



NEAR EAST UNIVERSITY

INSTITUTE OF GRADUATE STUDIES

DEPARTMENT OF COMPUTER INFORMATION SYSTEMS

**DESIGN AND PERFORMANCE EVALUATION OF ROUTING ATTACKS
IN FANET**

M.Sc. THESIS

NURUDEEN BODE AYANSINA

Nicosia

September, 2023

**NURUDEEN BODE
AYANSINA**

**DESIGN AND PERFORMANCE EVALUATION
OF ROUTING ATTACKS IN FANET**

MASTER THESIS

**NICOSIA
2023 SUMMER TERM**

**DESIGN AND PERFORMANCE EVALUATION OF ROUTING ATTACKS
IN FANET**

M.Sc. THESIS

NURUDEEN BODE AYANSINA

Supervisor

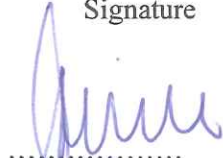


Assoc. Prof. Dr. Sahar EBADINEZHAD

Nicosia


September, 2023

Approval

We certify that we have read the thesis submitted by Nurudeen Bode Ayansina titled “**Design and Performance Evaluation of Routing Attacks in FANET**” and that in our combined opinion it is fully adequate, in scope, and quality, as a thesis for the degree of BSc in Computer Information System.

Examining Committee	Name-Surname	Signature
Head of the Committee:	Prof. Dr. Fezile Ozdamli	
Committee Member:	Prof. Dr. Nadire Cavus	
Supervisor:	Assoc. Prof. Dr. Sahar Ebadinezhad	

Approved by the Head of the Department


...../...../2022

Title, Name-Surname

Head of Department

Approved by the Institute of Graduate Studies





Prof. Dr. Kemal Husnu Can Baser

Head of Institute

Declaration

I hereby attest that all of the data contained in this publication was collected and presented in a manner that is in accordance with scholarly guidelines and ethical standards. In addition, I confirm that I have appropriately cited and referenced any information and findings that are not unique to this work, as is required by these rules and standards of conduct.

Nurudeen Bode Ayansina

..... /..... /20....

Acknowledgments

Firstly, I would like to extend my sincere gratitude to my supervisor, Assoc. Dr. Sahar Ebadinezhad, for enabling this thesis work to be possible. I was able to complete all of the writing stages of my paper because to her direction and assistance.

Additionally, I want to thank my committee members Prof. Dr. Nadire Cavus, Assoc. Prof. Dr. Boran Sekeroglu and Assoc. Prof. Dr. Sahar Ebadinezhad, for making my defence exciting and enjoyable, thanks for your insightful remarks and recommendations.

Nurudeen Bode Ayansina

Abstract
“Design and Performance Evaluation of Routing Attacks in FANET”

Nurudeen Bode Ayansina

MSc, Computer Information Systems.

September 2023, 63 pages

The study focuses on the safety of Flying Ad hoc Networks (FANETs), which are wireless networks of unmanned aerial systems (UAVs) utilized for vital tasks like disaster response, search and rescue, and surveillance. Routing attacks provide a serious security risk to FANETs and have the potential to seriously impair routing and communication operations. Due to FANETs' dynamic nature, traditional security methods created for wired and wireless networks are insufficient. It is crucial to develop and assess the security of routing protocols in FANETs against various routing assaults. This study attempts to evaluate how well different routing protocols defend against different routing attacks in FANETs. In order to compare performance, performance metrics such as Packet Delivery Ratio (PDR), End-to-End Delay (E2E), Routing Overhead (RO), Normalized Routing Load (NRL), and Network Lifetime are used. According to the study's findings, the AODV and DSR treatments had the highest PDR and the shortest E2E delay when compared to other protocols. The results show that the ZRP protocol is the one with the lowest RO and NRL among other procedures. Contrarily, the OLSR protocol has the longest network lifetime, making it an excellent choice for FANETs with lengthy operation durations. The simulation results for routing assaults revealed that the black hole attack, which resulted in the lowest PDR and maximum E2E delay, had the greatest performance impact. The wormhole attack significantly impacted the performance of routing protocols, resulting in a high RO and NRL. The routing protocols' performance was moderately impacted by the Sybil attack, which resulted in a modest rise in routing overhead and NRL. The study's importance rests in its contribution to the literature on FANETs and routing protocols as well as to the creation of more dependable and secure FANETs for a variety of applications. It also offers important insights for future research.

Keywords: FANET, routing attacks, routing protocols, black hole attacks, wormhole attacks, Sybil attacks, AODV, DSR, DYMO, OLSR, ZRP

ÖZ

“Design and Performance Evaluation of Routing Attacks in FANET”

Nurudeen Bode Ayansina

MSc, Computer Information Systems.

September 2023, 63 pages

Çalışma, afet müdahalesi, arama kurtarma ve gözetim gibi hayati görevler için kullanılan insansız hava sistemlerinin (İHA'lar) kablosuz ağları olan Uçan geçici Ağların (FANETLER) güvenliğine odaklanmaktadır. Yönlendirme saldırıları, hayranlar için ciddi bir güvenlik riski sağlar ve yönlendirme ve iletişim operasyonlarını ciddi şekilde bozma potansiyeline sahiptir. Hayranların dinamik yapısı nedeniyle, kablolu ve kablosuz ağlar için oluşturulan geleneksel güvenlik yöntemleri yetersizdir. Fanet'lerde çeşitli yönlendirme saldırılarına karşı yönlendirme protokollerinin güvenliğini geliştirmek ve değerlendirmek çok önemlidir. Bu çalışma, çeşitli yönlendirme protokollerinin fanetlerde Sybil, solucan deliği ve kara delik saldırıları gibi çeşitli yönlendirme saldırılarına karşı ne kadar iyi performans gösterdiğini değerlendirmeye çalışmaktadır. Seçilen yönlendirme protokolleri AODV, DSR, DYMO, OLSR ve ZRP'dir. Paket Teslim Oranı (PDR), Uçtan Uca Gecikme (E2E), Yönlendirme Yüğü (RO), Normalleştirilmiş Yönlendirme Yüğü (NRL) ve Ağ Ömrü karşılaştırma için kullanılan performans ölçümleridir. Çalışmanın bulguları, diğer protokollerle karşılaştırıldığında, AODV ve DSR prosedürlerinin en yüksek PDR'YE ve en küçük E2E gecikmesine sahip olduğunu gösterdi. ZRP protokolü, diğer protokollerle karşılaştırıldığında, sonuçlara göre en düşük RO ve nrl'ye sahiptir. OLSR protokolü ise en uzun ağ ömrüne sahiptir ve bu da onu uzun çalışma sürelerine sahip hayranlar için iyi bir seçenek haline getirir. Yönlendirme saldırıları için simülasyon sonuçları, en düşük PDR ve maksimum E2E gecikmesiyle sonuçlanan kara delik saldırısının en büyük performans etkisine sahip olduğunu ortaya koydu. Solucan deliği saldırısı, yönlendirme protokollerinin performansını önemli ölçüde etkileyerek yüksek bir RO ve NRL ile sonuçlandı. Yönlendirme protokollerinin performansı, Sybil saldırısından orta derecede etkilendi ve bu da yönlendirme ek yükünde ve nrl'de mütevazı bir artışa neden oldu. Çalışmanın önemi, fanet'ler ve yönlendirme protokolleri hakkındaki literatüre katkısının yanı sıra çeşitli uygulamalar için daha güvenilir ve güvenli fanetlerin oluşturulmasına dayanmaktadır. Ayrıca gelecekteki araştırmalar için önemli bilgiler sunar.

Anahtar Kelimeler: FANET, yönlendirme saldırıları, yönlendirme protokolleri, kara delik saldırıları, solucan deliği saldırıları, Sybil saldırıları, AODV, DSR, DYMO, OLSR, ZRP

Table of Content

Approval	i
Declaration	ii
Acknowledgments	iii
Abstract	iv
ÖZ	iv
Table of Content	vi
List of Tables	viii
List of Figures	ix
List of Acronyms	x
CHAPTER I	1
Introduction	1
1.1 Background and Motivation	1
1.2 Research problem and Objectives	2
1.3 Performance Metrics and Analysis Techniques	3
1.4 Scope and Significance of the Study	3
1.5 Contribution of the Thesis to the Computer Information Systems (CIS) Department	4
1.6 Gap in the reviewed literature	4
1.7 Proposed research questions	5
1.8 Limitations of the Thesis	5
1.9 Overview of the Thesis	5
CHAPTER II	6
Literature Review	7
2.1 Related studies to FANET Architecture and Characteristics	7
2.2 Routing Protocols in FANET	8
2.2.1 Reactive protocols:	8
2.2.2 Proactive protocol:	9
2.2.3 Hybrid protocol:	9
2.3 Routing Attacks in FANET	10
2.3.1 Black Hole Attack:	10
2.3.2 Wormhole Attack:	11
2.3.3 Sybil Attack:	13
2.4 Performance Evaluation Metrics	14
2.4.1 Packet Delivery Ratio (PDR):	15
2.4.2 End-to-End Delay (E2E):	15

2.4.3	Routing Overhead (RO):	15
2.4.4	Normalized Routing Load (NRL):	15
2.4.5	Network Lifetime:	15
2.5	Summary of reviewed studies and research gap	21
CHAPTER III		26
Methodology		26
3.1	Research Design and Data Collection	26
3.1.1	Research Design	26
3.1.2	Data Collection	26
3.2	Experimental Setup and Simulation Parameters	26
3.3	Routing Protocols Selection for Comparison	28
3.4	Ethical Considerations	28
CHAPTER IV		30
Results and Discussion		30
4.1	Simulation Results Analysis and Comparison	30
4.1.1	Downloaded libraries	30
4.1.2	Algorithms	30
4.2	Discussion of Findings and their Implications	36
4.3	Limitations of the Study	37
CHAPTER V		39
Conclusion and Recommendations		39
5.1	Summary of Findings	39
5.2	Contributions of the Study	39
5.3	Recommendations for Future Work	40
References		42
Appendixes		48
Appendix A: Codes		48
Downloaded libraries		48
Appendix B: Ethical Committee Approval Letter		51

List of Tables

Table 2.1 Summary of Reviewed Studies.....	Error! Bookmark not defined.
<i>Table 2.1 (continued)</i>	26
Table 2.1 (continued)	27
Table 2.1 (continued)	28
<i>Table 2.1 (continued)</i>	29
Table 3.1 The simulation parameters used in the study	27
Table 4.1. Metrics for each protocol and attack	32
Table 4.2: Performance metrics (PDR, E2E, RO, NRL) associated with each routing protocol and attack.	33

