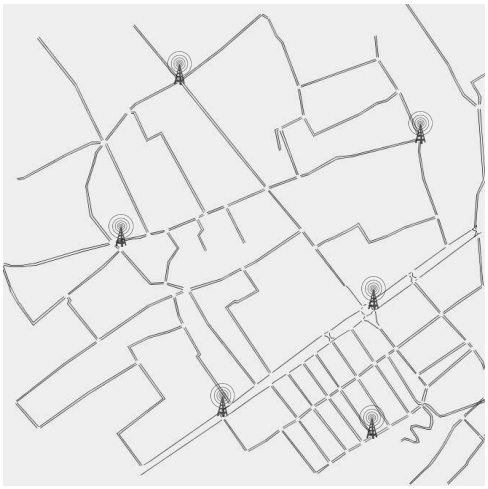


Figure 6.5: Simulated scenario of Laghouat city, Algeria.

6.2.3 Simulation results

To evaluate our proposal we relied on the NS-2 simulator [IH11] modified to support the IEEE 802.11p standard, and using the RAV propagation model [MFC+10]. The generated vehicular traffic is based on the Citymob mobility model [MCCM08], which uses SUMO [BBEK11] to create mobility traces based on real maps extracted from OpenStreetMap using the Krauss Mobility model [KHRW02]. In our case we used 6 roadside units distributed throughout a map from the downtown area of Laghouat, Algeria, as presented in figure 6.5.

Table I summarizes the main simulation parameters:

Table 6.1: Simulation settings.

Parameters	***Value***
Simulation area (km×km)	1×1
Simulation time (s)	300
Maximum transmission range (m)	250
Permissible lane speed (km/h)	[0,80]
Number of vehicles	[80, 200]
Dishonest vehicles presence (%)	{15, 25}

To assess the impact of the proposed trust establishment solution, we will measure our proposal's performance when facing two different ratios of dishonest nodes: Φ=15% and Φ=25%. Vehicles send random traffic packets (delay-sensitive, partially delay-tolerant, and delay-tolerant) every 10 seconds to randomly chosen destinations. Moreover, beacons are broadcasted with a frequency of 2 Hz.

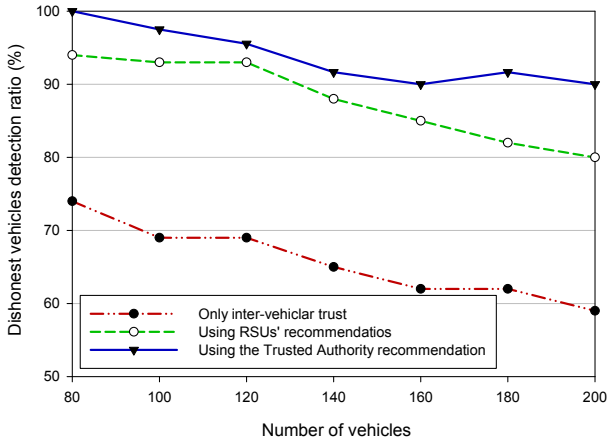


Figure 6.6: Detection performance for variants of the proposed scheme when varying vehicular densities (25% of dishonest vehicles).

Figure 6.6 represents the detection performances for the different versions of our proposal in the presence of 25% of the vehicles acting maliciously. Instead, figure 6.7 shows the detection performances of our whole proposal for dishonest node ratios of $\Phi = 15\%$ and $\Phi = 25\%$ with respect to the total number of vehicles. In our case, an attacker is detected whenever its trust decreases below the predefined trust threshold, which we fixed at 0.5 in these tests. We notice from figure 6.6 that, thanks to the hierarchical trust establishment, the detection performance exceeds 80% when relying on an RSU, and it is quasi optimal when using the trusted authority. However, these performances logically decrease when using only inter-vehicular trust. In addition, figure 6.7 shows that our whole proposal is able to sustain performance levels even for high attacker ratios.

Figure 6.8 shows how the wrong decision ratios vary with vehicular density in the presence of 25% of the nodes acting maliciously for the different versions of our proposal. The resulting curves clarify that, even in the presence of a high ratio of attackers (25%) and a high density of vehicles (200 vehicles), more than 90% of the relay decisions where correct for the protocol versions relying on either RSU or TA recommendations, while 10% less efficiency is achieved for the case of inter-vehicular trust; this is expected since the latter case lacks the global view achieved by the former two. However, Figure 6.9 shows that the required end-to-end delay is clearly reduced when using only inter-vehicular trust compared to the protocol versions using either RSU or TA recommendations. This way, we are able to support emergency scenarios with about 80% of correct decisions in the worst case. We also noticed that most of the wrong decisions occurred at the beginning of experiments, before inter-vehicular trust was updated.

Finally, when 200 vehicles are present within the network, figures 6.10 and 6.11 represent the trust variation for both sets of honest and dishonest vehicles with respect to the ratio of dishonest ones. Figure 6.11 shows that the attackers' trust is always less than the initially allowed trust value (0.5), which means that false

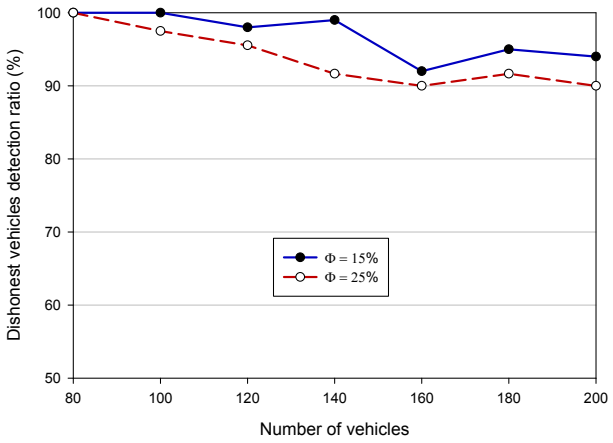


Figure 6.7: Detection performances when varying vehicular density for 15% and 25% of dishonest vehicles.

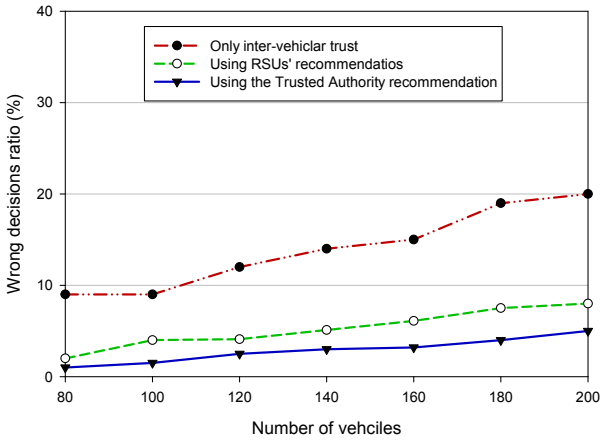


Figure 6.8: Wrong decisions ratio of our proposal for different densities when 25% of the vehicles are dishonest.

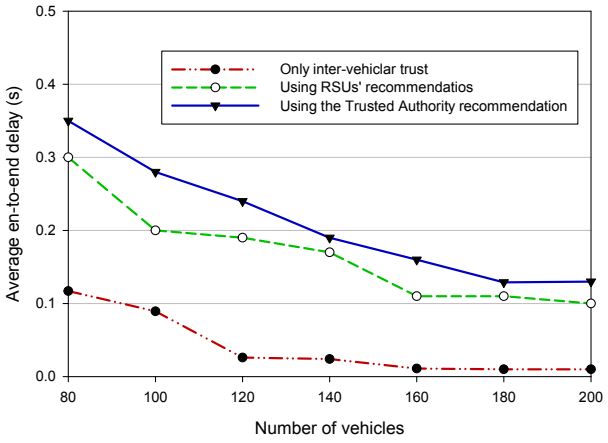


Figure 6.9: Average end-to-end delay for our proposal under different vehicular densities when 25% of the vehicles are dishonest.

negatives are nearly 0% for our solution. It also shows that the trust for honest vehicles can decrease below 0.5 in some cases, showing a reduced number of false positives (See figure 6.10). This occurs because, in some cases, our solution does not differentiate between malicious packet drops and network-related packet drops. Thus, such wrong judgments are prone to decrease their trust.

