الجمـــــهوريـة الجـــزائـريـة الديـــمقراطـيـة الشـــــعبيـــة
PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
وزارة الـــتعلـــيم العالـي والـبـحث العـلـــــمي
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
جامـعـــة عمّـــار ثلـيـجـي بـــالأغـواط
UNIVERSITY OF AMAR TELIDJI-LAGHOUAT
كـلـيـــــة العلـــــــوم
FACULTY OF SCIENCES
قسـم الاعـلام الألـي
COMPUTER SCIENCE DEPARTMENT

End of study dissertation for the Master's degree in Distributed Networks, Systems and Applications

PRESENTED BY

MEHENNI Safa & TAHIRI Malika

Theme

Trust management in FANET Network

Publicly defended in front of the jury composed of

Mr. BOUKHILA	President	Laghouat Univ
Mm. GUIBADJ Fatna	Examiner	Laghouat Univ
Mr. CHAIB Noureddine	Supervisor	Laghouat Univ

Order N° .... / Academic year 2022/2023

Dedications

I affectionately dedicate this modest work:
To my dear mother and father.
For their patience, love, support and
encouragement.
To my loved ones, my brothers and my sisters,
each in his own name, and to all my family.
and to all those who have taught me throughout
my school life.

MEHENNI Safa

I dedicate my work to my very dear
Parents who have sacrificed so much to
Make me succeed.

I extend heartfelt thanks to my sisters and
Brothers for their constant encouragement.

Lastly, I express my sincere appreciation
To my dear friends, who have stood by me

TAHIRI Malika

Acknowledgement

"*No work is exhilarating than that carried out with the moral and financial support of the people who are close to us"*

All our gratitude and thanks to the GOD who gave us the strength, the courage and the will to develop this work. We address our deep thanks to the supervisor Mr. CHAIB NOUREDDINE Professor at the University of Laghouat for directing this work and for his valuable advice and availability. We particularly address our thanks to the members of the jury for doing us the honor of judging our modest work. We would like to thank all the member of the AMAR TELIDJI University of Laghouat, the university that welcomed us with open arms. We would also like to thank the teachers and administrators of the computer science department.

Abstract

The technological advancement in the critical embedded system, avionic and micro electro mechanical system has paved the path to new fully fledged inter connected multi-UAV system, also acronyms as FANET.

FANETs considered as most powerful weapon in military assets as well as in civil applications. Due to its infrastructure less design and wireless nature network some security challenges are code overhead that may caused the network performance degradation. Malicious nodes are capable of degrading the network credibility. In our work we have proposed a mechanism based on a trust management in order to estimate the trust values among flying ad hoc nodes in order to eliminate the presence of malicious nodes caused by security issues in Flying Ad-hoc Networks. To demonstrate the effectiveness of our proposed approach we have used Network Simulator NS2 to demonstrate the entire process into simulated environment.

Keywords :

UAV, FANET, malicious nodes, Trust Management, NS2

Résumé

Les avancements technologiques dans les systèmes embarqués critiques, l'avionique et les systèmes micro-électromécaniques ont ouvert la voie à un nouveau système multi-UAV interconnecté entièrement développé, également connu sous le nom de FANET.

FANET sont considérés comme l'arme la plus puissante dans les actifs militaires ainsi que dans les applications civiles. En raison de sa conception sans infrastructure et de sa nature sans fil, le réseau présente certains défis de sécurité qui peuvent entraîner une dégradation des performances du réseau. Les nœuds malveillants sont capables de dégrader la crédibilité du réseau. Dans notre travail, nous avons proposé une approche basée sur la gestion de la confiance pour estimer les valeurs de confiance entre les nœuds afin d'éliminer la présence de nœuds malveillants causée par des problèmes de sécurité dans les réseaux FANET. Pour démontrer l'efficacité de notre approche, nous avons utilisé le simulateur de réseau NS2 pour simuler l'ensemble du processus dans un environnement simulé.

Mots clés :

UAV, FANET, nœuds malveillants, la gestion de la confiance, NS2

الـمـلـخص

أدى التقدم التكنولوجي في النظام المدمج والنظام الميكانيكي الكهربائي الجوي والدقيق إلى فتح الطريق إلى نظام جديد متعدد الطائرات بدون طيار مترابط بالكامل يدعىFANET .

تعتبرFANET أقوى سلاح في المجالات العسكرية وكذلك في التطبيقات المدنية بسبب تصميمها بدون بنية تحتية وطبيعة الشبكة اللاسلكية، تواجه الشبكة بعض التحديات الأمنية التي يمكن أن تؤدي إلى تدهور أداء الشبكة. يمكن للعقد الخبيثة أن تؤدي إلى تدهور مصداقية الشبكة.

في هذا العمل، اقترحنا آلية تعتمد على إدارة الثقة لتقدير قيم الثقة بين العقد للحد من وجود العقد الخبيثة التي تسببها مشاكل الأمان في FANETs. لإثبات فعالية الآلية المقترحة استخدمنا Simulator NS2 لإثبات العملية برمتها في بيئة محاكاة.

الكلمات المفتاحية:

الطائرات بدون طيار،FANET العقد الخبيثة، ادارة الثقة ,NS2.

Contents

Table of figures

List of tables

General Introduction

Flying will remain one of man's greatest pleasures. . .

In the past few years, the need for connectivity has become a fundamental requirement for people. This need has presented increasingly difficult challenges for modern technology, pushing it towards more innovation and creativity. As a result, new technologies have emerged, including wireless networks and Ad-hoc networks. Ad-hoc networks are wireless networks that can self-organize without any infrastructure, and in a mobile context, they are referred to as MANETs or mobile ad hoc networks.

A mobile ad hoc network (MANET) is a self-governing system of mobile nodes that are linked together via wireless connections. The nodes in the network act as routers and are free to move around randomly and organize themselves in any way they see fit. This means that the topology of the network can change rapidly and unpredictably. This type of network has captured the attention of both manufacturers and researchers, leading to the development of ad-hoc aerial communication networks (FANETs). FANETs are a type of network in which the nodes consist of Unmanned Aerial Vehicles (UAVs). However, these nodes are extremely mobile and able to move at high speeds.

FANETs face unique security challenges that can compromise the network's performance and make it vulnerable to attacks. security challenges in FANETs is the presence of malicious nodes, which can disrupt the network's operations and compromise the integrity of the data being transmitted. In FANET, where the presence of malicious nodes can pose a significant security threat, trust management can be particularly effective in identifying and eliminating these nodes.

We have proposed an approach based on trust management be to identify and eliminate malicious nodes. In our approach, we propose the following plan:

Chapter 1: Earlier, we provided an introduction to FANETs, explaining their fundamental characteristics. We also discussed the unique challenges faced by these networks. Additionally, we mentioned some of the potential applications of FANETs. We also briefly mentioned the different types of communication that can be used in FANETs.

Chapter 2: We have outlined the security issues and challenges that FANETs face.

Chapter 3: We conducted a simulation of a FANET using NS2 to test the effectiveness of our proposed mechanism in detecting malicious nodes that can potentially harm the network.

Finally, we will provide a general conclusion summarizing the work that has been conducted. This conclusion will highlight the key findings and contributions of our project and provide insights into the potential areas for future research.

Chapter 1:

Flying Ad Hoc Networks (FANETs)

1.1 Introduction

Technological advancements in electronics, sensors, and communication systems have enabled the production of small UAVs (unmanned aerial vehicles) that can be used in a variety of military, commercial, and civilian applications. However, the performance of a single small UAV is insufficient. Multiple UAVs can form a system that goes beyond the limitations of a single small UAV. Flying Ad Hoc Networks (FANETs) are such networks, consisting of groups of small UAVs that are self-organizingly connected and integrated into a team to achieve high-level goals. This chapter introduces the FANET network and its related concepts.

1.2 Ad-hoc Networks

Ad hoc networks are the ultimate frontier of wireless communications. The technology allows network nodes to communicate directly with each other via wireless transceivers (possibly via multi-hop paths) without the need for fixed infrastructure. This is a very special feature of ad hoc networks compared to traditional wireless networks such as cellular networks and WLANs, where nodes communicate with each other through base stations (Figure 1).

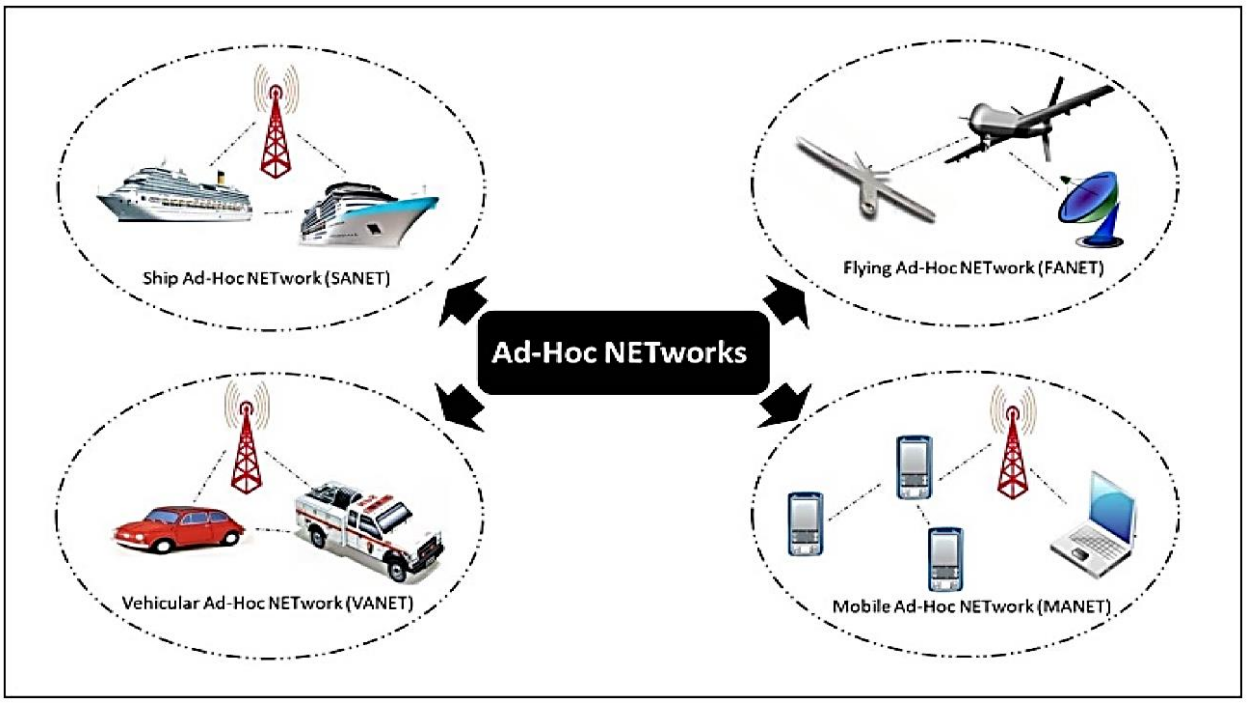

Figure 1: *Ad hoc networks*

1.3 MANET Network

The mobile ad-hoc network (MANET) is a collection of wireless nodes interconnected and dynamically configured at any place or at any time, excluding the pre-existing transport (in Figure 2). MANETs have many fields of application such as disaster relief, communication, urgent business meetings, etc. The main advantage of MANETs is their portability or mobility [1].