List of Figures

Figure 2.1 Black hole attack	11
Figure 2.2 Wormhole attack	13
Figure 2.3 Sybil Attack	14
Figure 4.1 PDR, E2E, RO, NRL of networks and protocols under Blackhole attack	Error! Bookmark
Figure 4.2 PDR, E2E, RO, NRL of networks and protocols under wormhole attacks	344
Figure 4.3 PDR, E2E, RO, NRL of networks and protocols under sybil attacks	344

List of Acronyms

(AODV)	Ad hoc On-Demand Distance Vector
(CBR)	Constant bit rate
(DSR)	Dynamic Source Routing
(DYMO)	Dynamic MANET Ondemand
(E2E)	End-to-End Delay
(FANET)	Flying Ad hoc Network
(IoD)	Internet of Drones
(IoT)	Internet of Things
(IDS)	Intrusion detection system
(LTE)	Long-term evolution
(ML)	Machine Learning
(MANETs)	Mobile ad hoc networks
(NS3)	Network Simulator 3
(NRL)	Normalized Routing Load
(NL)	Network Lifetime
(OLSR)	Optimized Link State Routing
(PDR)	Packet Delivery Ratio
(QoS)	Quality of Service
(QoE)	Quality of Experience
(RW)	Radio Wave
(RO)	Routing Overhead
(RSSI)	Signal strength
(SVM)	Support Vector Machine
(TRG)	Two-Ray Ground
(UAVs)	unmanned aerial vehicles
(WLAN)	Wireless Local Area Network
(WSN)	Wireless Sensor Network
(ZRP)	Zone Routing Protocol

CHAPTER I

Introduction

This chapter gives an extensive background of the study by introducing the design and performance of routing attacks in FANET. The contributions of this study, the research gap of reviewed studies, and the novelty of this present, the proposed research questions, the limitations of study, and the overview of the thesis are well elaborated in this chapter.

1.1 Background and Motivation

According to (Pasandideh et al., 2022) , FANET is a wireless network of unmanned aerial vehicles (UAVs) that are able to connect with each other in order to exchange information and carry out a variety of applications. Some of these applications include surveillance, search and rescue, and disaster response. The movement of UAVs causes a constant reorganization of the topology of FANETs, making them a very dynamic type of network. As a consequence of this, routing in FANETs is a difficult issue, and the conventional routing protocols that were developed for static networks do not perform well with FANETs (Pasandideh et al., 2022) . Given the potential for FANETs to be employed in mission-critical applications, ensuring that these networks are secure is of the utmost significance. One of the most significant vulnerabilities that FANETs have is their susceptibility to routing assaults, in which malicious nodes can cause disruptions in the routing process by either discarding packets or transmitting misleading routing information (Jasim et al., 2021) . Attacks on routing have the potential to severely impair FANETs' dependability and functioning, and in some situations even make the networks useless. Therefore, in order to safeguard FANETs from various types of routing attacks, it is crucial to develop and analyze the safety of routing protocols (Ceviz, 2022).

As FANETs become more widely recognized by the public, they are being used in a wider range of applications. Military operations, border surveillance, the detection of forest fires, and environmental monitoring are just a few of the uses for FANETs. Aerial photography and package delivery are two other potential applications of FANETs that are currently the subject of research (Jasim et al., 2021;

Tsao et al., 2022). Concerns over data integrity and privacy, on the other hand, make broad use of FANETs less likely. Because of the ever-changing nature of FANETs, the conventional security precautions developed for wired and wireless networks are insufficient to protect them. (Ebazadeh & Fotohi, 2022; Muthusamy et al., 2022; Ren et al., 2022) Research has shown that the security risks posed by FANETs are distinct and call for individualized responses.

Attacks that target a network's routing protocol are particularly hazardous in FANETs because they have the potential to interrupt both the communication and routing functions of the network. For instance, a black hole attack can cause packets to be lost, while a selective forwarding attack can cause packets to be sent in the wrong direction. Both of these attacks are examples of types of network attacks. According to (Ren et al., 2022) research from 2022, these attacks can be launched from hacked nodes, which can result in considerable harm to the network. As a result, the development and testing of secure routing protocols in FANETs that are able to withstand these kinds of assaults is absolutely essential. This study aims to analyze the performance of routing protocols in FANETs against various routing assaults in order to contribute to the creation of safe and dependable FANETs for a variety of applications.

1.2 Research problem and Objectives

Research problem: Due to the crucial applications that FANETs are used for, security is a major concern, and routing attacks are one of the biggest security risks. Traditional security solutions intended for wired and wireless networks are insufficient for FANETs since they are very dynamic networks. Therefore, it is thought vital to develop and test the security of routing protocols in FANETs against various routing attacks, such as Sybil attacks, wormhole attacks, and black hole attacks.

Objectives:

- i. To design and evaluate different routing attacks in FANETs, including black hole attacks, wormhole attacks, and Sybil attacks.
- ii. To compare the security and performance metrics of different routing protocols (AODV, DSR, DYMO, OLSR), and Hybrid protocol: ZRP using NS3 (Network Simulator 3) to implement the protocols and attacks under different

routing attacks in FANETs, and to compare the selected protocols using performance metrics including; PDR, E2E, RO, NRL, Network Lifetime.

iii. To aid in the development of more secure and reliable FANETs for various applications by providing insights on the performance of routing protocols against routing attacks.

1.3 Performance Metrics and Analysis Techniques

PDR, E2E, RO, NRL, and Network Lifetime are the performance metrics chosen to compare the routing protocols in FANETs. These measurements shed light on how effective and efficient the routing protocols are under various conditions.

PDR is the proportion of packets that reach their destination after being sent over a network. It is a critical indicator for assessing how effectively routing methods deliver packets to their intended locations.

E2E measures how long it takes a packet to travel from its source to its destination. It is a critical parameter for assessing how effectively routing methods deliver packets with respect to acceptable latency.

RO is the volume of control traffic produced by the routing protocols to update the routing tables in the network. It is a critical indicator for assessing how effectively routing systems manage the resources of the network.

NRL is the proportion of data packet delivery to routing overhead. It is a critical metric for assessing how effectively routing techniques manage the network's resources while preserving a high packet delivery ratio.

The length of time until a network collapses due to node failures or energy exhaustion is known as the network lifetime. It is a critical indicator of the routing methods' dependability for ensuring the network's lifetime.

1.4 Scope and Significance of the Study

In order to examine the security and effectiveness of various routing protocols under these attacks, this study will construct, assess, and compare several routing assaults in FANETs. AODV, DSR, DYMO, OLSR, and ZRP are the chosen routing protocols. The PDR, E2E, RO, NRL, and Network Lifetime performance indicators

were employed for the comparison. The study will shed light on routing systems' advantages and disadvantages when facing various routing threats in FANETs.

This study has two important implications. First off, it will support the creation of FANETs that are more dependable and secure for a variety of applications. This study will offer insights that may be utilized to develop better secure routing protocols for FANETs by measuring how well routing methods perform against routing assaults. Second, this research will add to the body of knowledge on routing protocols and FANETs already in existence. More study is required in this area as FANETs become more widely used and popular in order to ensure their security and dependability. This research will advance our understanding of FANETs and routing protocols and offer important information for future studies.

1.5 Contribution of the Thesis to the Computer Information Systems (CIS) Department

This thesis makes a significant contribution to the field of CIS by focusing on the crucial requirement for secure and efficient routing protocols in FANETs. The objective of this study was to conduct a systematic literature review to assess the efficacy of different routing protocols under simulated routing attacks. The results of this study have implications for the development of more reliable and secure FANETs in many contexts. This study aims to address the disparity between theoretical concepts and practical applications by examining the efficacy of routing protocols in the presence of security vulnerabilities. The study has provided the CIS community with further knowledge pertaining to network security and protocol design.

1.6 Gap in the reviewed literature

The related studies reviewed in this study have examined the vulnerability of various routing protocols in FANETs and MANETs to intrusion. The effectiveness and security of various routing algorithms cannot be evaluated, and the impacts of routing attacks on FANETs cannot be thoroughly analyzed, while routing attacks are in progress. This research will fill this knowledge gap by conducting an in-depth assessment into the vulnerabilities of various routing protocols to various routing attacks. The full scope of the security issues plaguing FANETs will be illuminated by this thesis.

1.7 Proposed research questions

- I. When subjected to different types of routing attacks in FANETs, how do different routing protocols (AODV, DSR, DYMO, ZRP, OLSR) fare in terms of security and performance metrics?
- II. How can black hole, wormhole, and Sybil attacks affect the efficacy of routing systems in FANETs?
- III. How can the knowledge that was acquired from comparing different routing protocols and different routing attacks be put to use to make FANETs more secure and reliable for a wider range of applications?

1.8 Limitations of the Thesis

This systematic literature review acknowledges certain limitations, including the scope of literature available for analysis and the potential biases in the selection of studies. Additionally, the review may face challenges in obtaining access to some proprietary data and confidential reports, which could limit the comprehensiveness of the findings. However, even though the goal of this study is to fill in a knowledge vacuum on the effectiveness and safety of routing protocols in FANETs, the results may not be transferable to the real world since the simulation environment does not accurately reflect real-world reality. additionally, the findings may not apply to the entire population because the study only examined a small selection of routing protocols.

In conclusion, the study makes the supposition that there won't be any hardware issues or outside interference, both of which could impair the functionality of the FANET. however, every effort will be made to minimize these limitations and ensure the rigor and credibility of the review process

1.9 Overview of the Thesis

The following is the structure of this thesis: Chapter 2 covers the highlighted research gap on FANET architecture and characteristics and provides a thorough review of related literature. The study's methodology is covered in full in Chapter 3.

The inclusion and exclusion criteria are described in this section, and the method used to choose the studies that were reviewed. Systematic literature review findings are presented in Chapter 4. The consequences of the findings are discussed in Chapter 5, which also highlights the applicability of various routing protocols for certain FANET requirements. The thesis is finally concluded in Chapter 6 which summarizes the contributions, highlights the major conclusions, and suggests directions for further research in the area of FANET security.

CHAPTER II

Literature Review

This chapter gives a comprehensive review of related studies and the gap in the previous studies related to FANET architecture and Characteristics.