For now, we presented a hierarchical trust establishment solution able to adapt to the Quality of Service requirements of different VANET applications. In the next section, we explain our idea of adding a social dimension to our proposal, and we also show the possibilities offered by cellular networks and 4G Internet to provide direct TA-to-vehicle communications even in the absence of roadside units, thereby enabling our proposal to operate in a broader range of environments.

6.3 Integrating the user honesty factor through Online Social Networks (OSNs)

In this section we present our view about how it is possible to enhance the safety and security of vehicular network systems by integrating human honesty indexes using data retrieved from online social networks. We start by first explaining social trust and socially-aware networks. Then, we describe how trust among peers is usually computed in OSNs. Finally, we describe our vision to extend trust by using OSNs.

6.3.1 Social trust and socially-aware networking

The proliferation of handheld devices requires mobile carriers to provide anytime and anywhere connectivity. The mobility patterns of mobile devices strongly depend on the users' movements, which are closely related to their social relationships

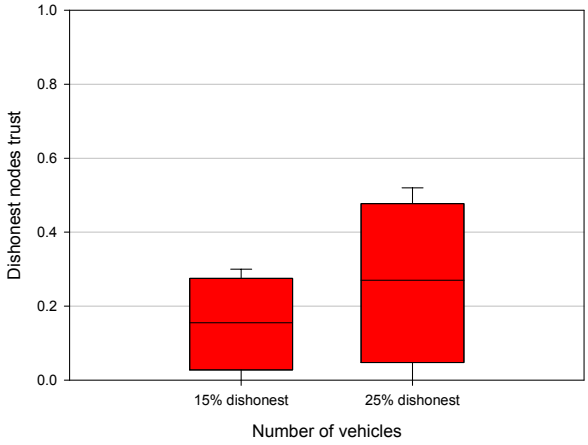


Figure 6.10: Dishonest vehicles trust variability throughout a 200-vehicle simulation (25% dishonest).

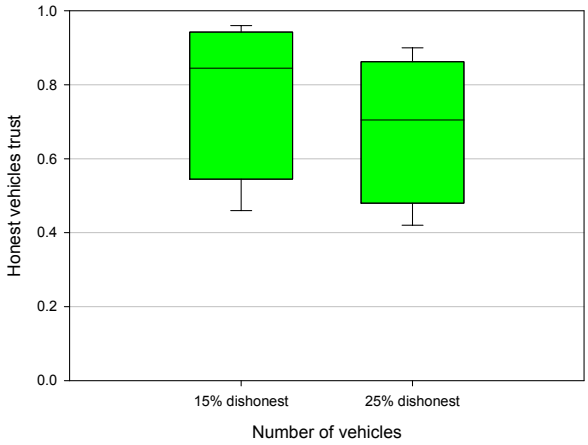


Figure 6.11: Honest vehicles trust variability throughout a 200-vehicle simulation (25% dishonest).

and behaviors. Consequently, today's mobile networks are becoming increasingly human centric. This leads to the emergence of a new field known as socially-aware networking (SAN)[XLL+15]. One of the major features of SAN is that social awareness becomes indispensable for the design of networking solutions. This emerging paradigm is applicable to various types of networks (e.g., opportunistic networks, mobile social networks, delay-tolerant networks, ad hoc networks, etc.) where the users have social relationships and interactions. By exploiting the social properties of nodes, SAN can provide better networking support to innovative applications and services. In addition, it facilitates the convergence of human society and cyberphysical systems.

Figure 6.12 represents a global overview of socially-aware networking concepts and its different layers. For our case we focus mainly on the red rectangle representing security and privacy protocols using online networks.

Notice that introducing online social networks in VANETs differs from the vehicular social networks approach where a set of vehicles located in the same geographical area, and typically going to the same destinations, can share some application, purposes, or services, thereby forming a temporal inter-vehicle social network.

6.3.2 Trust in Online Social Networks (OSNs)

As mentioned above, trust establishment has proved its efficiency at enhancing the security of different types of networks. Many proposals have been developed for OSNs as well [DGS11, KA13]. The general trust establishment proposals for OSNs are based either on the Advogato trust metric [LA98], or PageRank solutions [BP12].

Besides the graph-based logical structure of OSNs, figure 6.13 summarizes the application-oriented structure of trust establishment in Online social networks. In general, trust for OSNs can be categorized based on three complementary phases: (i) trust information collection, (ii) trust evaluation, and (iii) trust information dissemination. To identify how honest and trustful is a profile owner, social trust is based on a scalar estimation using the personal profile information, which includes user identity and interactions with other users. Once this social trust is estimated, it will be provided to the end users in different manners and for different purposes.

6.3.3 Trust computation in Vehicular Networks and Online Social Networks

Establishing trust in any network involves the inheritance of this network's features. Therefore, due to the distributed nature of vehicular networks, every vehicle locally evaluates its neighbors trustiness. This trust computation can be done either in a scalar way, using the piggybacked opinions within exchanged messages, or through clustered and group-based collaboration among vehicles located in a same area. Differently from this situation, trust in online social networks requires having a sink or a third trusted party that is responsible for evaluating the different peers. This sink can either handle the whole task of trust computation, or

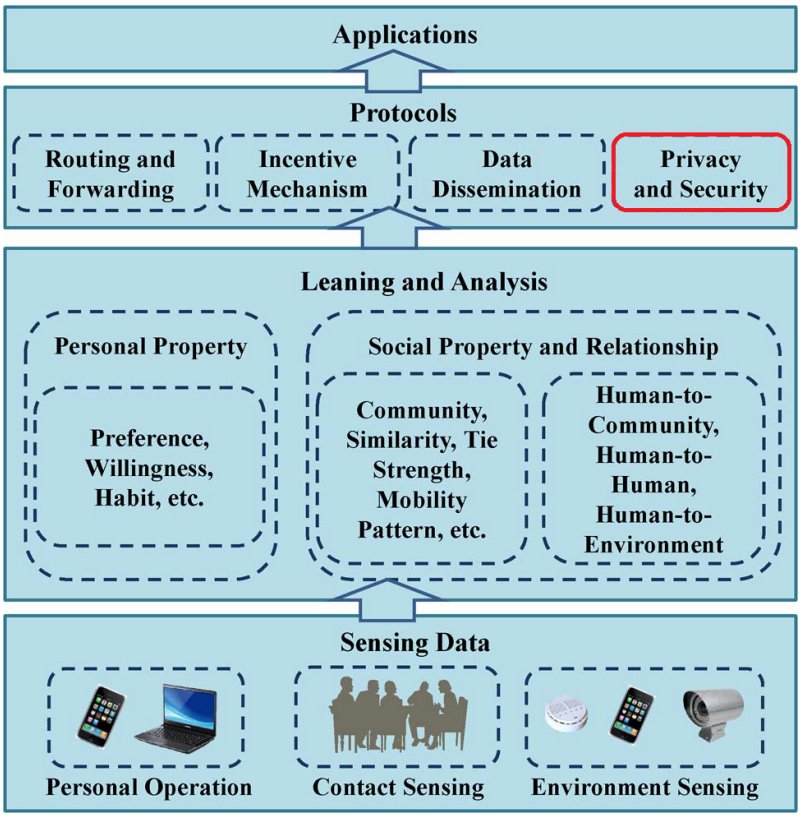


Figure 6.12: Socially-aware networking overview [XLL+15].