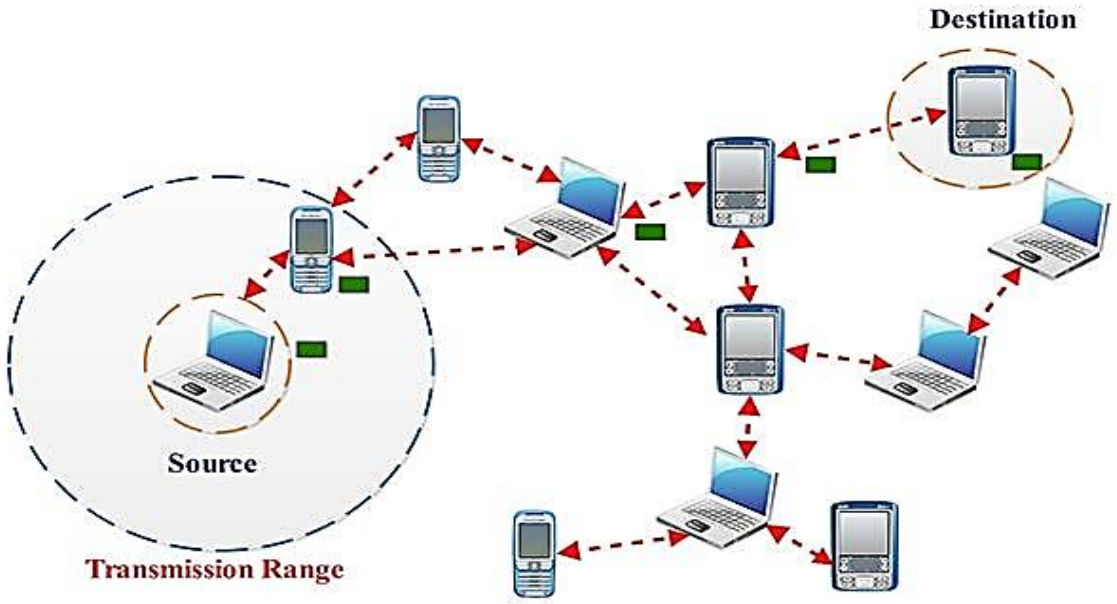

Figure 2:*MANET Network*

1.4 FANET Network

FANET (Flying Ad Hoc Network) is a special form of mobile ad hoc network in which the nodes are Unmanned Aerial Vehicles (UAVs). FANET nodes communicate with each other wirelessly through base stations to form an ad hoc network. UAVs transmit data and signals, there is no physical connection between them. A typical FANET architecture is shown in Figure 3.

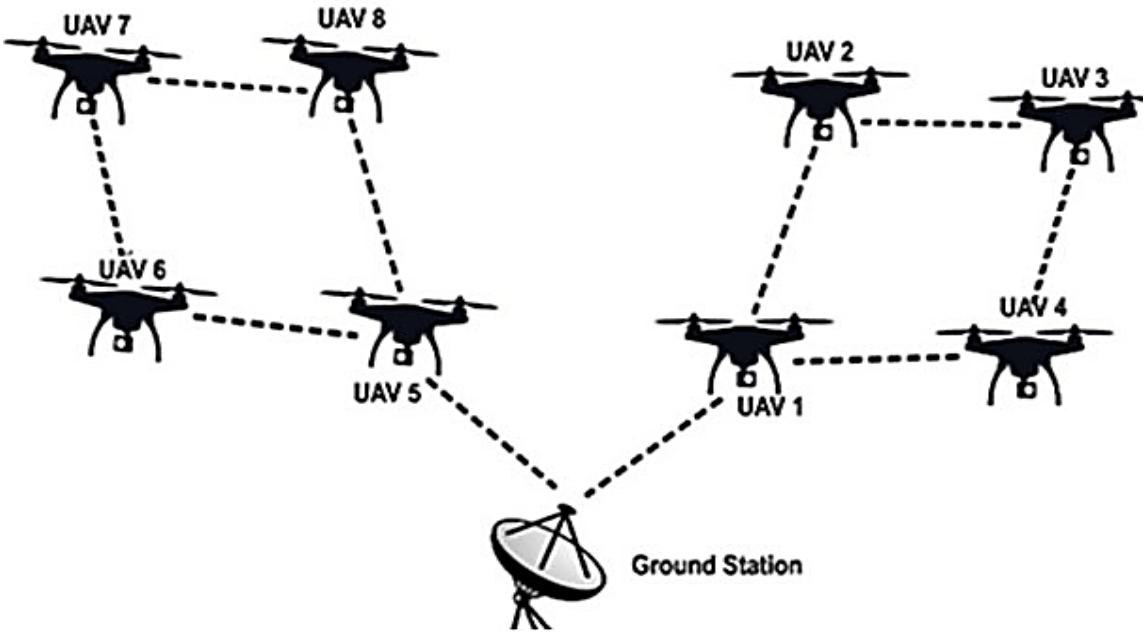

Figure 3: *FANET Network*

1.5 FANET architecture

The basic components of a FANET system as shown in figure.

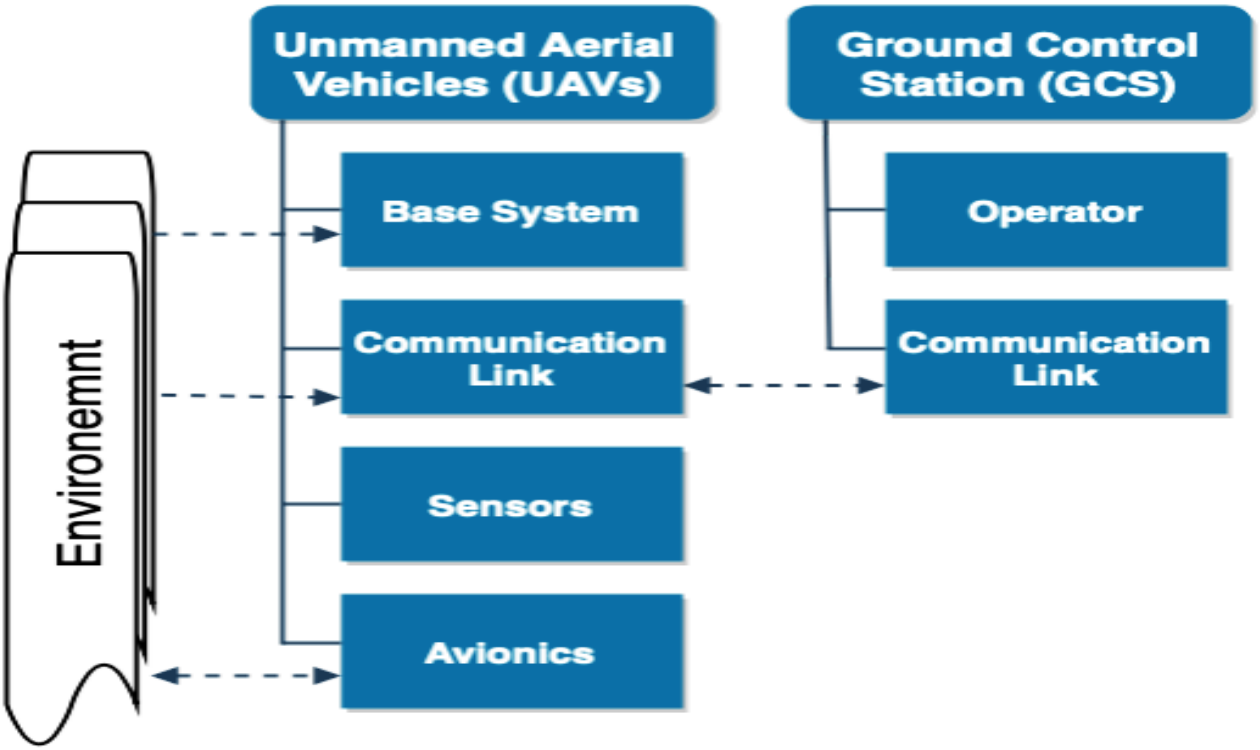

Figure 4:*Components of FANET Network and information flows*

1.5.1 UAVs (unmanned aerial vehicle)

The main component of the FANET network is the UAV. A UAV is an aircraft without a human pilot on board, commonly known as a drone. It is equipped with various additional devices such as base system and sensors. It flies very stably, can fly in the air and perform a variety of missions. Its versatility makes it very popular (Figure 5).

Figure 5:*unmanned aerial vehicle*

- ***Base system***

The UAV base system is designed for UAVs and is responsible for connecting all of the components. It is utilized to communicate amongst components as well as to control sensors and communication/navigation systems. The extra components are also included into the UAV base system.

- ***Sensor***

The entire spectrum of sensory apparatus, including sensors with cameras, GPS, and radars, is included in the UAV sensor system.

- ***Avionics***

The avionic system is in charge of carrying out control commands from the controller, such as engine commands, spoilers, flaps, and stabilizers.

UAVs rely on a wireless communication system, which can be either direct line of sight or indirect connection via satellites.

1.5.2 GCS (ground control station)

The ground-based station that connects with the UAV nodes is known as the GCS. The GCS is in charge of collecting data from the UAV nodes as well as guiding and controlling the nodes in FANET. The GCS plays several important roles in FANET architecture, including:

- ***Mission planning and control:***

The GCS is responsible for planning and controlling the missions of the UAVs in the network. It determines the flight path, altitude, and speed of the UAVs, and sends commands to the UAVs to carry out specific tasks.

- ***Communication and data exchange:***

The GCS provides a centralized communication and data exchange hub for the UAVs in the network. It receives data from the UAVs, processes it, and distributes it to other nodes in the network as needed.

- ***Monitoring and control:***

The GCS monitor the status of the UAVs in the network, including their position, altitude, battery life, and other key parameters. It can also issue commands to the UAVs to adjust their flight path or behavior as needed.

- ***Network management:***

The GCS is responsible for managing the overall operation of the FANET network. It ensures that the network is stable and reliable, and can take steps to address any issues that arise.

1.6 FANET Network characteristics

As shown in figure 6 flying ad-hoc networks have several important characteristics, which are detailed below.