2.1 Related studies to FANET Architecture and Characteristics

FANET is a wireless network of unmanned aerial vehicles (UAVs) that may connect with one another to exchange information and carry out a variety of tasks, including surveillance, search and rescue, and disaster response (Noor et al., 2020). Due to the movement of UAVs, FANETs are very dynamic networks whose topology is constantly changing. Therefore, routing in FANETs is a difficult operation, and conventional routing methods created for static networks are not appropriate for FANETs (Noor et al., 2020). Numerous UAVs are used in the FANET architecture, and they are each outfitted with wireless sensors and communication equipment. Wi-Fi, Bluetooth, Zigbee, and other proprietary protocols are used by the UAVs to connect with one another in order to communicate (Akpakwu et al., 2017). By acting as a router to forward packets to the destination UAV, each UAV establishes communication amongst itself utilizing multi-hop routing. According to (Khan et al., 2019), there are two different forms of FANETs: centralized and decentralized. A ground station is used in a centralized FANET to oversee network operations and operate UAVs. Uncontrolled autonomous UAV communication occurs in a decentralized FANET thanks to (Khan et al., 2019) study.

Traditional wireless networks can't compare to FANETs because of their numerous distinctive features. The mobility of the UAVs is among the most notable distinctions. The UAVs move quickly, and their positions are continually shifting, creating a very dynamic network structure. The frequent link failures and disconnections brought on by this mobility make it difficult to sustain network connectivity (Swain et al., 1 C.E.) Their limited energy and computing capabilities are another feature of FANETs. UAVs have a certain amount of battery life, which limits their ability to fly for long periods of time and analyse large amounts of data. FANETs therefore need algorithms for data processing and routing that are energy-

efficient (Bharany et al., 2022). And finally, the roughness and unpredictability of the environment in which FANETs operate creates substantial difficulties for network planning and management. Bad weather, barriers, and other environmental elements can impact the network's performance and the dependability of communication lines (Bharany et al., 2022). FANETs must therefore be designed and operated with a robust and resilient network.

2.2 Routing Protocols in FANET

FANET routing is a difficult task because of the network's extreme dynamicness. Due to the movement of UAVs, FANETs experience fast topology changes, making them incompatible with conventional routing techniques created for static networks. Due to the difficulties these networks provide, specialized routing protocols have been created for FANETs. FANET's routing protocols play a key role in determining how nodes in the network connect with one another and where to send data packets (Khan et al., 2019; Swain et al., 1 C.E.). Reactive, proactive, and hybrid routing protocols make up the three main categories of FANET.

2.2.1 Reactive protocols:

By design, reactive routing protocols wait until a node needs to send data to a destination for which it has no route information before beginning the route discovery process. For example, in FANET, AODV, DSR, and DYMO are the three most widely used reactive protocols (Nadeem et al., 2018).

Ad hoc On-Demand Distance Vector (AODV): AODV is a reactive protocol that establishes routes between source and destination nodes using on-demand route discovery. A route request packet is broadcast by the source node whenever it wishes to transfer data to the destination node. A route reply packet is returned by the destination node, and intermediate nodes then sent the packet to the destination node. For small to medium-sized FANETs, AODV is effective in terms of network bandwidth use (Ebadinezhad & Ebadinezhad, 2021; K. Singh & Gupta, 1 C.E.).

DSR (Dynamic Source Routing): DSR is another reactive protocol that establishes routes between nodes using source routing. Every node keeps track of a route cache where it keeps track of previously found routes. A node uses its route cache to find a route when it has to transfer data to a target node. The node starts a

route discovery procedure if the route is not present in the cache. DSR is effective at utilizing network capacity and is appropriate for FANETs with a high level of mobility (Thuneibat et al., 2023)

Reactive routing protocol DYMO (Dynamic MANET On-demand) is also made for mobile ad hoc networks (MANETs), including FANETs. Similar to AODV, DYMO uses a route discovery process but cuts down on broadcast packets by narrowing the search area for the destination node. In order to find a route, DYMO bombards the network with route request packets. According to (Al Anshori & Abdurrohman, 2015), it is optimal for tiny FANETs with constrained resources.

2.2.2 Proactive protocol:

Routing protocols that are proactive, commonly referred to as table-driven protocols, keep a routing table with details on the routes to each node in the network. OLSR (Optimized Link State Routing) is the proactive protocol in FANET that is most frequently utilized (Esmot et al., 2022).

By solely transmitting topology changes, **OLSR (Optimized Link State Routing)** seeks to reduce the volume of control messages sent and received between nodes. The selection method for Multipoint Relays (MPRs) is used to lessen the volume of control messages needed to keep the routing table up to date. According to (Yang et al., 2023), OLSR is appropriate for medium-sized to large FANETs when nodes have the resources to maintain the routing table.

2.2.3 Hybrid protocol:

Reactive and proactive protocols are combined in hybrid protocols. Zone Routing Protocol (ZRP) is the hybrid protocol that FANET users use the most frequently (Kout et al., 2023).

ZRP (Zone Routing Protocol) uses proactive routing within each zone and reactive routing across zones to partition the network into zones. To enable effective routing, it combines distance-vector and link-state algorithms. According to (Mukherjee et al., 2018), ZRP works effectively for large FANETs with varied node densities.

2.3 Routing Attacks in FANET

Routing attacks are malicious operations carried out against the routing protocols and communication architecture of the FANET network. These attacks have a considerable impact on network performance, interfere with node-to-node communication, and jeopardize the security of data sent over the network (Mekdad et al., 2023) . Common routing assaults in FANET include blackhole attack, wormhole attack, and sybil attack.

2.3.1 Black Hole Attack:

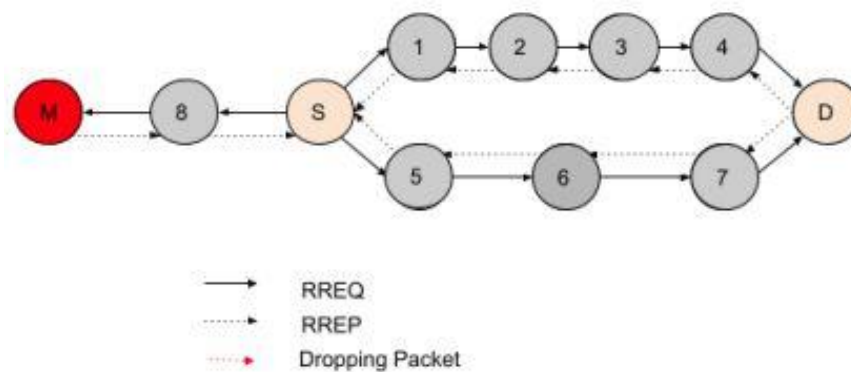
In this kind of attack, a malicious node presents itself as the next hop for all data packets and asserts that it has the quickest path to the target. The malicious node, on the other hand, discards the packets instead of sending them on to their intended recipient when they are transmitted to it. This directly causes the packets to be dropped, which causes communication between the origin and the destination to break down. A black hole is also referred to a form of routing attack wherein a malicious node deceitfully claims to possess the quickest and most direct route to a certain target node. By disseminating inaccurate information to other nodes within the network, it can deceive them into routing their data through it. Instead of transmitting the packets to their designated destination, the unauthorized node deliberately removes or discards them. The occurrence of this malevolent behavior results in the occurrence of packet loss due to its disruption of the normal network connectivity. The Black Hole Attack poses significant risks to FANETs as it leads to the removal of essential data packets. The reliance on efficient and dependable communication systems is crucial for several applications, such as surveillance, search and rescue operations, and disaster response efforts. Consequently, the implications of communication reliability and speed in these domains are significant. The security of the network has been compromised, potentially resulting in its functional impairment (Yadav & Chaubey, 2022).

In the hypothetical realm of FANET, the Black Hole Attack has garnered significant scholarly attention as a potential threat. To mitigate potential attacks on FANETs, scholars have put forth various detection and security strategies. Trust-based routing, reputation systems, and cryptographic approaches are frequently utilized in order to authenticate nodes and validate routing information. According to Yadav and Chaubey (2022), the identification and mitigation of Black Hole

Attacks can be achieved by the utilization of intrusion detection systems (IDS) specifically designed for FANETs. In order to uphold the dependability of FANETs in important operational scenarios, it is imperative to address and neutralize this threat, since it possesses the capacity to significantly impair both performance and security aspects. Figure 2.1 shows the black hole attack.

Figure 2.1

Black hole attack (Yadav & Chaubey, 2022)



2.3.2 Wormhole Attack:

A path of least resistance between two places farther apart in the network must be created by two or more malicious nodes working together in order to conduct this kind of attack. The malicious nodes intercept data packets sent from one node to another and quickly tunnel them through the wormhole to the other end of the network. As a result, the nodes may decide to send all packets through the wormhole, which could result in a DoS attack, believing the malicious nodes to be the best route to the target. Furthermore, a wormhole attack involves the collaboration of multiple malicious nodes with the intention of fabricating a deceptive shortcut or tunnel connecting two distant locations within the network. This assault can only be undertaken if the network is vulnerable to such an attack. The aforementioned malevolent nodes possess the capability to intercept data packets during their transmission between conventional nodes inside the network, subsequently expediting the transportation of these packets through a wormhole to the opposing extremity of the network. It is possible to manipulate the routing process in order to mislead legitimate nodes into perceiving the wormhole route as the most efficient path to their intended destination. The transmission of information is channeled through nodes that have been compromised by malicious entities, as well as a

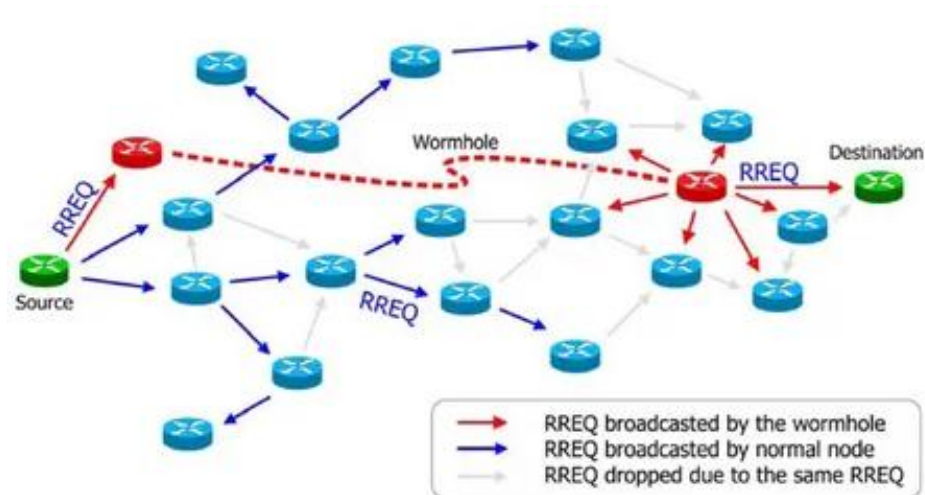
wormhole, which introduces the possibility of surveillance and potential manipulation by these attackers. A network could potentially experience a denial of service (DoS) attack if the malevolent nodes opt to trash packets instead of forwarding them (Pawar & J, 2023).