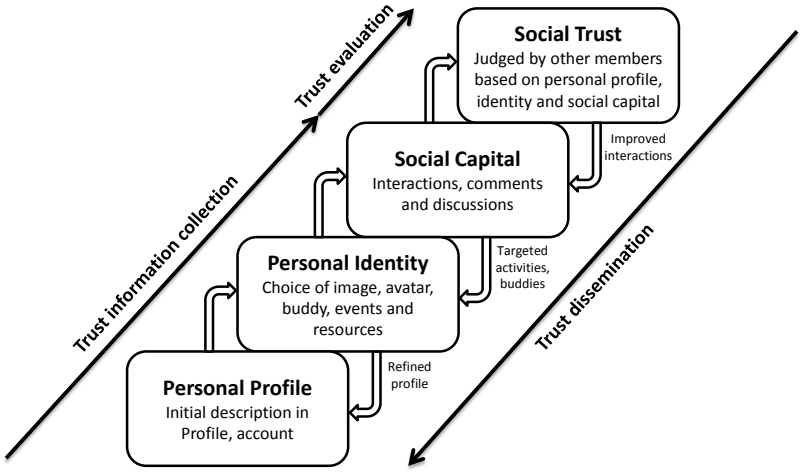


Figure 6.13: Trust establishment in OSNs.

it can distribute such task among secondary sinks, which are typically community leaders. Hence, by introducing the community context, trust computation is now based on a group instead of scalar information. Figure 6.14 summarizes the difference between VANET and OSN trust computations.

6.3.4 Socially-aware trust model overview

Incorporating the human honesty factor into VANET trust should be achieved by relying on third trusted authorities as intermediaries for this information, since the latter are the only ones having the possibility to trace/track vehicles identity together with their drivers. Accounting for the vehicles' identity is not a problem as every vehicle should have a valid certificate and a set of pseudonyms provided by the trusted authority. However, matching the driver identity and social account with the vehicle identity involves the use of other intermediate tools such as digital fingerprint, eyes and voice recognition systems, or a subscriber identification module (SIM), thus imposing more requirements onto the system.

Due to the high cost of smart vehicles, and to the probable lack of RSUs in rural environments, Android-based platforms including smartphones and tablets have recently emerged as an alternative solution to provide vehicular communications[1]. This way, any trusted third authority can be reached using different cellular network technologies. This new research area is know as Heterogeneous Vehicular Networking [ZZXW16].

Figure 6.15 represents an overview of our proposal, which is simply the extension of the three-level evaluation technique described in section 6.2 (see figure 6.3).

[1]The SmartCarPhone project, http://www.grc.upv.es/SmartCarPhone/

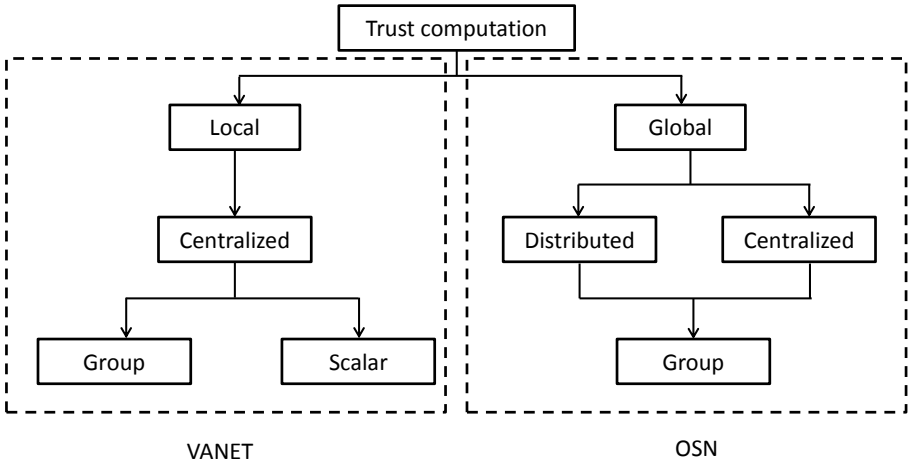


Figure 6.14: VANET trust vs OSN trust.

6.3.5 Trust computation

In addition to three-level evaluation described in section 6.2, vehicles can request the human honesty factor of some of their neighbors to the trusted authority.

Furthermore, if a vehicle has already demonstrated its honesty, and thereby benefits from an high trust value, there is no need to take the human honesty factor into account, and vice versa. Thus, nodes requiring the human honesty factor as complementary data should be only those nodes whose behaviour is fully clear, as show in figure 6.16.

Depending on the online social networks computed trust, the trusted authority matches, for each vehicle identity, an honesty factor called 'HHF', which refers to the Human Trust Factor of the current driver, a factor that varies within the range: $[-0.5, +0.5]$

Once the soliciting vehicles receive the HHF for neighbors they have concerns about, the trust computation function will be the following:

$$Tr(i,j) = \begin{cases} \left[DT(i,j) \cdot RCV(i,j)\right]^{\frac{1}{2}} & If\ No\ RSU\ Or\ Delay\ sensitive\ packet \\ \left[DT(i,j) \cdot RCR(RSU,j)\right]^{\frac{1}{2}} & If\ there\ is\ an\ RSU\ And\ Partially\ Delay\ tolerant\ packet \\ RCT(TA,j) & If\ there\ is\ an\ RSU\ And\ Delay\ tolerant\ packet \\ Tr(i,j) + HHF(j) & If\ j\ is\ a\ dubious\ node\ (for\ instance\ 0.4 \geq Tr(i,j) \geq 0.6) \end{cases} \tag{6.9}$$

In this equation, we test the trust evaluation $Tr(i,j)$ after every update to keep it within the range [0, 1].

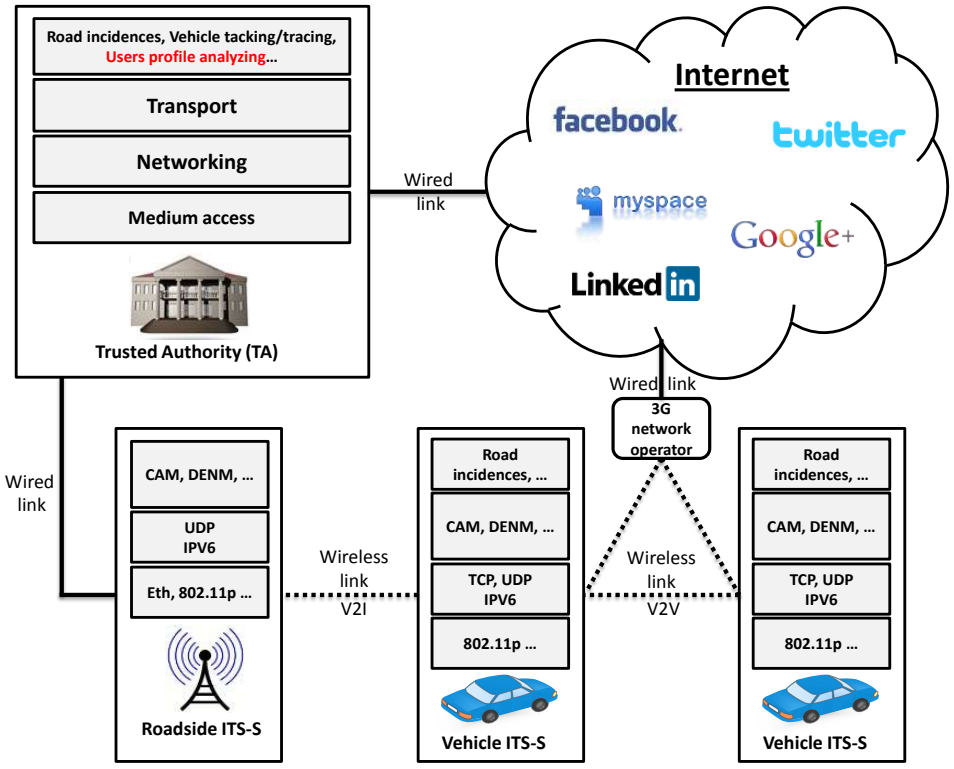


Figure 6.15: Proposal Overview.