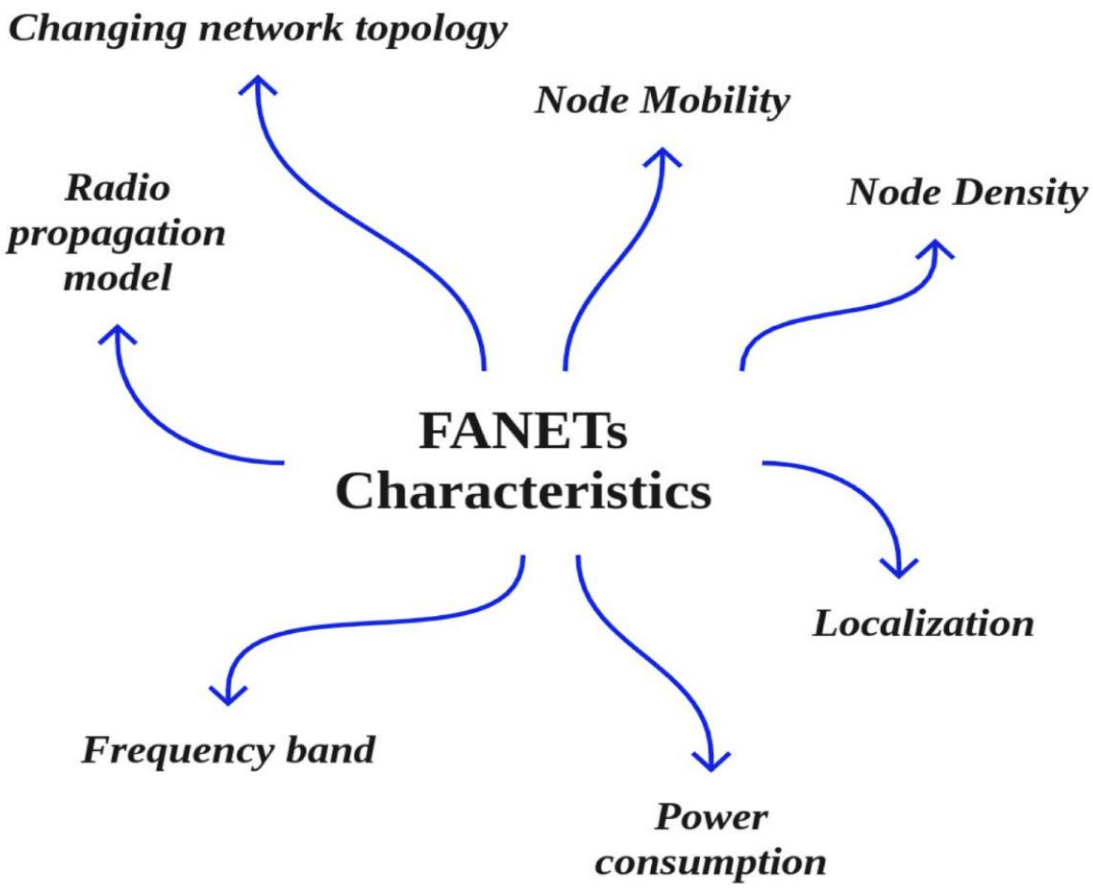

Figure 6:*FANET characteristics*

1.6.1 Changing network topology

FANET is a distributed, peer-to-peer, multi-connection network in terms of topology. Nodes join "on the fly" in accordance with the "with each other" principle. By consecutively or gradually replacing UAVs, this topology enables the expansion of the task completion area by streaming data constantly (up to 24 hours per day).

1.6.2 Node density

Node density refers to the average number of UAVs in a given area. Depending on the nature of the flight, there must have a sparse density separated by considerable distances in FANETs [2].

1.6.3 Node mobility

The UAV travels at a speed of 30-460 km/h, which poses a communication problem between the UAVs [2].

1.6.4 Power consumption

The communications equipment in FANETs is powered by the UAV's own power source. In this instance, unlike MANET applications, FANET designs may not be power sensitive. However, it is still a concern in mini-UAVs [3].

1.6.5 Radio propagation model

Differences in the operating environment of FANET and other ad-hoc networks affect radio propagation characteristics. MANET nodes are located close to the ground and often do not have direct connections between transmitters and receivers.

Therefore, radio signals are mainly affected by the geographical structure of the terrain. However, FANET nodes can be far from the ground and in most cases there is a direct line between UAVs [4].

1.6.6 Localization

Location means the location of each UAV. Due to the high speed and frequent changes of location, it is necessary to have high location information with low time intervals. Using GPS, information about new locations will be transmitted to the network every second, which is insufficient. Therefore, each UAV must contain a GP and an initial measurement unit to broadcast its location to all UAVs in the network at all times [5].

1.7 Communication Models in FANET

There are two types of communication for FANET:

1.7.1 UAV to UAV

Information exchange between UAVs directly through different routing algorithms. Maintaining communication between UAVs leads to multiple research directions [12] as the FANET topology changes frequently with the removal or addition of new UAVs (in figure 7).

1.7.2. UAV To infrastructure

A small number of UAVs that are in communication with the infrastructure (base station) form the basis of UAV-to-infrastructure communication. This method of communication necessitates the sharing of heavier data and delivers information about the intended tasks on a bigger scale [12] (in figure 7).

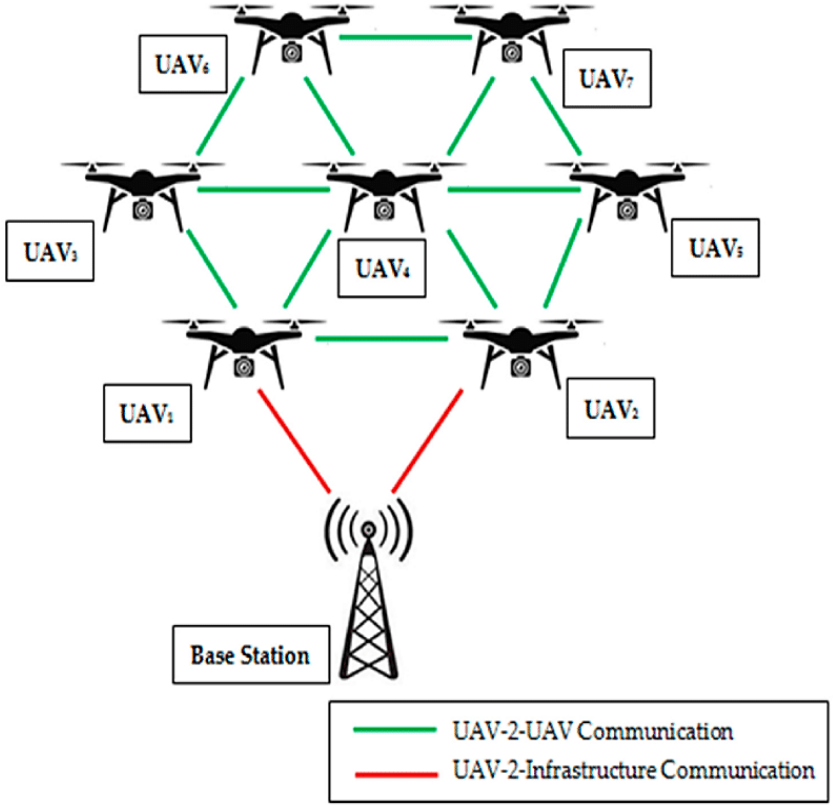

Figure 7 : *Communication Models in FANET*

1.8 FANET Applications

FANETs have a variety of applications because to their physical and architectural properties, some of these are stated below.

1.8.1 Disaster monitoring

In some disasters, a human may confront difficulties that prohibit him from analyzing the entire damaged area. In this case, FANETs can be used to completely evaluate the scenario [6] (in figure 8).

Figure 8:*Disaster monitoring*

1.8.2 Monitoring of agricultural areas

FANETs can be used in agriculture for a variety of purposes, including total crop evaluation, plant health analysis, and mapping of potential planting extension regions [6] (in figure 9).

Figure 9:*Monitoring of agricultural areas*

1.8.3 Search and rescue operations

When traditional mobile networks are destroyed during a rescue mission, FANETs can be utilized to search for hostages in the impacted area. Because of the size of the UAVs, it is possible to explore areas that a human would find impossible to approach [7] (in Figure 10).

Figure 10: *Search and rescue operations*

1.8.5 Product delivery

Some businesses already envision using UAVs to deliver products in order to lower costs and enhance the quality of their services [6]. A smart system will be included into the UAVs to enable autonomous performance of the service [8] (in Figure11).

Figure 11:*Product delivery*

1.8.6 Military service

Military personnel use FANETs extensively, primarily for communication between soldiers or between barracks. It can also be used in civil operations to keep society safe [7] (in figure 12).

Figure 12:*Military services*

1.9 FANET Routing Protocols

Finding a suitable path for data relaying in a network is the main goal of routing protocols [9]. Due to UAVs' high degree of mobility, FANET's topology will change continuously [10]. It is still being researched how to create a routing protocol that is effective for FANETs. The majority of the routing protocols created for MANET and VANET in conventional networks cannot be directly applied to FANETs due to UAVs' special characteristics [1]. Some already-used protocols have been modified for FANETs routing, and some new protocols have been proposed [11]. The four categories of FANET protocols are shown in Figure 13.

1. **Static protocols:** have static routing tables there is no need to refresh these table
2. **Proactive protocols:** also known as table driven protocols, are periodically refreshed Routing tables.

3. **Reactive protocols:** also called on-demand protocols, discover paths for messages on demand.
4. **Hybrid protocols:** use both proactive and reactive protocols.