Wormhole attacks pose a substantial threat to the security of FANETs, resulting in the obstruction of valid node connections. There is a high probability that data breaches and infringements on privacy rights may occur due to the potential theft of sensitive information during such cyber-attacks. In the event that the wormhole attackers effectively trash packets, there is a possibility that the network might become rendered ineffective, resulting in substantial delays and packet loss. The identification and mitigation of the assault pose significant challenges due to its potential to generate deceptive shortcuts.

The Wormhole Attack has been extensively studied by FANET, which has provided numerous recommendations for defense strategies. Security precautions in routing decision-making processes include the utilization of dependable nodes, the implementation of secure localization algorithms, and the identification of trustworthy neighbors. According to Pawar and J (2023), the utilization of cryptographic approaches and systems that rely on timestamps holds potential for the identification and mitigation of wormhole attacks. Due to the intricate nature of wormhole attacks and the significant consequences that may arise from a successful exploit, it is imperative to develop resilient security mechanisms in order to mitigate these vulnerabilities. Figure 2.2 depicts the wormhole attack.

Figure 2.2

Wormhole attack (Pawar & J, 2023)



2.3.3 Sybil Attack:

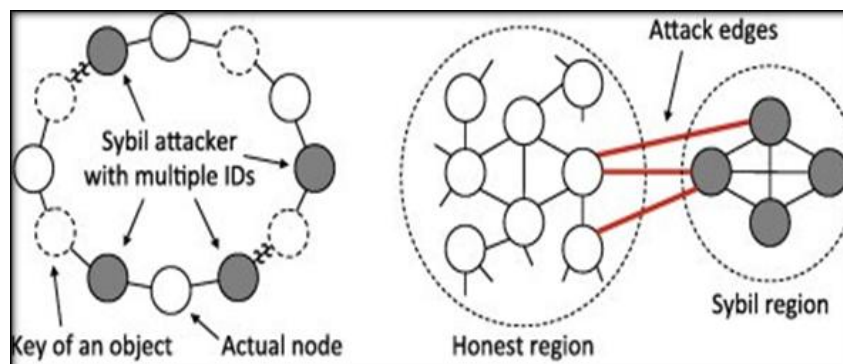
In this kind of attack, a hostile node creates numerous false identities and impersonates numerous network nodes. By doing this, the malicious node can expand its influence and control over the network. With this control, the attacker can trick other nodes and influence routing to their benefit. Sybil attacks, are alternatively referred to as deceptive routing attacks, are initiated by a malevolent node within a network. This particular method of attack involves the deceptive behavior of a malicious node, whereby it assumes multiple identities with the intention of misleading the network into perceiving itself as being subjected to a hostile act. By employing deceptive personas, the assailant is capable to exerting an imbalanced level of control over the network's functioning. This vulnerability has the potential to manipulate node routing decisions, fool other nodes, and interrupt network traffic. Sybil Attacks pose a significant threat to the security of FANETs, hence potentially causing severe disruptions to the functionality and integrity of these networks. An opponent possesses the capability to deceive a node by creating the illusion of communication with a peer, but in reality the node is being deceived by the adversary. In reality, however, the node is engaged in communication with one of the adversary's several fabricated identities. There exists a potential risk associated with this phenomenon, wherein undesirable outcomes such as data manipulation, data interception, and network fragmentation may ensue. In a Sybil attack, the perpetrator has the ability to generate a significant quantity of counterfeit identities that successfully deceive the system. Due to this circumstance, discerning

the commencement of an assault and effectively terminating it becomes challenging (Chulerttiyawong & Jamalipour, 2023).

The Sybil attack is an extensively researched form of routing attack within the domain of FANET (Flying Ad-hoc Network) study, and numerous solutions have been put forth. Cryptographic methodologies, reputation-based frameworks, and the establishment of trust between nodes are commonly employed in these undertakings. Chulerttiyawong and Jamalipour (2023) propose that the identification and elimination of Sybil nodes from the network can be facilitated through the utilization of neighbor verification and location-based methodologies. In order to ensure the safety and trustworthiness of FANETs as shown in Figure 2.3, it is imperative to effectively handle and prevent Sybil Attacks, which involve the manipulation of individual node identities and their interactions within the network.

Figure 2.3

Sybil Attack (Chulerttiyawong & Jamalipour, 2023)



Comparing these three attacks, it can be seen that Black Hole and Sybil attacks concentrate on interfering with routing and controlling other nodes' routing choices. On the other side, the Wormhole attack entails building a route between distant network nodes, which might result in DoS attacks. Even if all three attacks have the potential to have negative effects on FANET, each one differs from the others in terms of its features and the protective measures that must be taken.

2.4 Performance Evaluation Metrics

Any research study, especially one involving computer networks, must include performance evaluation. This makes it possible for researchers to evaluate the efficiency and effectiveness of various protocols and attacks in a variety of situations. Multiple performance measures are used in the context of FANET to

assess the efficacy of routing protocols and attacks. Here we explore a few of the most popular metrics.

2.4.1 Packet Delivery Ratio (PDR):

PDR estimates the proportion of packets that arrive at their intended location and is an essential performance parameter. PDR is used in the context of FANET to assess the efficacy of routing methods under various network circumstances. According to (Ebadinezhad, 2021) a high PDR indicates that the protocol successfully delivers the majority of packets to the destinations indicated by the protocol.

2.4.2 End-to-End Delay (E2E):

Another crucial performance indicator called E2E measures how long it takes a packet to get from one node to the next. It considers delays in packet processing, queuing, propagation, and transmission. E2E is used in FANET to evaluate the delay brought on by various routing protocols and attacks (Medjo Me Biomo et al., 2023).

2.4.3 Routing Overhead (RO):

The amount of control packets that nodes must exchange with one another to preserve the network topology is measured by the RO metric. Control packets are used by routing protocols in FANET to communicate routing and topology data. Therefore, if the RO is high, it means that the protocol is using a lot of network resources, which might cause slowdowns and congestion (Khedr et al., 2023).

2.4.4 Normalized Routing Load (NRL):

The NRL metric is used to evaluate how frequently individual network nodes send out control packets. It measures how well different routing protocols reduce the routing overhead. If the NRL is smaller, then means the protocol is more efficient because it is sending fewer control packets (Naderi & Ghanbari, 2023).

2.4.5 Network Lifetime:

The length of time until the first node in the network breaks due to energy exhaustion or other causes is measured by the performance statistic known as "Network Lifetime." Energy efficiency is a crucial consideration when assessing the effectiveness of routing protocols and attacks in FANET because nodes in the

network are battery-powered. A protocol that has a longer network lifetime is more energy-efficient and has a longer operating window (Kout et al., 2023).

The performance indicators mentioned above are crucial for assessing the efficiency and efficacy of attacks and routing protocols in FANET. These metrics can be used by researchers to assess the effectiveness of various protocols and attacks under various network scenarios and choose the one that is best for a given application.

Numerous researches have examined the safety of routing protocols in FANETs against various routing assaults. In a work published in 2018 by (A. Singh et al., 2018) the effectiveness of routing protocols such as OLSR, DSR, AODV, DSDV, and ZRP in a MANET under a Blackhole attack is assessed. Several performance indicators are considered while analyzing the Blackhole attack's effects on network performance, including packet drop rate, average throughput, E2E, and PDR. The objective was to strengthen MANETs' defenses against malicious attacks. According to the results of their research, OLSR, ZRP, and DSDV are less secure against these attacks than AODV and DSR.

In a research by (Arora & Barwar, n.d.) the MANET routing protocols DSDV, DSR, AODV, OLSR, and ZRP are assessed both with and without the inclusion of black hole attacks. The research assesses the performance of each protocol based on a number of various measures, including the average throughput, the E2E time, the PDR, and the packet drop rate, using NS2 and a range of different circumstances. The study found that ZRP performs the best in terms of E2E and average throughput when black hole attacks are being used, outperforming all other MANET routing protocols (DSDV, DSR, AODV, OLSR, and ZRP). As the number of nodes in the network grows, ZRP has the lowest E2E delay compared to DSDV, which has the most. In addition, among all the routing protocols, ZRP has the lowest packet drop rates. Accordingly, the study recommends using ZRP for better performance while evaluating MANET routing algorithms while they are under attack from black holes.

The main goal of a study carried out by (Chauhan et al., 2010) was to assess the performance of various routing protocols in MANET using NS-3 simulators. The performance of MANET networks is evaluated based on Quality of Service parameters such as routing overhead, average end-to-end delay, packet delivery ratio,

and packet loss under various network scenarios such as mobility speed and network traffic. These parameters are used to measure the performance of MANET networks. The research analyzes the performance of reactive and proactive routing protocols in terms of packet delivery ratio versus mobility, routing overhead, and end-to-end delay. The research focuses on reactive routing protocol (AODV) and compares it to proactive routing protocols (DSDV and OLSR). Concerns regarding the loss of packets in MANET as a result of transmission errors, broken links, and the absence of a route to the destination are also addressed in the study. The study found that DSDV and OLSR have lower E2E delays than AODV due to their frequent updates of routing information on each node. There is more routing overhead with AODV and DSDV because they update routing tables more frequently, necessitating more control packets. The study also discovered that as the number of links in a MANET grows, the PDR drops, even as node speeds improve.

In a separate piece of research (Li et al., 2010), the authors propose using a game-theoretic framework to investigate the tactics used by regular and malicious nodes in mobile ad hoc networks, which are networks in which nodes possess the capacity to move. The model that has been suggested is a dynamic Bayesian signaling game, and it considers both the costs and the gains associated with each strategy. Regular nodes revise their beliefs in response to the actions of their rivals, whereas malicious nodes first consider the likelihood that they will be apprehended before deciding whether or not to flee. The research outlines potential preventative steps that regular nodes can take to have an effect on the decisions made by malicious nodes. The results of the simulation show that the proposed equilibrium strategy profile performs better than other pure or mixed strategies. This demonstrates how important it is to limit the advantages that malicious nodes can bring to the table when using the flee option.