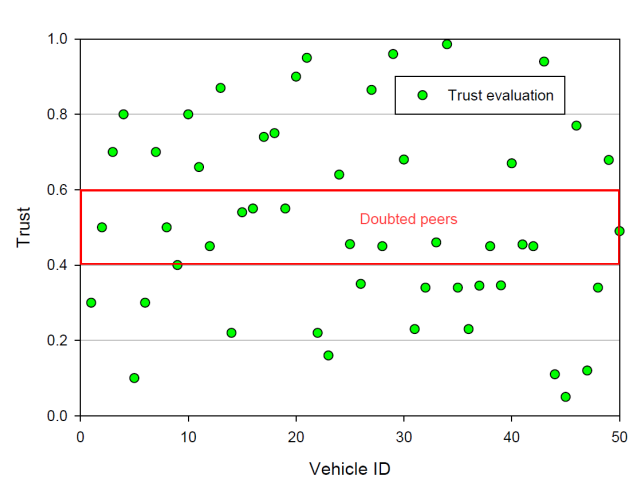


Figure 6.16: An example trust evaluation distribution for 50 nodes.

Using this strategy, the number of dubious nodes will be reduced as shown in figure 6.17. Thus, a decision about vehicles trustiness can be made.

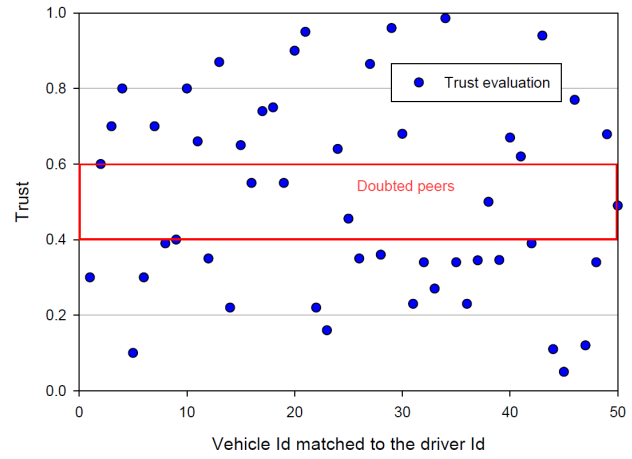


Figure 6.17: An example of trust evaluation distribution with 50 nodes.

6.4 summary

In this chapter we presented our view about trust-based next-generation safety and security systems for VANETs. First, we established a three-level hierarchical trust establishment solution. Second, we extended our proposal to consider the drivers' honesty through online social networks. This idea opens us various future

challenges related to the humans trust estimation, including users' posts, textual aggregation, sociological analysis, etc.

Chapter 7

Conclusions, Contributions and Future Works

The number of areas and problems to which vehicular communications are applied continuously, grow while known and unknown threats affect this kind of networks. Researchers are called to address the design of efficient protocols that are secure against possible attacks. This thesis allowed us to understand, classify, and the propose solutions to face the main inside threats. Together with the security issues and trust management solutions, we learnt through this thesis the different ITS applications, standards, and communication technologies.

Through our hovering upon the existing trust models in the literature, different shortcomings have appeared. First of all, we noticed that most of the existing solutions are entity-oriented models trying to filter out dishonest peers. Whereas, same as in information-centric networks [GSK+11], for VANET safety context, exchanged information trustiness is the most important factor. Another important point is the required detection time, we noticed also that even if most of the existing solutions are efficient in terms of detection accuracy, they suffer in terms of detection speed. Based on a developed intrusion detection module (IDM) and data centric verification, our first proposal called TFDD can insure both efficient and fast revocation of dishonest peers and malicious messages.

Furthermore, all the existing solutions including TFDD do not consider neither acknowledge the standardization efforts. However, to be used, deployed, and tested, all security solutions should be implementable over the existing standards. We noticed also that authors of the existing solution chose to test their proposal against autonomous attackers. Hence, testing these solutions against collaborative and synchronized attacks seems interesting. Our second proposal called T-VNets represents a novel trust establishment architecture that is fully compliant with the ETSI ITS standard. It takes advantage of the standardized periodically exchanged beacons (i.e CAM) and event triggered messages (i.e DENM) to continuously estimate the traffic and dishonest peers distribution in the network. In addition to the autonomous attackers, T-VNets can also face platooning and coalition scenarios of attacks.

While classifying the adopted adversaries, evaluation tools and metrics, we noticed also that all existing works use stable and continuous attacks scenarios. This means that the attacker do not stop the launched attack at any time instant. However, an attacker can alternate between legal and malicious behaviors to avoid being detected. Our third proposal called RITA handles the case of smart attackers adjusting their behaviors following the deployed security measurements.

Together with the above mentioned shortcomings, we also have the ignorance of the human-centric evaluation which is one of our future directions. In addition, we plan to use the key factor analysis [Jai90] to identify the most important metrics to consider and hence, harmonize the evaluation methods of VANET trust models.

Figure 7.1 summarizes the main shortcomings of the existing VANET trust models together with our contributions:

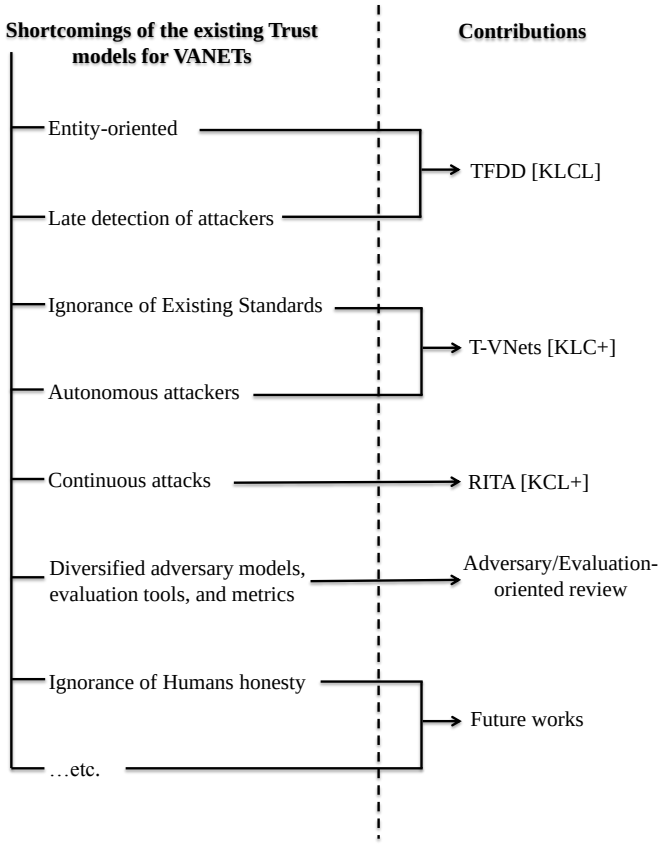


Figure 7.1: Main shortcomings of VANETs' Trust models.

In the rest of this chapter, we summarize the contributions of the research presented in this dissertation and suggest some future directions for our work.

7.1 Contributions Related to the Thesis

7.1.1 Journals

[KLC$^+$] Accepted (Online first 26 May 2016) "T-VNets: a novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS", in *Elsevier Computer Communications*

In this paper we proposed a novel trust establishment architecture that is fully compliant with the ETSI ITS standard, and that takes advantage of the periodically exchanged beacons (i.e CAM) and event triggered messages (i.e DENM). Our solution, called T-VNets, allows estimating the traffic density, the trust among entities, as well as the dishonest nodes distribution within the network. In addition, by combining different trust metrics such as direct, indirect, event-based and RSU-based trust, T-VNets is able to eliminate dishonest nodes from all network operations while selecting the best paths to deliver legal data messages by taking advantage of the *link duration* concept. Since our solution is able to adapt to environments with or without roadside units (RSUs), it can perform adequately both in urban and highway scenarios.