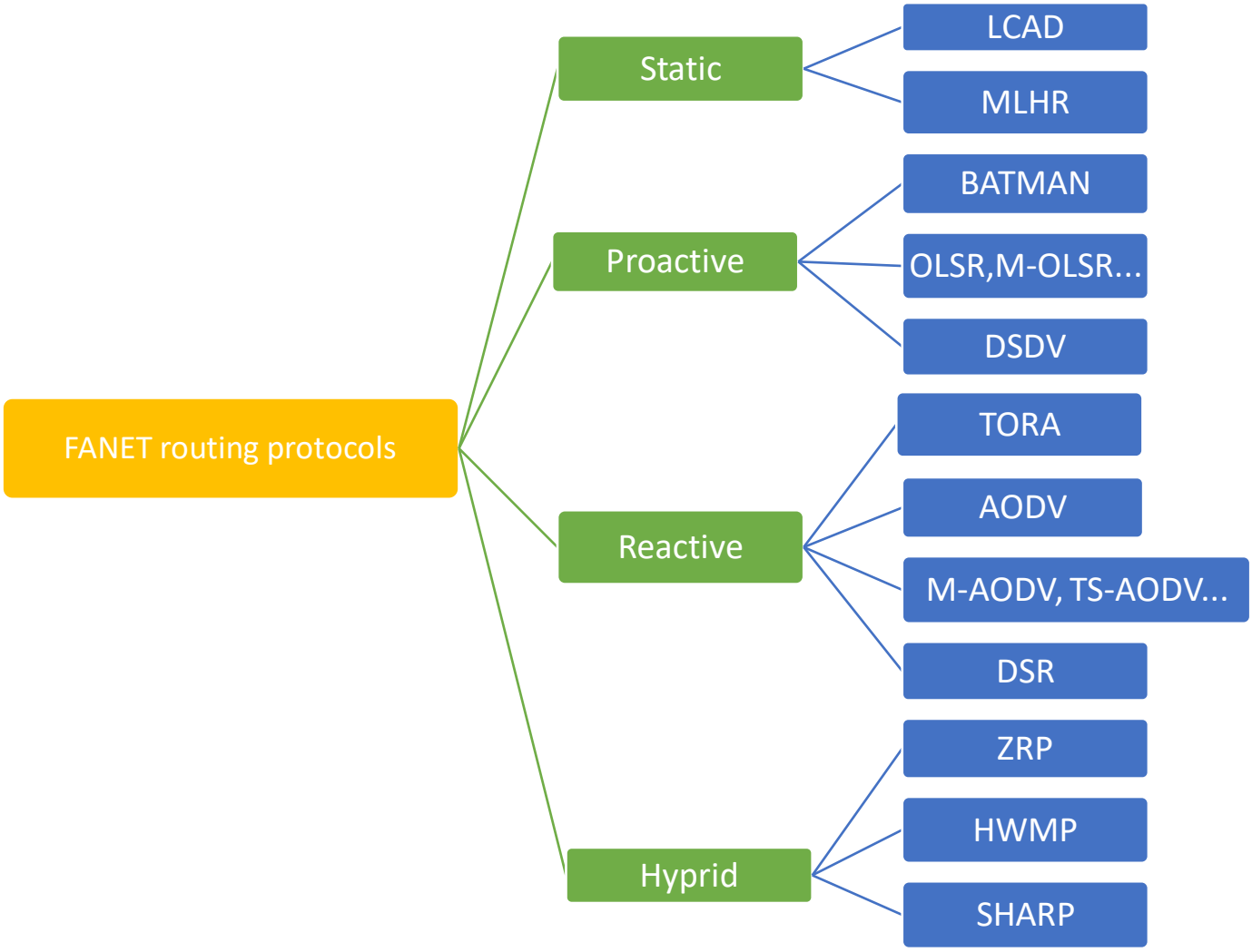

Figure 13: *FANET routing Protocol*

1.10 Mobility models

Mobility models Represent the motion of nodes and the way in which their location, speed and acceleration change over time. mobility models provide a realistic simulation environment. it showed how the performance of an ad hoc protocol can vary significantly with the help of various mobility models. Figure 14 shows our four mobility models in FANET.

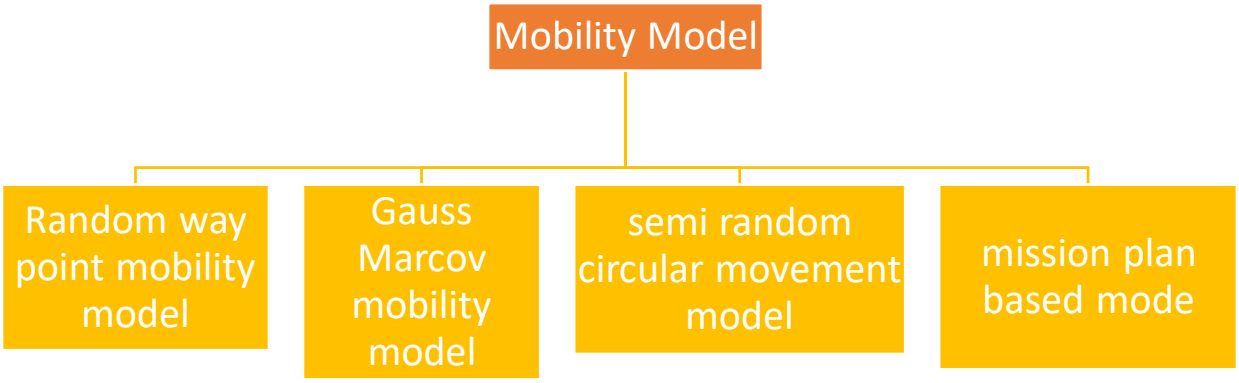

Figure 14:*Mobility models in FANET*

1.10.1 Random way point mobility model:

The Random Waypoint Mobility Model used by Johnson and Lee includes downtime between steering and/or speed changes. In all random based mobility models, the UAV nodes are free to roam around the simulation region in any direction. We may assert that a node is unrestricted in its ability to pick its position, speed, and direction from those of its neighbors. UAVs rely their decisions on predefined probabilities when deciding how to proceed.

In the majority of simulation situations up to this point, the random waypoint model has been employed as a synthetic mobility model. However, it is not appropriate for the aircraft example since aircraft cannot spend an extended period of time at the same location like the random waypoint model because they cannot change their direction and mobility speed quickly at the same time. Going "straight," turning "left," and turning "right" are the three activities on which this mobility paradigm is built.

1.10.2 Gauss-Markov Mobility Model:

The UAV behavior in a swarm is simulated using the Gauss Markov Mobility Model. The simulated area's size might vary. Due to its rapid movement, a node's position is always guided by its prior location. The model's memory determines the course of a drone. Each node in the Gauss-Markov Mobility Model is initialized with a direction and speed. Movement takes place at regular intervals, with each node's speed and direction being updated. To be more precise, a random variable and the values of speed and direction at the n-th instance of time are used to compute the value of speed and direction at the n-1 occurrence.

1.10.3 Semi random circular movement:

This mobility model was created to accommodate UAVs' curved moving patterns. It may be used to simulate UAVs spinning around in order to acquire data at a certain location. Unpredicted helper nodes like UAVs can use a mobility model with a hexagonal route rather than a random waypoint model since their flight path is not predefined.

1.10.4 Mission Plan Based Mobility Model:

In the MPB model, aircraft are already aware of the vast amount of trajectory information, which is typically planned in advance. This means that the aircrafts consistently follow the predetermined path when location information for potential targets is available, as shown in figure 15, where the aircrafts arrive at the mission area. After a certain amount of time has passed, the mobility files in the MPB mobility model are often produced and updated.

For aircraft that are expected to travel toward or away from their target, a mobility model based on the mission plan is used. Starting and finishing points are chosen at random for each aircraft, and flight time and velocity are provided. If an airplane reaches its destination before its flight time has expired, it reverses course and resumes its journey as a roundtrip.

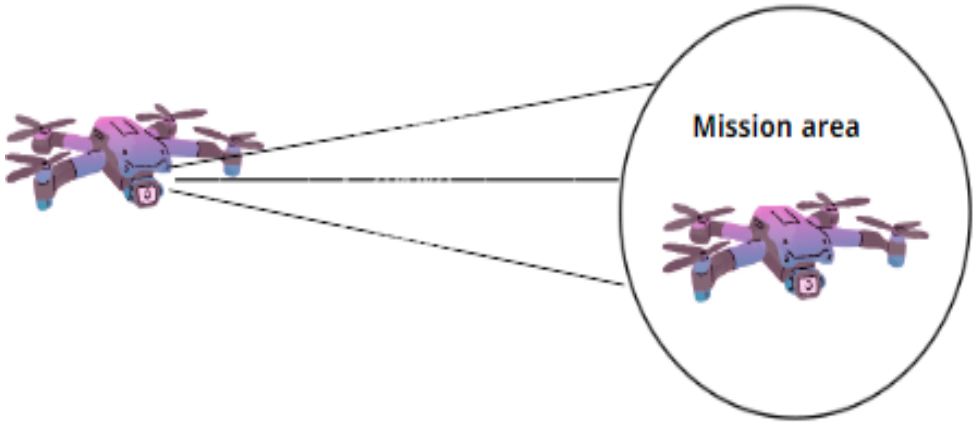

Figure 15:*Mission Plan Based Mobility Model*

1.11 Conclusions

In this chapter, we have provided an introduction to FANETs, which are wireless ad hoc networks comprising of unmanned aerial vehicles (UAVs) that communicate with each other to accomplish various tasks. We have discussed the various components of FANETs, including the UAVs, ground control stations, and communication links between them. We have also highlighted some of the characteristics of FANETs which make them suitable for a wide range of applications. Furthermore, we have explored the mode of communication in FANETs, which involves wireless communication between UAVs and ground control stations, as well as communication between UAVs themselves.

We have also discussed the various applications of FANETs, including surveillance, search and rescue, disaster management, and military operations. FANETs are also being explored for commercial applications, such as package delivery and agriculture.

Overall, FANETs have great potential in various domains due to their unique characteristics, and they are expected to play an increasingly important role in the future. It is crucial to continue researching and developing new technologies and security mechanisms to ensure the reliability and security of FANETs in various applications.

Chapter 2:
Security in FANET Network

2.1 Introduction

Security is one of the major factors in the ad hoc network. FANET are next-generation networks and by virtue of their characteristics legacy form wireless ad hoc network, many security issues and challenges exist and play an important role in degrading the network's life time, reliability and credibility. Successfully implementing this network in a real-world environment, the network must be secure in order for the end user to benefit from its life safety applications. This chapter includes an overview of fundamental security needs. In ad hoc networks and we have identified a variety of challenges and attacks which have exploited UAV security in FANET Network. As a solution to the potential attacks, trust mechanism has been discussed.

2.2 Requirements for Basic Security

Below are listed the essential security requirements. [13]:

2.2.1 Availability:

Nodes should continue to be able to supply all the designed services. The safety zone was desecrated during the denial of services attack without taking into account its security condition and each node that approves evaluates the data [14].

2.2.2 Authentication:

Authentication establishes the reliability of the communication between two dissimilar nodes. As the identification of the source node is being ensured so that the necessary participant be certain about your identification. Utilizing certificates as a means of providing this service, whoever in absence of central control unit, key management and key allocation can be contested.

2.2.3 Integrity:

Integrity refers to ensuring that data transmitted within the FANET system is not tampered with or modified in any unauthorized way.

The data may include control signals, sensor readings, or other data that are critical to the operation of the system. Mechanisms such as digital signatures or message authentication codes (MACs) can be used to ensure integrity.

2.2.4 Confidential data:

Confidentiality refers to protecting sensitive information from unauthorized access or disclosure. FANET systems may transmit sensitive information, such as mission-critical data or personal information, which needs to be protected from unauthorized access or disclosure. Therefore, mechanisms such as encryption or access control can be used to ensure confidentiality.

2.2.5 Authorization:

Authorization refers to ensuring that nodes within the FANET system have the necessary privileges to perform certain actions. Mechanisms such as access control can be used to ensure that only authorized nodes can perform certain actions, such as generating, editing, or removing packets.

2.2.6 Privacy:

Privacy retains the personal information of the node not dispersed therefore the Contact not known, whether made by the node itself or the system software.

these basic security requirements are essential for ensuring the security and reliability of a FANET system. By implementing these requirements, the system can be protected against various types of attacks and ensure that it operates effectively and efficiently.

2.3 Challenges in FANET

The difficulties with FANET are listed below [15]:

2.3.1 Routing:

FANET uses diversified routing from the other ad hoc network due of the high node mobility, moreover the topology modify very frequently, there are two significant obstacles to be seen:

- ✓ Algorithm for routing work high mobility
- ✓ It should be quick to update the routing algorithm.

2.3.2 UAV Placement and Mobility:

Basically, the placement of UAV is appropriate the major concern in FANET since UAV are the available diverse capabilities and capacities for different purposes. Open difficulties are to optimize the UAV placement.