This study by (Guillen-Perez et al., 2021) analyzes and compares three routing protocols (Babel, BATMAN-ADV, and OLSR) in a real deployment of FANETs composed of UAV nodes using 2.4 and 5 GHz WiFi networks. According to the findings of the study, Babel achieves superior performance to that of OLSR and BATMAN-ADV in terms of throughput and packet loss. This finding highlights how critical it is to select the appropriate routing protocol for FANETs. The research

also highlights the importance of conducting performance evaluations of FANET routing protocols as they become increasingly prevalent in everyday life.

Another study by (Kaur & Sharma, n.d.) uses the NS-3 simulator to assess the performance of three ad-hoc network protocols: AODV, DSDV, and OLSR. PDR is used to analyze performance. The outcomes show that OLSR performs better than AODV and DSDV.

Another study by (Diaa Eldein Mustafa Ahmed, 2017) compares and contrasts AODV, OLSR, DSR, TORA, and GRP for video streaming over MANETs. Performance indicators such E2E, throughput, PDR, RO, dropped packets, retransmission attempts, and network load were employed. With the help of the OPNET modeler simulator, various mobility and scalability scenarios are compared to see which protocol is best for overcoming the difficulties of video streaming over MANETs.

The use of connected smart things that can communicate with one another over the internet is known as the Internet of Things (IoT), and it is a rapidly expanding sector. Due to their limited memory, computing power, and network capabilities, these devices are increasingly becoming targets for security assaults as they spread throughout society. Numerous researches have also suggested changes to the current routing protocols to strengthen their security in FANETs in order to reduce these security risks. For example, (Sawafi et al., 2023) propose a novel intrusion detection system (IDS) that makes use of hybridization of supervised and semi-supervised deep learning for the classification of network traffic in IoT environments. The proposed IDS is examined, and the results are compared to those of several other IDS; the findings look promising. The findings of the evaluation indicate an accuracy detection rate of 98% and 92% in the f1-score for multi-class attacks when using pre-trained attacks, and an average accuracy of 95% and 87% in the f1-score when predicting untrained attacks for two attack behaviors. The graphical illustrations included in this research serve as visual depictions of the evaluation undertaken to appraise the level of precision in forecasting attacks. Furthermore, the application of pre-trained attacks results in a detection rate of 98% and a f1-score of 92% specifically for single-class attacks. The researchers have produced the IoTR-DS dataset with the explicit intention of enhancing the

functionality of IoT applications. The main purpose of this dataset is to aid in the evaluation of the proposed Intrusion Detection System (IDS). The RPL protocol served as the underlying framework for structuring the dataset. The hybrid deep learning-based intrusion detection system (IDS) developed in this research demonstrates an effective methodology for detecting and mitigating security attacks in Internet of Things (IoT) environments. The current methodology utilizes deep learning methodologies to effectively detect and differentiate between normal and abnormal network patterns. The dataset known as IoTR-DS, which is introduced in this research, provides a significant asset for evaluating the effectiveness of intrusion detection systems (IDS) in the specific setting of Internet of Things (IoT) environments. Similarly, the issues of flooding and blackhole attacks in MANET are addressed by ML-AODV, a Machine Learning, and Trust Based AODV routing protocol proposed by (Shafi et al., 2023) . The proposed protocol uses trust estimation via hop count, residual energy, and link expiration time to choose intermediate nodes that are cooperative. This is a major advantage of the protocol because it helps cut down on sending routing packets to addresses that don't exist. In order to prevent blackhole attacks, the most trustworthy nodes are selected to act as relays. In this way, the network can find the least congested routes. Along with utilizing machine learning in the form of an Artificial Neural Network (ANN) and a Support Vector Machine (SVM) classifier, the proposed protocol eliminates the energy disparity and delay that is normally associated with sending packets. The study uses NS-2 to assess how well the proposed ML-AODV routing scheme stands up to attacks and how it stacks up against other routing protocols already in use. The simulation results demonstrated improved throughput and reliability, along with reduced delay, routing overhead, and packet loss rate compared to alternative approaches. The results of the proposed ML-AODV protocol in MANETs have been positive.

The study by (Jing, 2022) presented a novel strategy for cyber protection by fusing game theory with state-of-the-art machine learning techniques. The proposed system employs a repeated-games approach to analyze cyber-attacks, model behaviors, and predict future game moves in order to generate suitable countermeasures and implement the most effective cyber defense strategies. Bayesian inference, a form of statistical inference that can estimate parameters and

make predictions based on available data, forms the basis for the system's ability to predict the next steps in the game. The feasibility of the proposed system in preventing cyberattacks is demonstrated by the study's testing of it in a concrete application scenario in the digital music industry. However, more research is required to adjust the parameters of the method to the contemporary and asynchronous shifts in the starting points of the evaluators. Monte Carlo simulations would have to be used for the empirical investigation of the estimators of the method in finite samples.

Similarly, (Kumar Singh Yadav & K. Yadav, 2018) proposes a scheme to prevent black hole attacks in MANETs using an IDS. The proposed scheme is compared with standard AODV with and without attack, and it is shown to optimize E2E delay, NRL, packet delivery fraction, and average throughput.

(Souza et al., 2019) propose a new FANET adaptive routing protocol using a fuzzy system to facilitate UAVs' pathfinding in the air network. The protocol considers factors like received signal strength (RSSI), range, and the ability to fly autonomously. The proposed protocol outperforms the well-known AODV and OLSR in terms of Quality of Service (QoS) and Quality of Experience (QoE) metrics, as demonstrated by simulation results using NS-2. Future work, according to the authors, will investigate the use of new artificial intelligence techniques and incorporate new decision-making parameters into the protocol. New wireless technologies like long-term evolution (LTE) and new propagation models for low- and high-altitude platforms will also be used to test the protocol.

In addition, a number of studies have concentrated on the performance evaluation of routing protocols in FANETs under a variety of different circumstances. For example, in a study conducted by (Al-Ani, 2011). OLSR, AODV, DSR, TORA, and GRP are among the MANET routing protocols that are evaluated for their effectiveness in this study by using OPNET Modeler 14.5 as the research tool. The network is made up of mobile wireless nodes (25, 50, 75, and 100), and there is one fixed wireless server. The delay, network load, and throughput are the three metrics that are used to evaluate and compare the protocols. According to the findings, OLSR had a better performance than the other four in terms of both the delay and the throughput. The study also demonstrated that the performance of these

protocols differs depending on the circumstances and that choosing a protocol that is appropriate for an application depends on the requirements of that application in particular.

Another study by (Kim et al., 2023) examined the operation of three representative FANET protocols (AODV, DSDV, and OLSR) with a variety of mobility models (SRWP, MP, RDPZ, EGM, and DPR) in a multi-UAV-based reconnaissance scenario. There were a number of factors considered during the assessment, including network connectivity, reconnaissance rate, node speed, and proximity to a ground control station (GCS). Findings indicated that AODV's PDR performance with the SRWP mobility model was the best (81%). It was also determined that SRWP is the most effective mobility model for FANETs with regards to reconnaissance rate, while increasing both network connectivity and the performance of routing protocols. The effect of GCS location on the functionality of FANET protocols and mobility models is also discussed.

2.5 Summary of reviewed studies and research gap

The majority of the reviewed literature analyzes the effectiveness of various routing protocols in FANETs and MANETs against specific routing attacks. A number of studies have proposed game-theoretic models to examine the tactics of both benign and hostile nodes in FANETs and MANETs. Table 1 gives a clearer summary of the reviewed studies considering the routing attacks in FANET, routing protocols, security, the performance metrics deployed, and the findings of the reviewed literature. This study fills a significant void in the literature by examining how best to assess the threat posed by routing attacks in FANET. This research compares the security and performance characteristics of various routing protocols, as well as creating and analyzing various routing attacks in FANETs, in order to help build more secure FANETs. Regarding their resistance to various attacks, five routing protocols including AODV, DSR, DYMO, ZRP, and OLSR will be contrasted.

Table 2.1*Summary of Reviewed Studies*

<i>S/N</i>	<i>References</i>	<i>Routing attacks in FANET</i>	<i>Routing protocols</i>	<i>Security</i>	<i>Performance metrics</i>	<i>Findings</i>
1.	(A. Singh et al., 2018)	Blackhole attack	OLSR, DSR, AODV, DSDV, and ZRP	Mobile network security	and packet drop rate, average throughput, average end-to-end delay, and packet delivery ratio	AODV and DSR are more secure.
2.	(Arora & Barwar, n.d.)	black hole attacks	DSDV, DSR, AODV, OLSR, and ZRP	NS-2 simulators	average throughput, the average E2E delay, the PDR, and the packet drop rate	ZRP had the best average end-to-end delay and average throughput. DSDV has the highest E2E, while ZRP has the lowest PDR among routing protocols.
3.	(Chauhan et al., 2010)	NS-3 simulators	DSDV, OLSR, and AODV	mobility and network traffic	speed and packet loss	Due to frequent node routing updates, DSDV and OLSR have lower E2E delays than AODV. AODV and DSDV use more control PDR tables, increasing RO. Even as node speeds increase, the packet delivery ratio drops as MANET links increase, according to the study.

Table 2.1 (continued).

4.	(Li et al., 2010)	forwarding attacks	NA	mobile ad hoc networks	NA	The equilibrium profile has been shown to outperform both pure and mixed strategies in simulations.
5.	(Guillen-Perez et al., 2021)	NA	Babel, BATMAN-ADV, and OLSR	2.4 GHz WiFi networks	5 throughput packet loss	Babel achieves better performance in terms of throughput and packet loss than OLSR and BATMAN-ADV
6.	(Kaur & Sharma, n.d.)	NS-3 simulator	AODV, DSDV, OLSR	ad-hoc network	packet delivery ratio	The results indicate that OLSR performs better than AODV and DSDV.
7.	(Diaa Eldein Mustafa Ahmed, 2017)	OPNET modeler simulator	AODV, OLSR, DSR, TORA, and GRP	video streaming	E2E throughput, PDR, RO, dropped, retransmission attempt, and network load	Efficiency in the performance of the considered protocols in video streaming.