[KCL$^+$] Accepted (Online first 06 October 2016) "RITA: RIsk-aware Trust-based Architecture for collaborative multihop vehicular communications", in *Wiley security and communication Networks*

Trust establishment over vehicular networks can enhance the security against probable insider attackers. Regrettably, existing solutions assume that attackers have a dishonest behavior that remains stable over time. This assumption may be misleading, as the attacker can behave intelligently to avoid being detected. In this paper we proposed a novel solution that combines trust establishment and risk estimation concerning behaviour changes. Our proposal, called RITA, evaluates the trust among vehicles for independent time periods, while the risk estimation computes the behavior variation between smaller, consecutive time periods, in order to prevent risks like an intelligent attacker attempting to bypass the security measures deployed. In addition, our proposal works over a collaborative multi-hop broadcast communication technique for both Vehicle-To-Vehicle (V2V) and Vehicle-To-Roadside unit (V2R) messages in order to ensure an efficient dissemination of both safety and infotainment messages.

[KLCL] Accepted (Online first 16 December 2016) "TFDD: a Trust-based Framework for Reliable Data Delivery and DoS defense in VANETs", in *Elsevier Vehicular Communications*

In this paper we propose 'TFDD', a trust establishment scheme for enhancing inter-vehicular communication and preventing DoS attacks. Based on a developed intrusion detection module (IDM) and data centric verification,

our framework allows preventing DDoS attacks and eliminating misbehaving nodes in a distributed, collaborative and instantaneous manner. In addition, a trusted routing protocol is proposed that, using context-based information such as link stability and trust information, delivers data in the most reliable way.

[KCC+] Accepted (Online first 26 December 2016) "Trust management for Vehicular Networks: An Adversary-Oriented Overview", in *IEEE Access*

Cooperative Intelligent Transportation Systems (C-ITS), mainly represented by vehicular ad-hoc networks (VANETs), are among the key components contributing to the Smart City and Smart World paradigms. Based on the continuous exchange of periodic and event triggered messages, smart vehicles can enhance safety on roads, while also providing support for comfort applications. In addition to the different communication protocols, securing such communications and establishing certain trustiness among vehicles are the main challenges to address as the presence of dishonest peers can lead to unwanted situations. To this end, existing security solutions are typically divided into two main categories, cryptography and trust, where trust appeared as a complement to cryptography on some specific adversary models and environments where the latter was not enough to mitigate all possible attacks. In this paper we provide an adversary-oriented survey of the existing trust models for VANETs. We also show when trust is preferable to cryptography, and the opposite. In addition, we shown how trust models are usually evaluated in VANET contexts, and finally we point out some critical scenarios that existing trust models cannot handle, together with some possible solutions.

7.1.2 International Conferences

[KLL14] "Trust model with delayed verification for message relay in VANETs", in *International Wireless Communications and Mobile Computing Conference (IWCMC), 2014*

Trust management is one of the major issues for secure communication in vehicular networks. Most of the existing trust models are identity-based and use excessive periodic exchange between vehicles to build a decision about trustiness of participating vehicles. Malicious data can be minimized in such models by using the identities reputation. In general, the nature and the quality of the data are not taken into account, despite some models which may revoke messages based on their nature and their type. In this paper, we propose a new trust model for VANETs based on the early detection of attacks by relying on the opinion of the last forwarder, and also on the delayed verification of the exchanged messages. We develop an intrusion detection module which performs such operation, evaluating the trustiness of received messages. We introduce a new concept of companion vehicles which

is used to filter out and select the most trusted nodes among neighboring vehicles, to be used as relays in the forwarding procedure. The deployment of this mechanism allows us to prevent vehicles identified as probable dishonest nodes from participating in the network.

[KLCL15] "TROUVE: A trusted routing protocol for urban vehicular environments", in *IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2015*

Delivering data through the most reliable and trusted path is essential for any kind of network. Moreover, in highly mobile and dynamic networks such as VANETs, the problem is more complex since every node requires, at least, a previous knowledge about its own neighborhood to select the most adequate path. In addition, the open communication medium causes other problems that any routing protocol must manage, without forgetting the VANETs' sensitivity to delay. In this paper we proposed a trust-based routing protocol for vehicular urban environments called TROUVE. The proposed protocol aims at finding the shortest and most trusted path to a destination taking into account the real traffic information and the distribution of dishonest nodes in the network.

[KCL+16b] "Trust-aware Opportunistic Dissemination Scheme for VANET Safety Applications", in *The 13th IEEE International Conference on Ubiquitous Intelligence and Computing (UIC), 2016*

Enhancing road safety is the main goal of Vehicular Adhoc Networks (VANETs). In this paper, we proposed an opportunistic alert dissemination mechanism based on the trust relationship among vehicles. Our proposal takes advantage of the standardized alert messages (i.e DENM) to carry the needed information to establish trust and select the most trustable vehicles as the next broadcasters. Our solution can ensure real event alerts dissemination in a wide area without exhausting network resources.

[KCL+16a] "Hierarchical Adaptive Trust Establishment Solution for Vehicular Networks", in *The 27 annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2016*

Most VANET applications, including safety ones, are based on multi-hop communications. Hence, a certain trustworthiness should exist among vehicles to ensure a reliable and trusted communication excluding dishonest peers from all network operations. In this paper we proposed an hierarchical trust establishment solution able to cope with VANET applications and their requirements. Our solution is based on a three-level architecture, which enables it to adapt to the specific communications scenario and the required security level.

7.2 Future works

In the development of this thesis several issues emerged which deserve further scrutiny in a future. The ones we consider most relevant are the following:

- Implementing our protocol on hardware devices and run some real tests.
- Developing our human-aware trust model.
- Solving some privacy concerns.
- Taking advantage of transport buses as mobile certification authorities.
- Extending our solution to take into account the new paradigm of Unmanned Aerial Vehicles (UAVs).

In addition, we also plan to develop some trust-based security solution for contact-based and negotiation-based networks such as named data networks, opportunistic networks, and smart grids.

Bibliography

[BAS14] Tarek Bouali, El-Hassane Aglzim, and Sidi-Mohammed Senouci. A secure intersection-based routing protocol for data collection in urban vehicular networks. In *Global Communications Conference (GLOBECOM), 2014 IEEE*, pages 82–87. IEEE, 2014.

[BBEK11] Michael Behrisch, Laura Bieker, Jakob Erdmann, and Daniel Krajzewicz. Sumo–simulation of urban mobility. In *The Third International Conference on Advances in System Simulation (SIMUL 2011), Barcelona, Spain*, 2011.

[BFIK99] Matt Blaze, Joan Feigenbaum, John Ioannidis, and Angelos D Keromytis. The role of trust management in distributed systems security. In *Secure Internet Programming*, pages 185–210. Springer, 1999.

[BH07] Levente Buttyan and Jean-Pierre Hubaux. *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing*. Cambridge University Press, 2007.

[BK06] Jeppe Bronsted and Lars Michael Kristensen. Specification and performance evaluation of two zone dissemination protocols for vehicular ad-hoc networks. In *Proceedings of the 39th annual Symposium on Simulation*, pages 68–79. IEEE Computer Society, 2006.

[BL02] Alina Bejan and Ramon Lawrence. Peer-to-peer cooperative driving. In *Proceedings of ISCIS*, pages 259–264, 2002.

[BL04] Eric Byres and Justin Lowe. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress*, volume 116, pages 213–218, 2004.