2.3.3 Quality of Service (QOS):

In FANETs UAVs transmit data includes audio, video, images, text, GPS locations etc. To transfer such data, it should via high-quality services with few delays and errors [16].

2.3.4 Reliable Data delivery:

Apps using FANET transport highly significant data that must be supplied on time to other apps. Consequently, the network must have very high trust [17].

2.3.5 Security:

In FANET mange the secure routing point is: Make sure Confidentiality, Integrity and Availability of precious information so these networks are essential to manage Lack of physical security node compromises. There is another issue in FANET, Trust management is another important point in FANET, nodes leave and join very frequently, Accessibility routing algorithms for ad-hoc networks are unable in the opposition to frequent network topology modify and malicious attacks in FANET.

2.4 Potential Attacks in FANETs

Due to features that FANETs inherited from MANETs, they are vulnerable to different security attacks. These assaults aim to compromise the availability, confidentiality, and integrity of nodes. Table 1 listed a few attacks of FANETs [19–21].

Attacks	Source	Target	Attacking Behavior	Attacks Consequences
Malicious hardware or software	In	Confidentiality	A Trojan of backdoor is installed in ground control unit.or flight controller	Loss of confidential mission data.
Sybill	In	Confidentiality	A node uses several identities to pretend as multiple nodes in the networks	Eavesdropping between legitimate nodes using links.
Sinkhole	In	Availability	draw in all network traffic.by showing the best path through it.	Erroneous route creation.
Bad mounting attack	In	Availability	To make other nodes less trustworthy, the attacking node disseminated false trust values.	Block the real path.
Conflict behavior	In	Availability	Attacker node exhibits different behaviors for differents nodes.	Conflicting opinions make to lesse trustworthy
Selfishness	In	Availability	In order to conserve resources like batteries, an attacking node may decide not to transmit data.	Increased packet drop rates and end-to-end delays.

Table1: *Attacks in FANETs*

2.5 Trust Management

Trust is the belief between two or more communicative parties. Blaze et al [21] defined "Trust Management" as different components of security networks in the intrusion detection systems, the trust management is very important. Access control systems, malicious node detection, safe routing, and authentication.

Trust management starts from trust establishment, followed by updating trust values depending on interactions, and lastly, Revocation of trust is possible if the trust values fall short of the required level. The difficulty of this task increases for ad-hoc networks.

2.6 Conclusion

In this chapter, we discussed the fundamental security requirements in ad hoc networks, which are essential to ensure the confidentiality, integrity, and availability of data. We also highlighted the unique challenges and attacks that are specific to FANETs.To address these security issues, we introduced the concept of trust management as a potential solution to identify and isolate malicious node.

In summary, trust management is a promising approach to addressing the security challenges in FANETs. By implementing appropriate trust management systems, it is possible to enhance the security and reliability of FANETs and ensure the successful deployment of various applications in domains such as military operations, disaster management, and surveillance.

Chapter 3:

Detection of black hole attack using trust management

3.1 Introduction

FANETs are vulnerable to various attacks, particularly those resulting from node misbehavior. One of the most dangerous attacks in FANETs is the black hole attack, where a malicious node drops data packets from the network without forwarding them to their intended destination, acting like a black hole in the universe. Unfortunately, traditional routing protocols, such as AODV, do not monitor or attempt to reduce this type of malicious activity.

To address this issue, we proposed a mechanism based on trust management to detect and prevent black hole attacks. This mechanism involves establishing and maintaining trust relationships between nodes in the network, based on various factors such as communication history, and performance metrics. By utilizing trust management mechanisms, we can effectively detect and isolate malicious nodes, mitigate the impact of black hole attacks, and improve the overall security and reliability of FANETs.

3.2 AODV Routing Protocol

Ad hoc networks frequently employ the Ad hoc On-Demand Distance Vector (AODV) routing protocol. For wireless and mobile ad hoc networks, AODV is a reactive and routing protocol. For route finding, AODV protocol employs a straightforward request-reply mechanism. In order to construct a route to the destination D, source node S broadcasts RREQ packets. After receiving an RREQ packet, nodes A, B, and C do one of the following actions:

1) If the node is the destination node or has a recent enough path to the destination, send an RREP packet back.

2) Rebroadcast the RREQ after updating the routing table.

The destination sends RREP back to the source after receiving RREQ. The intermediary nodes will change their routing tables as a result of the RREP message reaching the source node through them. This RREP is accepted by the source node if:

1) The destination sequence number is greater than the routing table's value.

2) If the hop count at the source is lower than the hop count in the routing table and the destination sequence number is equal to the one in the routing table.

3.3 Black hole attack

A black hole attack [23] that is simple to use against routing in ad-hoc networks. A malicious node claims that it has the shortest path to any destination node in an attempt to attract all packets. Without first checking its routing table, the attacker node sends a false RREP message containing a false route to the destination over itself after receiving an RREQ message, setting the hop count value to the lowest values and the sequence number to the highest values to settle in the routing table of the victim source node.

Therefore, source node considers that route discovery procedure is finished and disregards further RREP signals before starting to deliver packets through attacker node. In this manner, the attacker node assaults all RREQ messages and seizes control of all routes. As a result, after being transmitted down a path, all packets are simply dropped and fail to reach their intended destination (in figure 16).

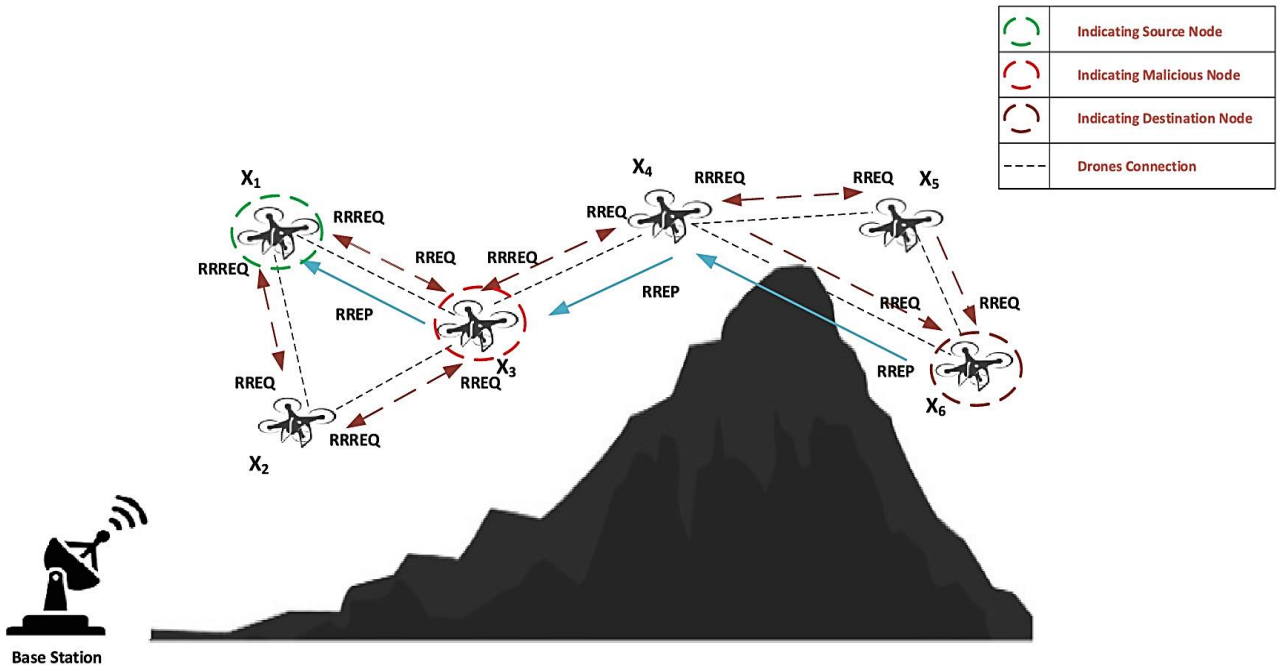

Figure 16:*Black hole attack*

3.4 Proposed mechanism to detect black hole

As the demand for FANET continues to rise, the need to detect network attacks has become increasingly crucial due to the rising number of attacks in networks. To address this issue, we proposed a method for identifying malicious attacks, specifically black holes, which pose a significant threat to FANETs.

Our approach involves estimating the trust value of the network, and we set the threshold initially to 0.5. If the trust value falls below this threshold, it indicates the presence of a malicious node in the network. This malicious node can then be detected by analyzing the trace file.

3.4.1 Trust value calculation

To determine the trust value of the network, a straightforward formula is used, which involves dividing the number of packets dropped by the number of packets sent. The resulting value represents the network's trustworthiness and will range from 0 to 1.

$$T = 1 - (D/F)$$

- T: Trust value
- D: Number of dropped packets.
- F: Number of forwarded packets.

3.5 Performance metrics:

There is a large set of metrics we can measure performance of routing protocols. In what follows the criteria used for our simulation of FANET:

3.5.1 Ratio of packets delivered:

The packet delivery ratio can be expressed by

$$PDR = (\sum R / \sum T) * 100$$

- PDR: packet delivery ratio
- R: Number of received packets
- T: Number of Packets transmitted

3.6 Simulation scenario

In a network consisting of many UAV nodes that use the AODV protocol, the presence of a malicious node (represented by the red node) can cause significant disruption. This malicious node can intercept the RREQ request made by the sender node (represented by the green node) and redirect the packet flow towards the destination node (represented by the blue node).

Consequently, the packets are directed towards the attacking node, which then acts as a black hole and retains all the data without transmitting it to the destination node. As a result, the data is lost, and the network's overall performance is compromised.

3.7 Simulation tool NS 2.35

For the purpose of researching the dynamic behavior of communication networks, Network Simulator (NS) is only a discrete event-driven network simulation tool. For the modeling of many protocols via wired and wireless networks, NS2 offers a lot of support. It offers a highly modeling framework for wired and wireless networks that supports various network components, protocols, traffic patterns, and routing types [24]. The two main languages used in NS2 are Tool Command Language (tcl) and C++.

A tcl (Tool Command Language) file is produced by the NS2 simulator. Three additional files are produced when a TCL file is executed, the first of which is a Terminal File that displays the status of the packet and the nodes from which it was forwarded and to whom it was delivered.

The nam (Network Animator) file, the second file, is a visual representation of all the mobile nodes and the network's packet flow. The Trace File, displays all pertinent details about the network and data flow.

3.8 Simulation Parameters

Table below present the parameters we used in our FANET simulation scenario such as routing protocol, mobility model and traffic Model by utilizing these parameters in the FANET simulation scenario, it was possible to evaluate the performance.

Paramètre	***Value***
Protocol	AODV
Application Traffic	CBR /UDP
MAC type	Mac/802_11
Channel type	Wireless Channel
Simulation time	5 s
Number of nodes	7
Area	800 m * 800 m
Mobility Model	Two Ray Ground
Types of attack	Blackhole attack

Table2: Simulation Parameters

3.9 Results & Analysis

In our simulation scenario, we constructed a FANET network consisting of 7 UAVs and employed AODV as the routing protocol to transmit packets from a sender to a receiver. To detect the presence of a black hole node, we implemented the trust-based mechanism that we proposed.