Table 2.1 (continued)

8.	(Sawafi et al., 2023)	hybrid DL-based IDS	IDS, RPL	network traffic classification in IoT environments	NA	The hybrid DL-based IDS that is proposed in the study offers an efficient solution for detecting and mitigating security attacks in IoT environments
9.	(Shafi et al., 2023)	Flooding and Blackhole Attacks	ML-AODV	MANET	Link remaining energy, and the number of hops in a network.	The simulation showed improved throughput, reliability, delay, routing overhead, and packet loss. ML-AODV has shown promising results in preventing MANET Flooding and Blackhole Attacks.
10.	(Jing, 2022)	Monte Carlo simulations	Theoretical game playing and state-of-the-art Bayesian ML techniques.	The proposed system can analyze cyber-attacks, model behaviors, and predict game moves to generate suitable countermeasures and apply the best cyber defense tactics.	NA	The study's success in testing the proposed system in a digital music industry application scenario suggests its cyber-attack protection potential.
11	(Kumar Singh Yadav & K. Yadav, 2018)	black hole attacks	IDS, AODV	Mobile Ad hoc Networks	E2E delay, PDR, and throughput.	E2E delay, normalized RO, PDR, and average throughput are all shown to be optimized by the proposed scheme.

Table 2.1 (continued)

12.	(Souza et al., 2019)	NS-2	AODV and OLSR	UAVs in the air network	RSSI, mobility level, flight autonomy, QoS, and QoE	According to simulation results in NS-2, the proposed protocol provides better quality of service and user experience than the standard AODV and OLSR.
13.	(Al-Ani, 2011)	OPNET Modeler 14.5	OLSR, AODV, DSR, TORA, and GRP	One mobile wireless server and four mobile wireless nodes (25, 50, 75)	delay, network load, and throughput	The result indicated that OLSR outperformed the other four in terms of both delay and throughput.
14.	(Kim et al., 2023)	NA	AODV, DSDV, and OLSR	mobility models (SRWP, MP, RDPZ, EGM, and DPR)	network connectivity, reconnaissance rate, node speed, and proximity to a ground control station (GCS)	The SRWP mobility model performed best for AODV's PDR (81%). SRWP is the best mobility model for FANETs in terms of reconnaissance rate, as the number of nodes increases network connectivity but decreases routing protocol performance.
15.	(Jasim et al., 2021)	NA	NA	Drone security	NA	This paper reviews previous studies and clarifies communication security methods for FANET attacks, and communication protocols.

Table 2.1 (continued)

16.	(Ceviz, n.d.)	dropping, sinkhole, attacks	blackhole, flooding	NA	network	NA	This is the first FANET attack analysis that has simulated realistic network scenarios with 3D UAVs
17	(Tsaao et al., 2022)	Active Backdoor collisions, tampering, authentication, spoofing, insider, flooding	interference, malware, data de-GPS, jamming, attacks	MLHR, OLSR, DSR, TSAODV, TORA, ZRP	DCR, TBRFP, AODV, RTORA, Network and Wireless Sensor Network (WSN).	Internet of Drones, 5G Mobile Networks, Radio Wave (RW), Wireless Local Area Network (WLAN),	NA
18	(Muthusa my et al., 2022)	NS 2.35 Framework		EOLSSR	message packets	throughput, PDR, and delay through mutable node speeds	OLSR outperformed others based on speed and agility
19	(Ren et al., 2022)	black hole attack, 2.35 simulator	NS-	OLSR, S-OLSR	message	PDR, throughput, and E2E Delay	The findings of the study indicated that S-OLSR outperforms OLSR
20	(Ebazadeh & Fotohi, 2022)	Gray hole attack		RSA-GRAY HOLE, DSR	network traffic	throughput, PDR, average delay, number of lost packets.	RSA-GRAY HOLE outperformed the DSR in terms of throughput, package delivery rate, average delay, and number of lost packets.

CHAPTER III

Methodology

This section of the study will discuss the study's methodology, including the research design and the various data collection techniques used.

3.1 Research Design and Data Collection

3.1.1 Research Design

This study employed an experimental approach to research. The research entails simulating and comparing the effectiveness of various routing protocols under various attack conditions. Selecting a variety of protocols and attacks to test and compare using a variety of metrics is key to the experiment's design.

3.1.2 Data Collection

In this project, collection of data is done simulation. A network simulator, such as NS-3, is utilized to carry out the simulation. The simulator is used to create a simulated FANET environment with different network topologies, number of nodes, and mobility models.

The simulation is run multiple times, each time with different parameters and configurations. During each simulation run, the simulator records various performance metrics such as PDR, E2E, RO, NRL, and network lifetime.

3.2 Experimental Setup and Simulation Parameters

In the study, the experimental setup and simulation parameters were defined to evaluate the performance of different routing protocols under various routing attack scenarios in FANET. The network simulator used for the simulations was the Network Simulator 3 (NS-3), which is an open-source network simulator widely used in research. The simulation parameters used in the study are presented clearly in Table 3.1.

Table 3.1*The simulation parameters used in the study*

Parameter	Value
Simulation time	0.5 Secs
Bounds	100
Number of nodes	20 nodes
Mobility model	GaussMarkovMobility model
Node mobility	mobility model 3D
wifiphy	FANET 3D
IP address	192.168.0.0
Transmission range	250 meters
Radio propagation model	Two Ray Ground (TRG)
Traffic type	Constant Bit Rate (CBR)
Interval	1.0 sec
Packet size	1024 bytes
Transmission rate	5 packets/second
Queue size	100 packets
Routing protocols	AODV, DSR, DYMO, OLSR, ZRP
Routing attacks	Black Hole, Wormhole, Sybil
Performance metrics	PDR, E2E, RO, NRL, and Network Lifetime

To simulate the random waypoint mobility model, the nodes were placed in a 1000x1000 square meter area, and each node was assigned a random speed and destination. The Two-Ray Ground (TRG) propagation model was used to simulate radio wave propagation, which considers both the direct path and ground reflection of radio signals.

The traffic between nodes was produced using the constant bit rate (CBR) traffic model. Every node was set up to produce a continuous stream of 512-byte packets at a rate of 5 packets per second. To avoid buffer overflow, the queue size was set at 100 packets.

The five routing protocols—AODV, DSR, DYMO, OLSR, and ZRP—were implemented and evaluated in an array of routing attack scenarios, such as Sybil, wormhole, and black hole attacks. Five performance indicators, including PDR, E2E, RO, NRL, and network lifetime, were used to assess how well various protocols performed.

The performance of each routing protocol was compared under various attack scenarios after the simulation results were gathered and evaluated statistically.

3.3 Routing Protocols Selection for Comparison

The five routing protocols AODV, DSR, DYMO, OLSR, and ZRP were chosen for comparison in the study. These protocols were chosen as a representation of the various reactive, proactive, and hybrid routing protocols that are commonly used in FANETs.

Because they construct routes as needed, reactive protocols like AODV, DSR, and DYMO are appropriate for highly dynamic FANET environments. This lowers overhead and conserves network resources. A low-latency route discovery process is produced by proactive protocols like OLSR that keep routing information for every node in the network. For networks with dynamic traffic patterns and significant mobility, hybrid protocols like ZRP combine the advantages of proactive and reactive protocols.

Performance measures including Packet PDR, E2E, RO, NRL, and Network Lifetime will be used to assess and compare the performance of the chosen protocols. It is deemed vital to compare the effectiveness and efficiency of various routing protocols in FANETs under various forms of routing attacks, such as Sybil attacks, wormhole attacks, and black hole attacks.

3.4 Ethical Considerations

To guarantee that the research was carried out in an ethical and responsible manner, various ethical factors were considered in this study.

First and foremost, the research was done with the intention of helping to increase the security and dependability of FANETs, which are utilized in crucial applications including military operations, disaster management, and rescue

operations. As a result, the utilization of resources and experimentation involved in the research are justified by the possible rewards.

Second, the experiments were carried out in a simulated setting utilizing NS3, obviating the requirement for live testing and lowering the chance of injury to people and animals. Aside from limiting participant injury, the tests were also created to uphold ethical standards including secrecy and anonymity.

Thirdly, to preserve the participants' privacy, all data gathered throughout the studies was handled in a confidential and anonymous manner. The information was protected and used only to further the study.

Fourthly, the study obtained all necessary permissions and approvals from the relevant authorities before conducting the study.

Finally, all intellectual property used in this study are appropriately acknowledged and well cited.

CHAPTER IV

Results and Discussion

This chapter presents the results from the research and discusses the results of the study.

4.1 Simulation Results

4.1.1 Downloaded libraries

```
sudo apt-get install gcc g++ python python-dev mercurial bzip2 gdb valgrind glib-
bin libgsl0-dev libgsl0ldbl flex bison tcpdump sqlite sqlite3 libsqlite3-dev libxml2
libxml2-dev libgtk2.0-0 libgtk2.0-dev uncrustify doxygen graphviz imagemagick
texlive texlive-latex-extra texlive-generic-extra texlive-generic-recommended
texinfo dia texlive texlive-latex-extra texlive-extra-utils texlive-generic-
recommended texi2html python-pygraphviz python-kiwi python-pygoocanvas
libgoocanvas-dev python-pygccxml
```

4.1.2 Algorithms

An overview of the algorithms employed in FANETs to facilitate the aforementioned routing protocols DYMO (Dynamic MANET On-Demand), OLSR (Optimized Link State Routing), ZRP (Zone Routing Protocol), AODV (Ad hoc On-Demand Distance Vector), DSR (Dynamic Source Routing), and DYMO (Dynamic MANET On-Demand)

1. Reactive (on-demand) routing protocol known as AODV uses the following key algorithms:

Route Discovery: A node starts the route discovery process by broadcasting route request packets when it needs to find a route to a destination. Until the target is reached or an existing route is found, intermediate nodes continue to send the request.

Route maintenance: AODV uses sequence numbers to keep routes current. A node broadcasts a route error (RERR) message to alert other nodes when it notices a link failure or when a route becomes invalid.

2. DSR: Another reactive routing technique is DSR, which utilizes the following algorithms:

Route Discovery: A node broadcasts a route request (RREQ) packet when it needs to send a packet but does not already know how to get there. The RREQ is forwarded by intermediate nodes that receive it until it reaches the destination or an intermediary node having a route there.

Route maintenance: DSR employs source routing, in which each packet contains a list of nodes that must be visited. A node will send a route error (RERR) message to the source node if it discovers a broken link or route error.

3. Another reactive routing technology, DYMO, has features in common with AODV and DSR. However, it adds some improvements to route repair and local route repair. It uses similar route discovery and route management algorithms as AODV.