[BP12] Sergey Brin and Lawrence Page. Reprint of: The anatomy of a large-scale hypertextual web search engine. *Computer networks*, 56(18):3825–3833, 2012.

[Bre14] Ross Brewer. Advanced persistent threats: minimising the damage. *Network security*, 2014(4):5–9, 2014.

[But91] John K Butler. Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory. *Journal of management*, 17(3):643–663, 1991.

[CAM14] Etsi eurpean standard, en 302 637-2 - v1.3.1, (2014-09). 2014.

[CB05] David R Choffnes and Fabián E Bustamante. An integrated mobility and traffic model for vehicular wireless networks. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pages 69–78. ACM, 2005.

[CHDV03] Dmitri Chkliaev, Jozef Hooman, and Erik De Vink. Verification and improvement of the sliding window protocol. In *Tools and Algorithms for the Construction and Analysis of Systems*, pages 113–127. Springer, 2003.

[Com13] Intelligent Transportation Systems Committee. Ieee standard for wireless access in vehicular environments-security services for applications and management messages. *IEEE Vehicular Technology Society*, 1609, 2013.

[CW13] Yi-Ming Chen and Yu-Chih Wei. A beacon-based trust management system for enhancing user centric location privacy in vanets. *Communications and Networks, Journal of*, 15(2):153–163, 2013.

[CYHL11] Tat Wing Chim, Siu-Ming Yiu, Lucas CK Hui, and Victor OK Li. Specs: Secure and privacy enhancing communications schemes for vanets. *Ad Hoc Networks*, 9(2):189–203, 2011.

[CZLF12] Shenlong Chen, Yuqing Zhang, Qixu Liu, and Jingyu Feng. Dealing with dishonest recommendation: The trials in reputation management court. *Ad Hoc Networks*, 10(8):1603–1618, 2012.

[Dal09] Michael K Daly. Advanced persistent threat. *Usenix, Nov*, 4, 2009.

[DEN14] Etsi en 302 637-3 - v1.2.2, vehicular communications; basic set of applications; part 3: Specifications of decentralized environmental notification basic service (2014-11). 2014.

[DFM05] Florian Dotzer, Lars Fischer, and Przemyslaw Magiera. Vars: A vehicle ad-hoc network reputation system. In *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*, pages 454–456. IEEE, 2005.

[DGS11] Thomas DuBois, Jennifer Golbeck, and Aravind Srinivasan. Predicting trust and distrust in social networks. In *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on*, pages 418–424. IEEE, 2011.

[DJ07] Sandor Dornbush and Anupam Joshi. Streetsmart traffic: Discovering and disseminating automobile congestion using vanet's. In *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, pages 11–15. IEEE, 2007.

[DLJZ10] Qing Ding, Xi Li, Ming Jiang, and XueHai Zhou. Reputation management in vehicular ad hoc networks. In *Multimedia Technology (ICMT), 2010 International Conference on*, pages 1–5. IEEE, 2010.

[ETS] ETSI. Intelligent Transport Systems.

[ETS12] Etsi ts 102 940 v1.1.1 , intelligent transport systems (its); security; its communications security architecture and security management (2012-06). 2012.

[Fes14] Andreas Festag. Cooperative intelligent transport systems standards in europe. *IEEE communications magazine*, 52(12):166–172, 2014.

[FKL16] David Förster, Frank Kargl, and Hans Löhr. Puca: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks. *Ad Hoc Networks*, 37:122–132, 2016.

[GBW07] Jinhua Guo, John P Baugh, and Shengquan Wang. A group signature based secure and privacy-preserving vehicular communication framework. *Mobile Networking for Vehicular Environments*, 2007:103–108, 2007.

[Ger07] Matthias Gerlach. Trust for vehicular applications. In *Autonomous Decentralized Systems, 2007. ISADS'07. Eighth International Symposium on*, pages 295–304. IEEE, 2007.

[GGS04] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and correcting malicious data in vanets. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 29–37. ACM, 2004.

[GLSB13] Sashi Gurung, Dan Lin, Anna Cinzia Squicciarini, and Elisa Bertino. Information-oriented trustworthiness evaluation in vehicular ad-hoc networks. In *NSS*, pages 94–108. Springer, 2013.

[GRBB12] Tahani Gazdar, Abderrezak Rachedi, Abderrahim Benslimane, and Abdelfettah Belghith. A distributed advanced analytical trust model for vanets. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 201–206. IEEE, 2012.

[GSK+11] Ali Ghodsi, Scott Shenker, Teemu Koponen, Ankit Singla, Barath Raghavan, and James Wilcox. Information-centric networking: seeing the forest for the trees. In *Proceedings of the 10th ACM Workshop on Hot Topics in Networks*, page 1. ACM, 2011.

[GWZZ14] Wei Gao, Mingzhong Wang, Liehuang Zhu, and Xiaoping Zhang. Threshold-based secure and privacy-preserving message verification in vanets. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*, pages 795–802. IEEE, 2014.

[HFFB09] Jérôme Härri, Marco Fiore, Fethi Filali, and Christian Bonnet. Vehicular mobility simulation with vanetmobisim. *Simulation*, 2009.

[HL06] Yih-Chun Hu and Kenneth P Laberteaux. Strong vanet security on a budget. In *Proceedings of Workshop on Embedded Security in Cars (ESCAR)*, volume 6, pages 1–9, 2006.

[HL08] Hannes Hartenstein and LP Laberteaux. A tutorial survey on vehicular ad hoc networks. *IEEE Communications magazine*, 46(6):164–171, 2008.

[HL10] Hannes Hartenstein and Kenneth Laberteaux. *VANET: vehicular applications and inter-networking technologies*, volume 1. Wiley Online Library, 2010.

[HRGD13] Nadia Haddadou, Abderrezak Rachedi, and Yacine Ghamri-Doudane. Trust and exclusion in vehicular ad hoc networks: an economic incentive model based approach. In *Computing, Communications and IT Applications Conference (ComComAp), 2013*, pages 13–18. IEEE, 2013.

[HRGD15] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane. A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. *Vehicular Technology, IEEE Transactions on*, 64(8):3657–3674, Aug 2015.

[IH11] Teerawat Issariyakul and Ekram Hossain. *Introduction to network simulator NS2*. Springer Science & Business Media, 2011.

[Jai90] Raj Jain. *The art of computer systems performance analysis: techniques for experimental design, measurement, simulation, and modeling*. John Wiley & Sons, 1990.

[JCOB02] David Julian, Mung Chiang, Daniel O'Neill, and Stephen Boyd. Qos and fairness constrained convex optimization of resource allocation for wireless cellular and ad hoc networks. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, pages 477–486. IEEE, 2002.

[JKS+12] Wen-Long Jin, Candy Kwan, Zhe Sun, Hao Yang, and G Qijian. Spivc: smart-phone-based intervehicle communication system. In *Proceedings of transportation research board annual meeting*, 2012.

[JRS15] Auxeeliya Jesudoss, SV Kasmir Raja, and Ashraph Sulaiman. Stimulating truth-telling and cooperation among nodes in vanets through payment and punishment scheme. *Ad Hoc Networks*, 24:250–263, 2015.

[JSRGD09] Moez Jerbi, Sidi-Mohammed Senouci, Tinku Rasheed, and Yacine Ghamri-Doudane. Towards efficient geographic routing in urban vehicular networks. *Vehicular Technology, IEEE Transactions on*, 58(9):5048–5059, 2009.

[KA13] Young Ae Kim and Muhammad A Ahmad. Trust, distrust and lack of confidence of users in online social media-sharing communities. *Knowledge-Based Systems*, 37:438–450, 2013.

[KAS15] Uzma Khan, Shikha Agrawal, and Sanjay Silakari. Detection of malicious nodes (dmn) in vehicular ad-hoc networks. *Procedia Computer Science*, 46:965–972, 2015.