During the simulation, we analyzed the performance metric packet delivery ratio identify any anomalies or suspicious behavior that might indicate the presence of a black hole node. We also monitored the trust levels of each node in the network, based on their communication history.

3.9.1 The simulation of one black hole attack in a FANET network

The figure 17 shows the simulation of one black hole attack in a FANET network.

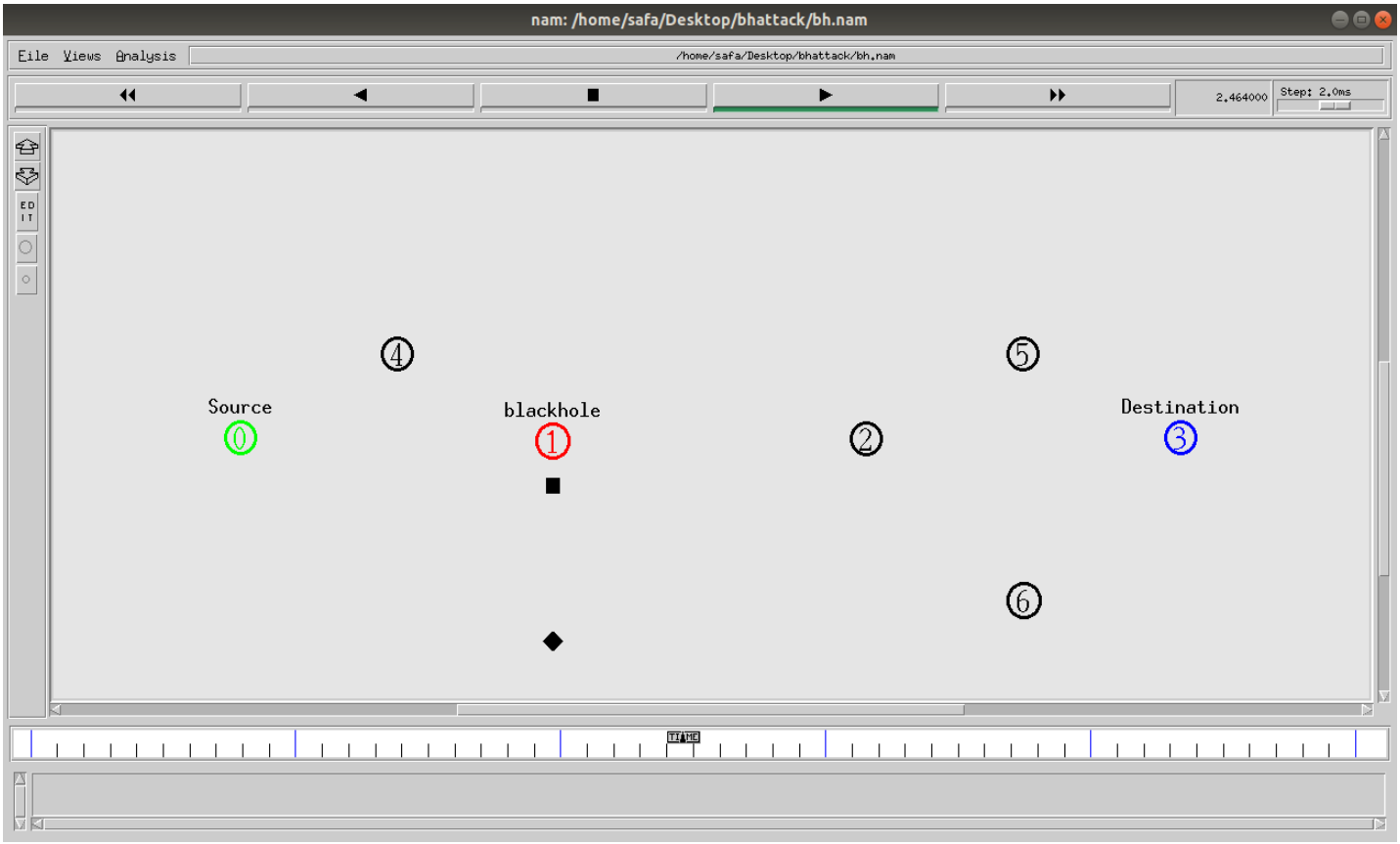

Figure 17: *Simulation of one black hole attack*

The result of trust calculation and PDR in presence of one black hole attack:

```
safa@safa-HP-ProBook-11-G2: ~/Desktop/bhattack
File  Edit  View  Search  Terminal  Help
the blackhole is n(1)
safa@safa-HP-ProBook-11-G2:~/Desktop/bhattack$ ns bhattack.tcl
num_nodes is set 7
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
Number of packets dropped : 35
Number of packets forwarded : 54
trust value : 0.35185185185185186
Packet Delivery Ratio : 35.185185185185183
the blackhole is n(1)
```

Figure 18: *Trust & PDR results in presence of one black hole attack*

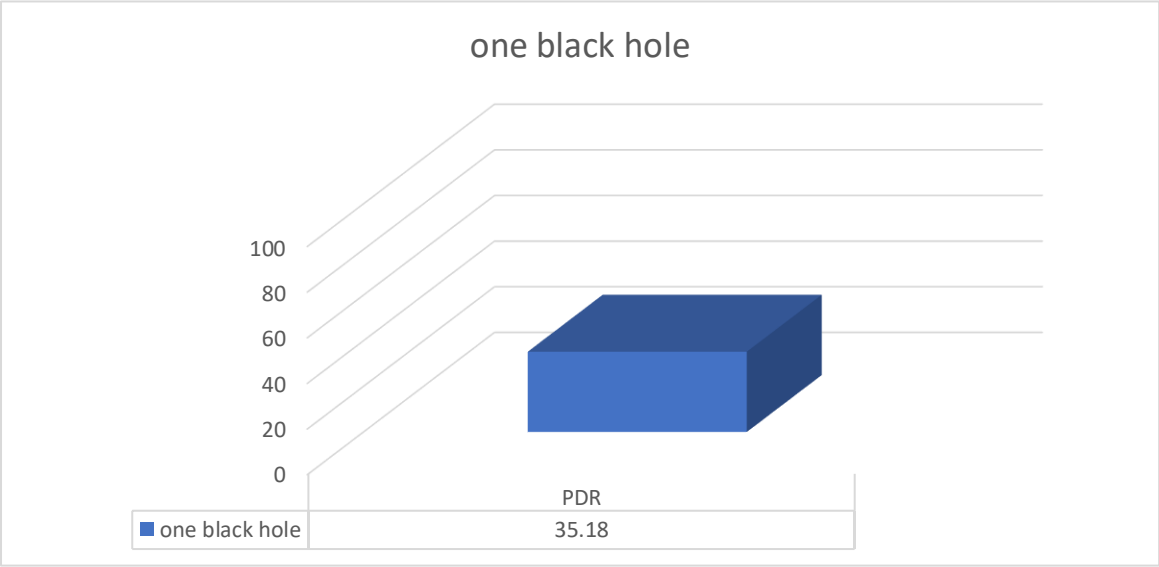

Figure 19: *PDR diagram in presence of one blackhole attack*

3.9.1 The simulation of two black hole attack in a FANET network

The figure 19 shows the simulation of two black hole attack in a FANET network.

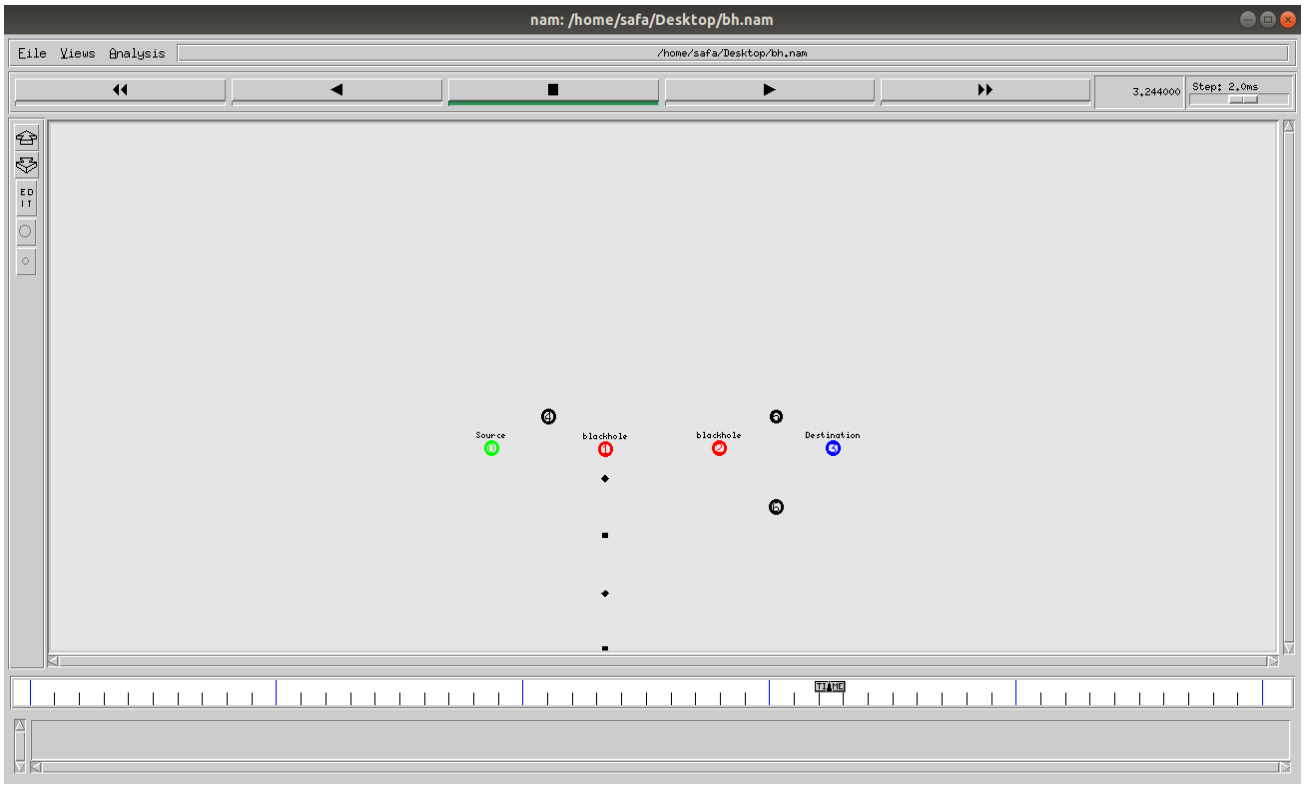

Figure 20: *Simulation of two black hole attack*

The result of trust calculation and PDR in presence of one black hole attack:

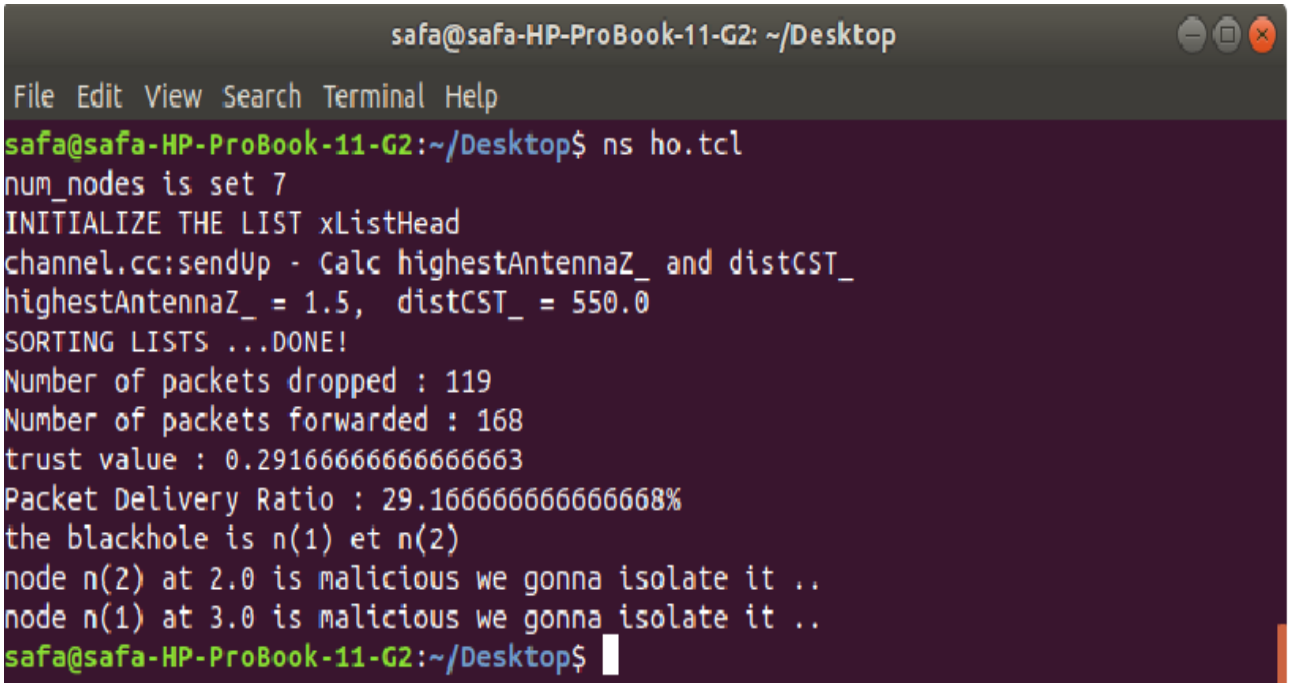

Figure 21: *Trust & PDR results in presence of one black hole attack*

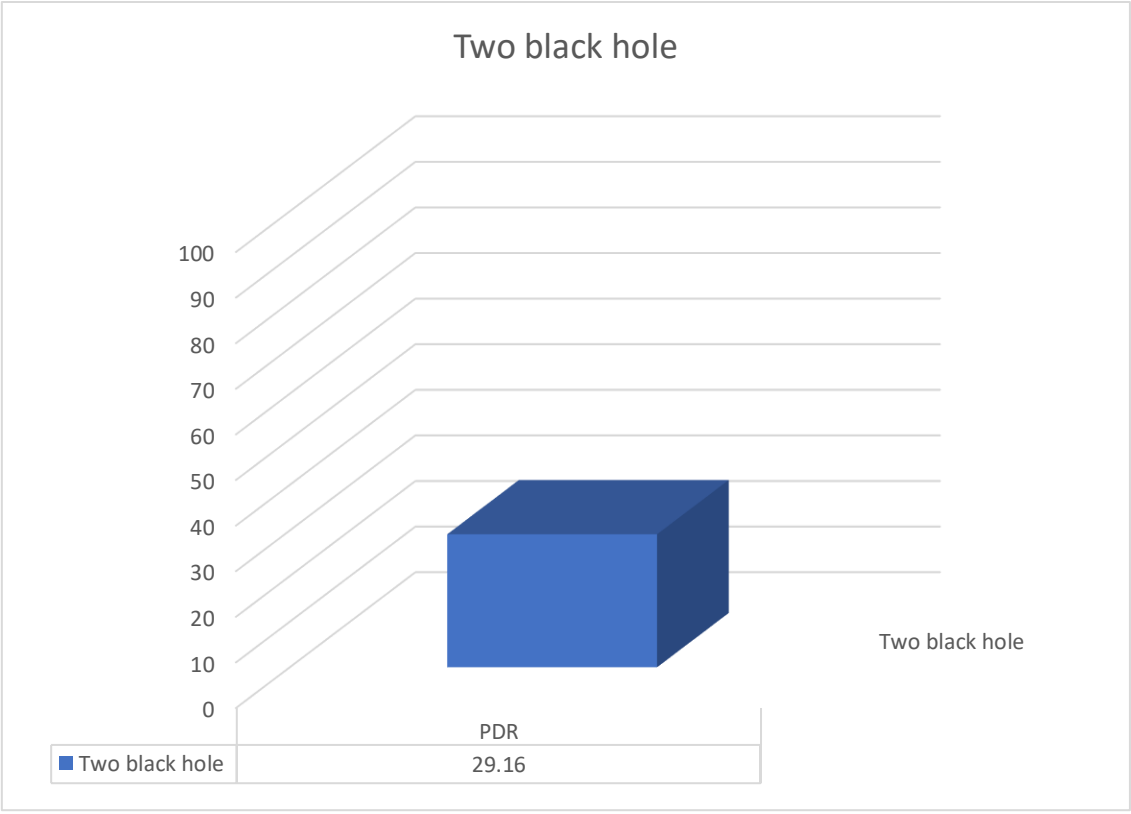

Figure 22: *PDR diagram in presence of two blackhole attack*

3.9.3 Using proposed approach:

The calculated trust level of a node is less than a predetermined threshold that means the presence of malicious presence of a malicious node, indicating a black hole attack. In this case, we can isolate the malicious node from the network to prevent further disruption.

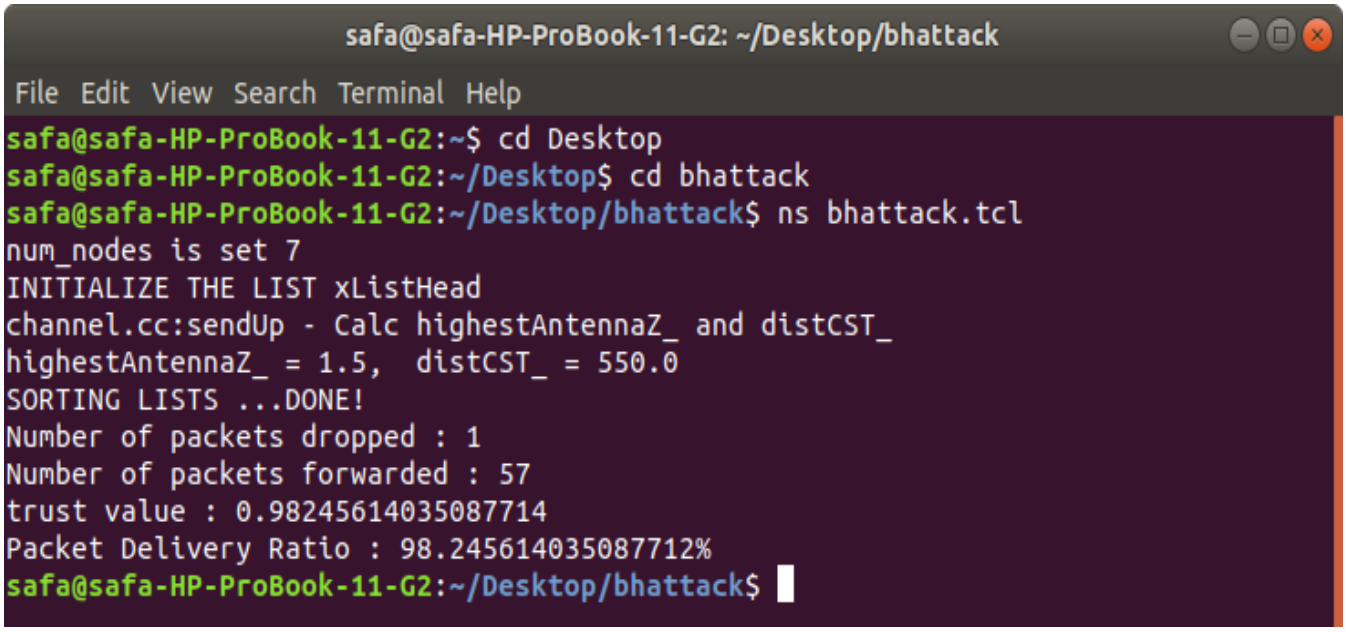

Figure 23: *Trust & PDR results after isolating malicious node*

The results of isolating the malicious node can be observed in the figure below, which will show an improvement in the packet delivery ratio (PDR)

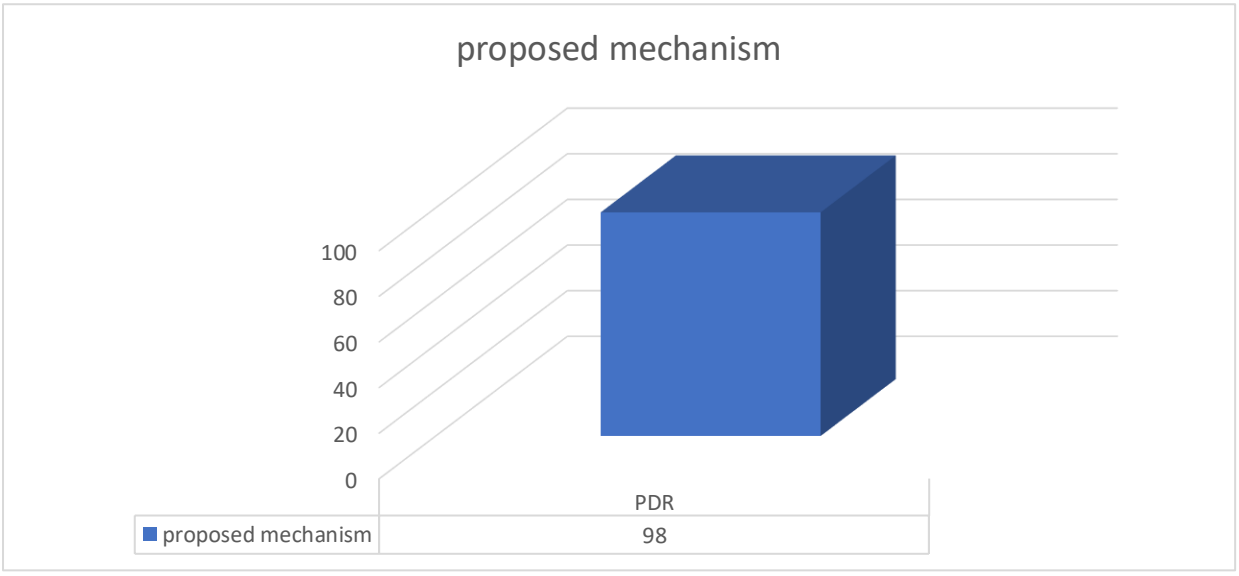

Figure 24: *PDR diagram in proposed mechanism*

Figure 25 illustrates a comparison of the packet delivery ratio (PDR) between the proposed mechanism and a scenario under a black hole attack. In the proposed mechanism, the trust level of each node is monitored and it reaches 1 when no packets are dropped.