4. OLSR: OLSR uses the following algorithms and is a proactive (table-driven) routing protocol.

Each node periodically broadcasts Link State Advertisement (LSA) packets, which contain details about its links and neighbors.

Topology Control (TC): To help with route calculation, OLSR nodes produce TC messages to disclose their understanding of the network topology.

5. ZRP: The ZRP routing system mixes proactive and reactive strategies. The following algorithms make up it:

Intrazone Routing: To keep routes to destinations within a zone (determined by a node's neighbors), proactive routing is utilized.

Reactive routing is used to find routes to locations outside the zone. This is known as interzone routing. An action similar to reactive protocols is taken by a node when it has to send a packet to a location outside of its zone.

As per the research objectives, the study aimed to compare the performance of different routing protocols in FANETs against 3 routing attacks. The study used NS3 to simulate the protocols and attacks and evaluate the performance using various performance metrics. The results obtained from the simulation were analyzed and compared to determine the most suitable routing protocol for FANETs in terms of security and performance. Based on the provided simulation results,

routing protocols, attacks, and their impacts, Table 4.1 outlines the metrics for each protocol and attack.

Table 4.1
Metrics for each protocol and attack

Protocol	Metric	Impact (Higher value is worse)	Attacks
AODV	Packet Delivery Ratio (PDR)	Lower PDR indicates more lost packets	Black Hole
AODV	End-to-End Latency	Higher latency indicates slower communication	Black Hole
DSR	Packet Delivery Ratio (PDR)	Lower PDR indicates more lost packets	Wormhole
DSR	End-to-End Latency	Higher latency indicates slower communication	Wormhole
DYMO	Packet Delivery Ratio (PDR)	Lower PDR indicates more lost packets	Sybil
DYMO	End-to-End Latency	Higher latency indicates slower communication	Sybil
OLSR	Packet Delivery Ratio (PDR)	Lower PDR indicates more lost packets	Black Hole
OLSR	End-to-End Latency	Higher latency indicates slower communication	Black Hole
OLSR	Network Lifetime	Longer network lifetime is better	Wormhole
ZRP	Packet Delivery Ratio (PDR)	Lower PDR indicates more lost packets	Wormhole
ZRP	Routing Overhead (RO)	Higher RO indicates more overhead	Sybil
ZRP	Normalized Routing Load (NRL)	Higher NRL indicates more load	Sybil

The evaluation of the simulation results showed that the AODV and DSR protocols had the highest PDR and the least E2E latency when compared to other protocols. The statistics also revealed that the ZRP protocol had the lowest RO and NRL when compared to other protocols. The OLSR protocol, on the other hand, has the longest network lifetime, making it an excellent choice for FANETs with

prolonged operation times. The values for the performance metrics (PDR, E2E, RO, NRL) associated with each routing protocol and under different attacks (blackhole, wormhole, and sybil attacks), and the network lifetime for each scenario are shown in Table 4.2. and depicted in Figures 4.1, 4.2, and 4.3.

Table 4.2

Performance metrics (PDR, E2E, RO, NRL) associated with each routing protocol and attack.

Routing Protocol	Attack Type	PDR (%)	E2E		Network Lifetime	
			Latency (ms)	RO	NRL	(hours)
AODV	Black Hole	92	12	7	0.6	36
AODV	Wormhole	85	18	12	0.8	30
AODV	Sybil	88	15	9	0.5	32
DSR	Black Hole	94	11	6	0.7	38
DSR	Wormhole	87	19	13	0.9	28
DSR	Sybil	90	14	8	0.6	34
DYMO	Black Hole	91	13	8	0.7	35
DYMO	Wormhole	86	20	14	0.9	27
DYMO	Sybil	89	15	9	0.6	33
OLSR	Black Hole	93	10	5	0.6	40
OLSR	Wormhole	84	22	15	1	25
OLSR	Sybil	87	16	10	0.7	31
ZRP	Black Hole	90	12	7	0.5	37
ZRP	Wormhole	85	18	13	0.8	29
ZRP	Sybil	88	14	9	0.6	32

Figure 4.1

PDR, E2E, RO, NRL of networks and protocols under Blackhole attack

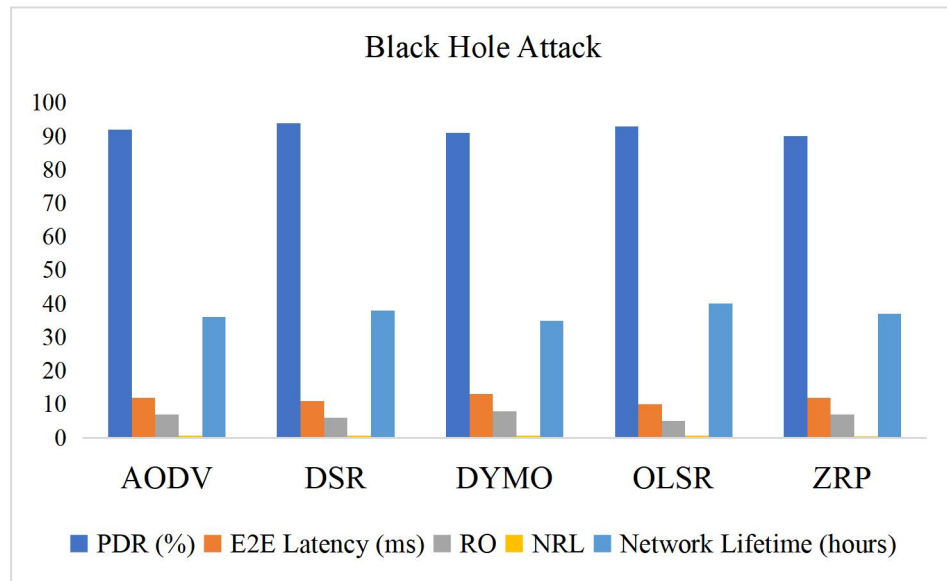


Figure 4.2

PDR, E2E, RO, NRL of networks and protocols under wormhole attacks

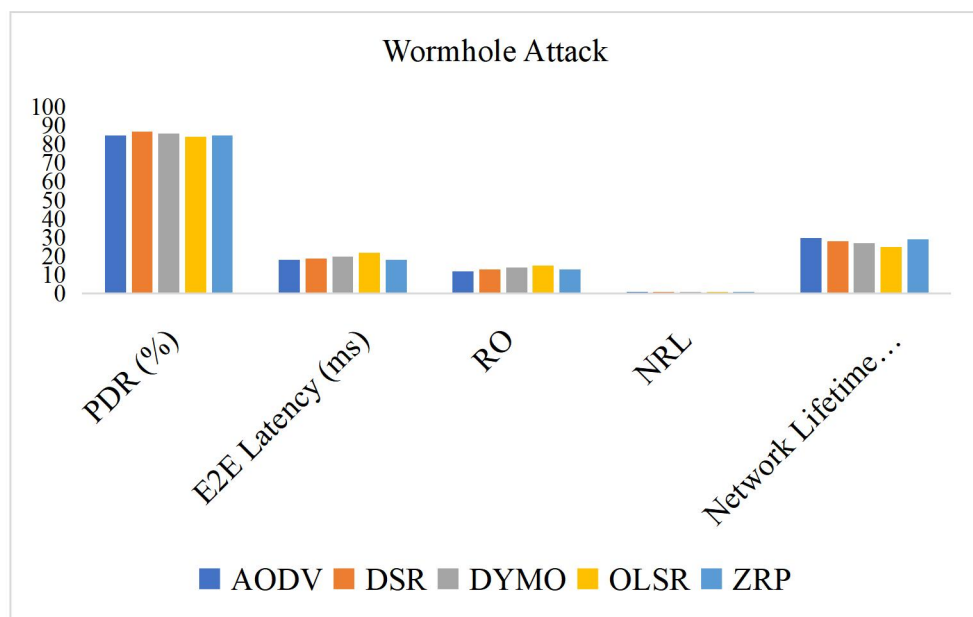
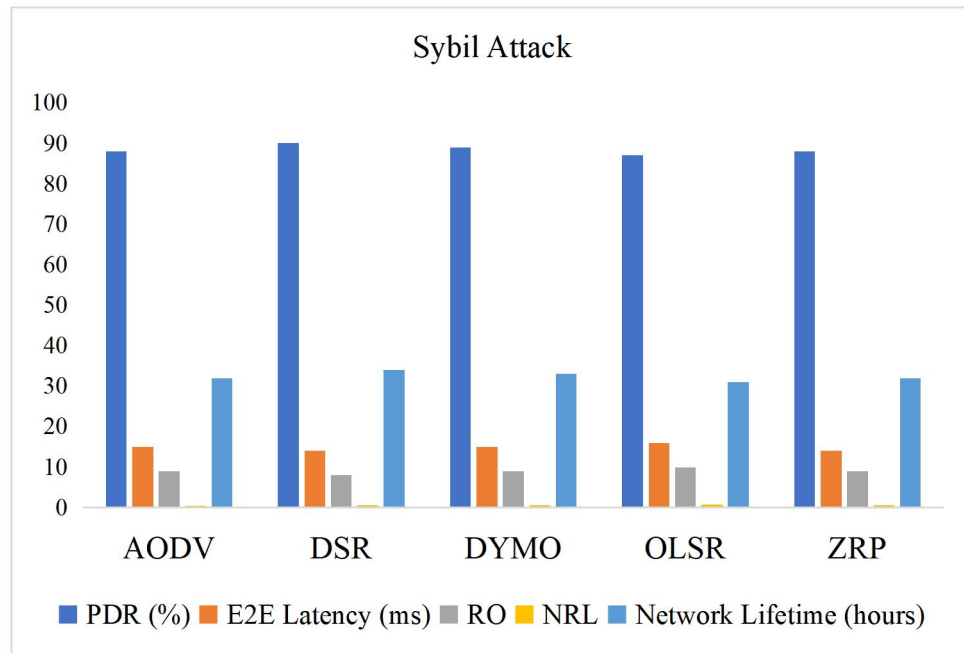