[KC14] Neeraj Kumar and Naveen Chilamkurti. Collaborative trust aware intelligent intrusion detection in vanets. *Computers & Electrical Engineering*, 40(6):1981–1996, 2014.

[KCC+] Chaker Abdelaziz Kerrache, Carlos T Calafate, Juan-Carlos Cano, Nasreddine Lagraa, and Pietroe Manzoni. Trust management for vehicular networks: An adversary-oriented overview. *Submitted to Computers and Security*.

[KCL+] Chaker Abdelaziz Kerrache, Carlos T Calafate, Nasreddine Lagraa, Juan-Carlos Cano, and Pietroe Manzoni. Rita: Risk-aware trust-based architecture for collaborative multihop vehicular communications. *Submitted to Security and Communication Networks*.

[KCL+16a] Chaker Abdelaziz Kerrache, Carlos T Calafate, Nasreddine Lagraa, Juan-Carlos Cano, and Pietro Manzoni. Hierarchical adaptive trust establishment solution for vehicular networks. In *The 27 annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2016*. IEEE, 2016.

[KCL+16b] Chaker Abdelaziz Kerrache, Carlos T Calafate, Nasreddine Lagraa, Juan-Carlos Cano, and Pietro Manzoni. Trust-aware opportunistic dissemination scheme for vanet safety applications. In *The 13th IEEE International Conference on Ubiquitous Intelligence and Computing (UIC), 2016*. IEEE, 2016.

[KHRW02] Daniel Krajzewicz, Georg Hertkorn, Christian Rössel, and Peter Wagner. Sumo (simulation of urban mobility)-an open-source traffic simulation. In *Proceedings of the 4th Middle East Symposium on Simulation and Modelling (MESM20002)*, pages 183–187, 2002.

[KKPG16] Chaitanya Kumar Karn and Chandra Prakash Gupta. A survey on vanets security attacks and sybil attack detection. *International Journal of Sensors Wireless Communications and Control*, 6(1):45–62, 2016.

[KLC+] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T Calafate, Juan-Carlos Cano, and Pietro Manzoni. T-vnets: a novel trust architecture for vehicular networks using the standardized messaging services of etsi its. *Computer Communications*, 2016.

[KLCL] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T Calafate, and Abderrahmane Lakas. Tfdd: a trust-based framework for reliable data delivery and dos defense in vanets. *Submitted to Vehicular Communication*.

[KLCL15] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T Calafate, and Abderrahmane Lakas. Trouve: A trusted routing protocol for urban vehicular environments. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on*, pages 260–267. IEEE, 2015.

[KLL14] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, and Abderrahmane Lakas. Trust model with delayed verification for message relay in vanets. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International*, pages 700–705. IEEE, 2014.

[LA98] Raph Levien and Alex Aiken. Attack-resistant trust metrics for public key certification. In *Usenix Security*, 1998.

[LBV06] Jean-Yves Le Boudec and Milan Vojnovic. The random trip model: stability, stationary regime, and perfect simulation. *IEEE/ACM Transactions on Networking (TON)*, 14(6):1153–1166, 2006.

[LHH08] Kenneth P Laberteaux, Jason J Haas, and Yih-Chun Hu. Security certificate revocation list distribution for vanet. In *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, pages 88–89. ACM, 2008.

[LHL+07] Da Li, Hongyu Huang, Xu Li, Minglu Li, and Feilong Tang. A distance-based directional broadcast protocol for urban vehicular ad hoc network. In *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, pages 1520–1523. IEEE, 2007.

[LHSW04] Tim Leinmüller, Albert Held, Günter Schäfer, and Adam Wolisz. Intrusion detection in vanets. In *In proceedings of 12th IEEE International Conference on Network Protocols (ICNP 2004) Student Poster Session*. Citeseer, 2004.

[LLLS13] Xiaoqing Li, Jicheng Liu, Xuejun Li, and Weiying Sun. Rgte: A reputation-based global trust establishment in vanets. In *Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on*, pages 210–214. IEEE, 2013.

[Mat] Matlab - mathworks. *www.mathworks.com/products/matlab/*.

[MBOH14] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66, 2014.

[MCCM08] Francisco J Martinez, Juan-Carlos Cano, Carlos T Calafate, and Pietro Manzoni. Citymob: a mobility model pattern generator for vanets. In *Communications Workshops, 2008. ICC Workshops' 08. IEEE International Conference on*, pages 370–374. IEEE, 2008.

[MDS95] Roger C Mayer, James H Davis, and F David Schoorman. An integrative model of organizational trust. *Academy of management review*, 20(3):709–734, 1995.

[MFC+10] Francisco J Martinez, Manuel Fogue, Manuel Coll, Juan-Carlos Cano, Carlos T Calafate, and Pietro Manzoni. Assessing the impact of a realistic radio propagation model on vanet scenarios using real maps. In *Network Computing and Applications (NCA), 2010 9th IEEE International Symposium on*, pages 132–139. IEEE, 2010.

[MFU+15] Pietro Manzoni, Marco Fiore, Sandesh Uppoor, Francisco J Martínez Domínguez, Carlos Tavares Calafate, and Juan Carlos Cano Escriba. Mobility models for vehicular communications. In *Vehicular ad hoc Networks*, pages 309–333. Springer, 2015.

[MM99] Bob McQueen and Judy McQueen. *Intelligent transportation systems architectures*. 1999.

[MP09] Félix Gómez Mármol and Gregorio Martínez Pérez. Trmsim-wsn, trust and reputation models simulator for wireless sensor networks. In *Communications, 2009. ICC'09. IEEE International Conference on*, pages 1–5. IEEE, 2009.

[MP12] Félix Gómez Mármol and Gregorio Martínez Pérez. Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, 35(3):934–941, 2012.

[MTC+09] Francisco J Martinez, Chai-Keong Toh, Juan-Carlos Cano, Carlos T Calafate, and Pietro Manzoni. Realistic radio propagation models (rpms) for vanet simulations. In *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*, pages 1–6. IEEE, 2009.

[MWR+06] Rahul Mangharam, Daniel Weller, Raj Rajkumar, Priyantha Mudalige, and Fan Bai. Groovenet: A hybrid simulator for vehicle-to-vehicle networks. In *Mobile and Ubiquitous Systems: Networking & Services, 2006 Third Annual International Conference on*, pages 1–8. IEEE, 2006.

[NS-a] Network simulator (ns-2). *http://www.isi.edu/nsnam/ns/ Checked on: 2015/12/03.*

[NS-b] Network simulator (ns-3). *http://www.nsnam.org Checked on: 2015/12/03.*

[OW09] Stephan Olariu and Michele C Weigle. *Vehicular networks: from theory to practice.* Crc Press, 2009.

[Pap10] Dimitri Papadimitriou. Ethernet traffic parameters. 2010.

[Pat16] Al-Sakib Khan Pathan. *Security of self-organizing networks: MANET, WSN, WMN, VANET.* CRC press, 2016.

[PBH+07] Panagiotis Papadimitratos, Levente Buttyan, J-P Hubaux, Frank Kargl, Antonio Kung, and Maxim Raya. Architecture for secure and private vehicular communications. In *Telecommunications, 2007. ITST'07. 7th International Conference on ITS*, pages 1–6. IEEE, 2007.

[PK93] Ramjee Prasad and Adriaan Kegel. Effects of rician faded and log-normal shadowed signals on spectrum efficiency in microcellular radio. *Vehicular Technology, IEEE Transactions on*, 42(3):274–281, 1993.

[PLH06] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong. Security in wireless sensor networks: issues and challenges. In *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, volume 2, pages 6–pp. IEEE, 2006.