It is clear from the figure that the proposed mechanism significantly reduces the number of dropped packets, resulting in an increased PDR.

In contrast, under a black hole attack, the PDR decreases significantly over time since the malicious node(s) drop or discard packets, causing disruption in the network. However, by detecting the presence of the black hole nodes using the trust-based mechanism, the malicious nodes can be isolated from the network, mitigating the impact of the attack and increasing the PDR .

In summary, the comparison in Figure 22 demonstrates that the proposed trust-based mechanism is effective in reducing the number of dropped packets and increasing the PDR compared to a scenario under a black hole attack.

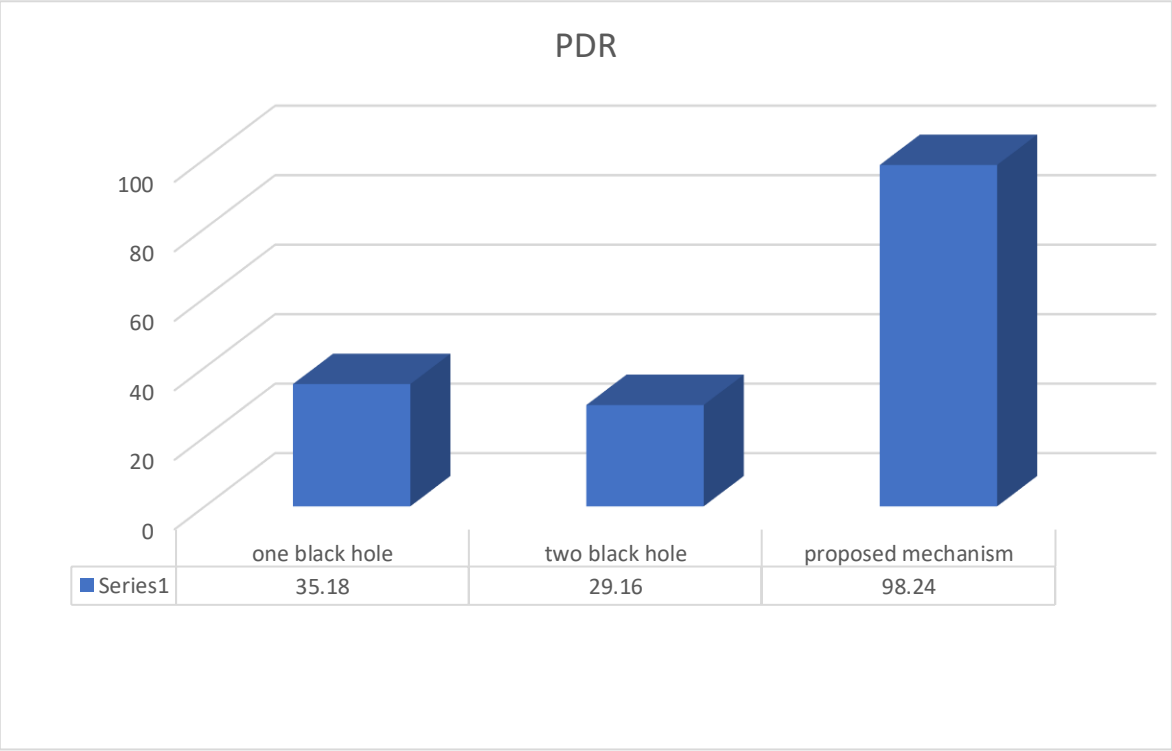

Figure 25:*comparison of the packet delivery ratio (PDR)*

3.10 Conclusion

After conducting a simulation, it is clear that a black hole attack can have a significant impact on the packet delivery rate in a FANET network. The attack disrupts communication by intercepting and dropping or discarding data packets, leading to a decrease in the packet delivery rate. However, with the proposed mechanism in place, it is possible to detect and prevent black hole attacks, leading to better transmission efficiency. The mechanism involves monitoring the behavior and communication history of each node in the network to calculate their trustworthiness. By analyzing the trust levels of each node, it is possible to identify any nodes with suspicious behavior and isolate the malicious node responsible for the black hole attack.

By preventing the black hole node from dropping or discarding packets, the proposed mechanism can significantly improve the packet delivery rate, ensuring the security and reliability of the FANET network. Therefore, it is crucial to detect and prevent black hole attacks using appropriate security mechanisms to maintain the performance and efficiency of the FANET network.

General Conclusion

FANETs, flying ad hoc networks, have emerged as a cutting-edge technique for reaching locations without enduring infrastructure FANETs are utilized in a variety of applications, including both military and civilian ones. As each type of network has its own specification and using the protocol depends on this specification, it is important to use a reliable protocol for this kind of networks. FANET Network face many challenges, one of the important challenges is security.

Security in the Flying Ad hoc Network is a very crucial challenge it needs constant attention to improve communication and ensure the security of data flow. Although some experts put out various security measures to guard against network intrusions, there is still a security gap that leaves systems open to various threats including black hole assaults. This work concludes a proposed mechanism based on trust management to detect black hole attack and isolate the malicious node. The proposed mechanism has been implemented in NS2 it had a very high performance and they were successful to detect black hole attack in the network.

In the future we plan to implement a real-time detection mechanism in FANETs can significantly enhance the security of the network by detecting and preventing attacks before they happen. A real-time detection mechanism involves applying the detection mechanism from the beginning of transmission in the FANET network to detect attacks before they happen and prevent them from occurring.

Overall, implementing a real-time detection mechanism in FANETs is a promising approach to enhance the security and reliability of the network. However, it requires further research and development to ensure that it is efficient, reliable, and suitable for various applications.

Bibliography

[1] A. Nadeem, Turki Alghamdi, A.Y. Mehmood, A. Siddiqui, M. Shoaib: A review and classification of Flying Ad Hoc Network (FANET) routing strategies. J. Basic Appl. Sci. Res. 8(3), 1–8 (2018). ISSN 2090-4304.

[2] I. Bekmezci, O. Sahingoz, Ş. Temel: "Flying ad-hoc networks (FANETs): A survey." Ad-Hoc Networks 11. No 3 1254-1270, 2013.

[3] A. Purohit, F. Mokaya, P. Zhang, "Collaborative indoor sensing with the sensor fly aerial sensor network", in: Proceedings of the 11th International Conference on Information Processing in Sensor Networks, IPSN, ACM, New York, NY, USA, pp.145–146,2012.

[4] M.Watfa "Advances in Vehicular Ad-Hoc Networks: Developments and Challenges: Developments and Challenges". IGI Global, 2010.

[5] Singh, A. K. "Applying OLSR routing in FANETs", "In Advanced Communication Control and Computing Technologies", (ICACCT), 2014.

[6] Cruz E. A comprehensive survey in towards to future FANETs. IEEE Latin America Transactions. 2018; 16(3):876-884

[7] Singh K, Verma AK. Flying ad hoc networks concept and challenges. In: Khosrow-Pour M DBA, editor. Advanced Methodologies and Technologies in Network Architecture, Mobile Computing, and Data Analytics. Hershey, PA: IGI Global; 2019. pp. 903-911. DOI: 10.4018/978-1-5225-7598-6.ch065

[8] Job Selection in a Network of Autonomous UAVs for Delivery of Goods [Internet]. 1999. Available from: https://arxiv.org/ftp/arxiv/papers/1604/1604.04180.pdf

[9] Yassein, M.B., Alhuda, N.: Flying Ad Hoc Networks: routing protocols, mobility models, issues. Int. J. Adv. Comput. Sci. Appl. (IJACSA) 7(6) (2016).

[10] Lalar, S., Yadav, A.K.: Comparative study of routing protocols in MANET. Orient. J. Comput. Sci. Technol. 10(1), 174–179 (2017). ISSN 0974-6471.

[11] Saranya, S., Chezian, R.M.: Comparision of proactive, reactive and hybrid routing protocol in manet. Int. J. Adv. Res. Comput. Commun. Eng. 5(7) (2016). ISSN (online) 2278-1021, IJARCCE, ISO 3297:2007 Certified.

[12] W.Zafar and Bilal Muhammad Khan, "Flying Ad-Hoc Networks", IEEE Technology and Society Magazine, june 2016.

[13] Sumra, Irshad Ahmed; Ahmad, Iftikhar; Hasbullah, Halabi; bin Ab Manan, Jamalul lail, Behavior of attacker and some new possible attacks in Vehicular Ad hoc Network (VANET), Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on, vol., no., pp.1-8, 5-7 Oct. 2011.

[14] Arun Kumar Yadav Karan Singh "Advanced Research in Computer Science and Software Engineering Evaluation of Security Threats and Solutions in MANET'S «International Journal Volume 6, Issue 2, February 2016

[15] Fida, N., Khan, F., Jan, M. A., & Khan, Z. (2016, September). Performance Analysis of Vehicular Ad hoc Network Using Different Highway Traffic Scenarios in Cloud Computing. In International Conference on Future Intelligent Vehicular Technologies (pp. 157-166). Springer.

[16] N.M Rodday, R.D Schmidt "Exploring securities vulnerabilities of unmanned aerial vehicles", "in IEE/IFIP Network Operations and management symposium", (NOMS), April 2016, pp.993-994.

[17] D. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks in Mobile Computing", (T. Imielinskiand H. Korth, eds.), Kluwere Academic Publishers.

[18] Singh, A. K. "Applying OLSR routing in FANETs", "In Advanced Communication Control and Computing Technologies", (ICACCT), 2014.

[19] Kim, A., Wampler, B., Goppert, J., Hwang, I., & Aldridge, H. (2012). Cyber-attack vulnerabilities analysis for unmanned aerial vehicles. In Infotech@ Aerospace (p. 2438).

[20] Mansfield, K., Eveleigh, T., Holzer, T. H., & Sarkani, S. (2013, November). Unmanned aerial vehicle smart device ground control station cyber security threat model. In 2013 IEEE International Conference on Technologies for Homeland Security (HST) (pp. 722–728). IEEE.

[21] Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized trust management. In Security and Privacy, 1996. Proceedings, 1996 IEEE Symposium on (pp. 164–173). IEEE.

[22] Perkings, C., E. Belding-Royer, S. Das: Ad hoc On-Demand Distance Vector (AODV) Routing. Ietf Rfc 3561 (2003)

[23] Shurman, M.A., Yoo, S.M., Park, S (ACMSE 2004): Black hole attack in wireless ad hoc networks. In: ACM 42nd Southeast Conference

[24] Mohammad. S, Obaidat Petros, Nicopolitidis; Faouzi, Zarai: Modeling and Simulation of Computer Networks and Systems ,2015.