[PRL+08] Michal Piorkowski, Maxim Raya, A Lezama Lugo, Panagiotis Papadimitratos, Matthias Grossglauser, and J-P Hubaux. Trans: realistic joint traffic and network simulator for vanets. *ACM SIGMOBILE mobile computing and communications review*, 12(1):31–33, 2008.

[RH05] Maxim Raya and Jean-Pierre Hubaux. The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 11–21. ACM, 2005.

[RH07] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[RK05] Sini Ruohomaa and Lea Kutvonen. Trust management survey. In *Trust Management*, pages 77–92. Springer, 2005.

[RNT+15] Karim Rostamzadeh, Hasen Nicanfar, Narjes Torabi, Sathish Gopalakrishnan, and Victor Leung. A context-aware trust-based information dissemination framework for vehicular networks. *Internet of Things Journal, IEEE*, 2(2):121–132, 2015.

[RPGH08] Maxim Raya, Panos Papadimitratos, Virgil D Gligor, and Jean-Pierre Hubaux. On data-centric trust establishment in ephemeral ad hoc networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008.

[SA14] Riaz Ahmed Shaikh and Ahmed Saeed Alzahrani. Intrusion-aware trust model for vehicular ad hoc networks. *Security and communication networks*, 7(11):1652–1669, 2014.

[SD14] Christoph Sommer and Falko Dressler. *Vehicular networking*. Cambridge University Press, 2014.

[SE13] Aditya K Sood and Richard J Enbody. Targeted cyberattacks: a superset of advanced persistent threats. *IEEE security & privacy*, (1):54–61, 2013.

[sec12a] Etsi eurpean standard,ts 102 867 v1.1.1 (2012-06). 2012.

[sec12b] Ieee std. 1609.2 draft d12 (january 2012)"wireless access in vehicular environments - security services for applications and management messages". 2012.

[SGD11] Christoph Sommer, Reinhard German, and Falko Dressler. Bidirectionally coupled network and road traffic simulation for improved ivc analysis. *Mobile Computing, IEEE Transactions on*, 10(1):3–15, 2011.

[SH16] Irshad Ahmed Sumra and Halabi Bin Hasbullah. Using trusted platform module (tpm) to secure business communciation (sbc) in vehicular ad hoc network (vanet). *Safety*, 5:5–865, 2016.

[SPBN12] Rashmi Ranjan Sahoo, Rameswar Panda, Dhiren Kumar Behera, and Mrinal Kanti Naskar. A trust based clustering with ant colony routing in vanet. In *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on*, pages 1–8. IEEE, 2012.

[SS15] Hichem Sedjelmaci and Sidi Mohammed Senouci. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Computers & Electrical Engineering*, 43:33–47, 2015.

[SWA] Swans, extensions to the scalable wireless ad-hoc network simulator. *http://www.aqualab.cs.northwestern.edu/projects*.

[Tan11] Colin Tankard. Advanced persistent threats and how to monitor and deter them. *Network security*, 2011(8):16–19, 2011.

[TKC10] Ayman Tajeddine, Ayman Kayssi, and Ali Chehab. A privacy-preserving trust model for vanets. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, pages 832–837. IEEE, 2010.

[TPC+15] Sergio M Tornell, Subhadeep Patra, Carlos T Calafate, Juan-Carlos Cano, and Pietro Manzoni. Grcbox: Extending smartphone connectivity in vehicular networks. *International Journal of Distributed Sensor Networks*, 2015:5, 2015.

[TWLY10] Daxin Tian, Yunpeng Wang, Guangquan Lu, and Guizhen Yu. A vehicular ad hoc networks intrusion detection system based on busnet. In *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*, volume 1, pages V1–225. IEEE, 2010.

[VBC13] Anna Maria Vegni, Mauro Biagi, and Roberto Cusani. *Smart vehicles, technologies and main applications in vehicular ad hoc networks.* INTECH Open Access Publisher, 2013.

[VBT10] Wantanee Viriyasitavat, Fan Bai, and Ozan K Tonguz. Uv-cast: an urban vehicular broadcast protocol. In *Vehicular Networking Conference (VNC), 2010 IEEE*, pages 25–32. IEEE, 2010.

[WBH+08] Philipp Wex, Jochen Breuer, Albert Held, Tim Leinmüller, and Luca Delgrossi. Trust issues for vehicular ad hoc networks. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2800–2804. IEEE, 2008.

[WLLS10] Albert Wasef, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]. *Wireless Communications, IEEE*, 17(5):22–28, 2010.

[WMWY15] Yue Wu, Fanchao Meng, Guanghao Wang, and Ping Yi. A dempster-shafer theory based traffic information trust model in vehicular ad hoc networks. In *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*, pages 1–7. IEEE, 2015.

[WTL05] Irene Woon, Gek-Woo Tan, and R Low. A protection motivation theory approach to home wireless security. *ICIS 2005 proceedings*, page 31, 2005.

[WVB+06] Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger, and Scott Shenker. Ddos defense by offense. In *ACM SIGCOMM Computer Communication Review*, volume 36, pages 303–314. ACM, 2006.

[WZWG16] Jin Wang, Yonghui Zhang, Youyuan Wang, and Xiang Gu. Rprep: A robust and privacy-preserving reputation management scheme for

pseudonym-enabled vanets. *International Journal of Distributed Sensor Networks*, 2016, 2016.

[XLL+15] Feng Xia, Li Liu, Jie Li, Jianhua Ma, and Athanasios V Vasilakos. Socially aware networking: A survey. *IEEE Systems Journal*, 9(3):904–921, 2015.

[Yan13] Nianhua Yang. A similarity based trust and reputation management framework for vanets. *International Journal of Future Generation Communication and Networking*, 6(2):25–34, 2013.

[Yeu06] Chan-Yeob Yeun. Security protocol model for ubiquitous networks, September 20 2006. US Patent App. 11/533,728.

[YLN03] Jinsu Yoon, Minggang Liu, and Brian Noble. Random waypoint considered harmful. In *INFOCOM 2003. twenty-second annual joint conference of the IEEE computer and communications. IEEE societies*, volume 2, pages 1312–1321. IEEE, 2003.

[YMF06] Saleh Yousefi, Mahmoud Siadat Mousavi, and Mahmood Fathy. Vehicular ad hoc networks (vanets): challenges and perspectives. In *ITS Telecommunications Proceedings, 2006 6th International Conference on*, pages 761–766. IEEE, 2006.

[ZCC13] Jie Zhang, Chen Chen, and Robin Cohen. Trust modeling for message relay control and local action decision making in vanets. *Security and Communication Networks*, 6(1):1–14, 2013.

[ZCCM11] Jorge Zaldivar, Carlos T Calafate, Juan Carlos Cano, and Pietro Manzoni. Providing accident detection in vehicular networks through obd-ii devices and android-based smartphones. In *Local Computer Networks (LCN), 2011 IEEE 36th Conference on*, pages 813–819. IEEE, 2011.

[Zha11] Jie Zhang. A survey on trust management for vanets. In *Advanced Information Networking and Applications (AINA), 2011 IEEE International Conference on*, pages 105–112. IEEE, 2011.

[ZLL+08] Chenxi Zhang, Rongxing Lu, Xiaodong Lin, Pin-Han Ho, and Xuemin Shen. An efficient identity-based batch verification scheme for vehicular sensor networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008.

[ZLLH08] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, and Pin-Han Ho. Raise: an efficient rsu-aided message authentication scheme in vehicular communication networks. In *Communications, 2008. ICC'08. IEEE International Conference on*, pages 1451–1457. IEEE, 2008.

[ZPU08] Jian Zhang, Phillip A Porras, and Johannes Ullrich. Highly predictive blacklisting. In *USENIX Security Symposium*, pages 107–122, 2008.

[ZZXW16] Kan Zheng, Lin Zhang, Wei Xiang, and Wenbo Wang. *Heterogeneous Vehicular Networks.* Springer, 2016.