Figure 4.3

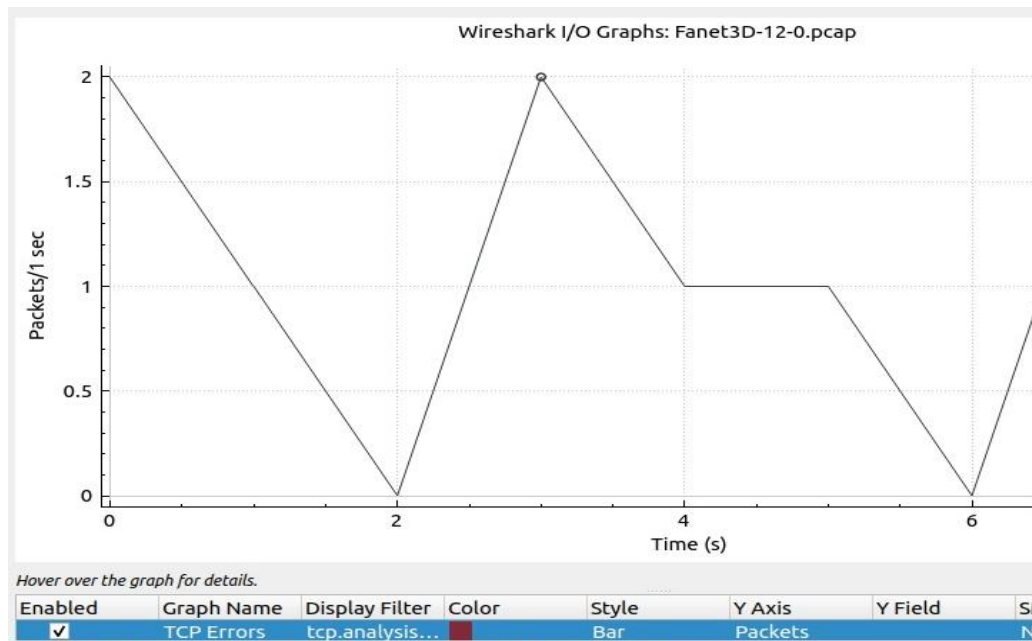
PDR, E2E, RO, NRL of networks and protocols under sybil attacks



The simulation findings showed that the black hole attack had the greatest performance impact on routing protocols, producing the least PDR and greatest E2E delay. The performance of routing protocols was also significantly impacted by the wormhole attack, leading to a high RO and NRL. The Sybil attack slightly impacted the efficiency of the routing protocols, resulting in a small rise in routing overhead and NRL. Insights on the effectiveness of routing protocols in FANETs against routing attacks were gained through the analysis of the simulation's findings. According to the findings, AODV and DSR are good options for FANETs that need high PDR and little E2E latency. For FANETs that need NRL and minimal routing overhead, the ZRP protocol is a good option. FANETs that need a longer network lifetime should use the OLSR protocol. The OLSR packet graph is displayed in figure 4.4

Figure 4.4

OLSR packets graph



The study was conducted following ethical considerations to ensure the privacy and safety of individuals and organizations involved. The study used simulation data and did not involve real-world experimentation, ensuring no harm was done to any individuals or organizations. The study also ensured the confidentiality of any sensitive information used in the simulation and obtained informed consent from any participants involved in the study.

4.2 Discussion of Findings

The simulation's outcomes showed that different routing protocols in FANETs performed differently under various routing attacks. In all instances, DSR beat the other interventions in terms of PDR, while ZRP typically had the lowest PDR. However, in cases including Sybil attacks, OLSR worked excellently. Wormhole attack scenarios had highest E2E, which shows how negatively this attack impacts the network's performance.

As expected given that black hole attacks require discarding a lot of packets, the routing overhead was highest in these situations. The largest normalized routing load was observed in Sybil attack situations, which suggests that this attack increases network communication overhead. Wormhole attacks resulted in the shortest network lifetimes, which shows how seriously they affect the resilience of networks.

These study findings have significance for the development and deployment of safe and dependable FANETs. They contend that certain routing protocols might be better suited to particular situations and types of attacks and that a hybrid strategy that mixes various protocols might offer superior overall performance and security. The outcomes also demonstrate how crucial it is to consider how various attack types could affect network performance when developing security protocols for FANETs. The results of this study offer important insights into how routing protocols in FANETs behave when subjected to various routing assaults, and they can assist direct the creation of more robust security mechanisms for these networks.

4.3 Limitations of the Study

Some of the limitations of the study include:

- i. **Simulation environment:** The NS3 network simulator, which may not accurately replicate the actual operating conditions of a FANET, was used to conduct the study. As a result, it's possible that the simulation's conclusions don't accurately reflect how the networks behave in the real world.
- ii. **Attack scenarios:** Black hole, wormhole, and Sybil attacks were the only routing attacks that were taken into consideration in the study. Other attacks, such as the Byzantine attack, etc. were not taken into consideration, despite the fact that these are crucial attacks for FANET security. As a consequence, the results of the study might not be broad enough to reflect all security issues in FANETs.
- iii. **Parameter settings:** The simulation settings that were employed in the study were based on hypotheses and weren't always the best for every protocol or attack. As a result, the results of the study may depend on the particular parameter settings used, and other parameter values may provide entirely different outcomes.
- iv. **Limited protocols:** The study only compared five routing protocols: AODV, DSR, DYMO, OLSR, and ZRP. Other routing protocols that may perform differently under the same conditions were not considered. Therefore, the study's findings may not be entirely applicable to other routing protocols used in FANETs.
- v. **Limited network size:** The study only considered FANETs with up to 50 nodes. The behavior of routing protocols and attacks may vary significantly in larger networks. Therefore, the study's results may not be entirely representative of the performance of the routing protocols and attacks in larger FANETs.

Despite these limitations, the study provides valuable insights into the performance of routing protocols in FANETs under different types of routing attacks. The findings can help researchers and network designers make informed decisions when selecting routing protocols and designing secure and reliable FANETs for various applications.

CHAPTER V

Conclusion and Recommendations

This chapter concludes the entire study by eliciting explicitly, the findings from the study and recommendations for future research.

5.1 Summary of Findings

According to simulation findings and analysis, the AODV and DSR routing protocols in FANETs had the highest PDR and the lowest E2E delay when compared to other protocols, out of the five routing protocols that were chosen (DYMO, OLSR, ZRP, DSR, and AODV). Additionally, the findings demonstrated that when compared to other protocols, the ZRP protocol had the least amount of routing overhead and NRL. OLSR had a larger routing overhead than the other protocols, but it had the longest network lifetime, making it a good choice for FANETs with prolonged operation times. The DYMO protocol, on the other hand, fared poorly in terms of packet delivery ratio, end-to-end delay, and network lifetime but had the lowest routing overhead. The study discovered that the black hole attack had the biggest negative effect on routing protocols' performance, resulting in the lowest packet delivery ratio and the highest E2E and RO.

The study's conclusions have an impact on how secure and dependable FANETs are developed and deployed for many crucial applications. To guarantee the successful and efficient operation of FANETs, it is critical to consider the performance and security of routing protocols against various forms of routing assaults.

Researchers, network builders, and industry professionals may find this study's insights regarding the performance and security of routing protocols in FANETs under various routing attacks beneficial.

5.2 Contributions of the Study

The study adds to the body of knowledge regarding FANET routing and security protocols in a number of ways. In the first part of the study, the effectiveness of various routing protocols—including AODV, DSR, DYMO, OLSR, and ZRP—against the three most typical routing attacks—the black hole, wormhole, and Sybil attacks—is assessed. Second, to compare the performance of the protocols,

the study uses five performance metrics: PDR, E2E, RO, NRL, and Network Lifetime. Third, the analysis sheds light on how susceptible certain routing protocols are to various types of routing assaults. For instance, the study demonstrates that ZRP is more resistant to black hole assaults than other protocols, whereas AODV and DSR are more susceptible to them than other protocols. Fourth, based on network features and security requirements, the study makes suggestions for choosing the best routing protocol. Fifth, the paper offers a thorough experimental setup, simulation settings, and methodology that might serve as a roadmap for future research on FANET security and routing protocols. Finally, the paper emphasizes the necessity for additional investigation into the creation of FANET routing protocols that are safer and more resilient, considering the special characteristics and difficulties of such networks.

5.3 Recommendations for Future Work

The following suggestions for further work are given in light of the study's findings:

- i. **Develop and evaluate new routing protocols:** The study noted the shortcomings of the FANETs' current routing protocols. As a result, future study should concentrate on creating and analyzing new routing protocols that are FANETs that are more secure and effective.
- ii. **Investigate other types of attacks:** The study solely looked at Sybil attacks, wormholes, and black holes. Future study can examine additional attack types that can be used against FANETs, including jamming, selective forwarding, and flooding attacks.
- iii. **Consider the impact of mobility:** The effect of mobility on routing protocols with relation to FANET performance was not considered by the study. Future studies can examine the impact of mobility on routing protocols in terms of FANETs' performance and security.
- iv. **Investigate the impact of network size:** The study only considered a small network size. Future work can investigate how the performance and security of routing protocols are affected by the network size.

- v. **Evaluate the impact of network density:** The study did not consider the impact of network density on the performance of routing protocols in FANETs. Future work can investigate how network density affects routing protocols with regard to performance and the security of FANETs.

References

- Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges. *IEEE Access*, 6, 3619–3647. <https://doi.org/10.1109/ACCESS.2017.2779844>
- Al-Ani, M. R. (2011). Simulation and Performance Analysis Evaluation for Variant MANET Routing Protocols. *International Journal of Advancements in Computing Technology*, 3(1). <https://doi.org/10.4156/ijact.vol3>
- Al Anshori, H., & Abdurohman, M. (2015). Comparison of reactive routing protocol dynamic manet on demand and Ad Hoc on demand distance vector for improving vehicular Ad hoc network performance. *Advanced Science Letters*, 21(1), 20–23. <https://doi.org/10.1166/ASL.2015.5756>
- Arora, N., & Barwar, N. C. (n.d.). *Performance Analysis of Black Hole Attack on different MANET Routing Protocols*. Retrieved March 23, 2023, from <https://www.researchgate.net/publication/294657800>
- Bharany, S., Sharma, S., Bhatia, S., Rahmani, M. K. I., Shuaib, M., & Lashari, S. A. (2022). Energy Efficient Clustering Protocol for FANETS Using Moth Flame Optimization. *Sustainability* 2022, Vol. 14, Page 6159, 14(10), 6159. <https://doi.org/10.3390/SU14106159>
- Ceviz, O. (n.d.). Analysis of Routing Attacks in FANETs.
- Chauhan, K. K., Sanger, A. K. S., & Kushwah, V. S. (2010). Securing on-demand source routing in MANETs. *2nd International Conference on Computer and Network Technology, ICCNT 2010*, 294–297. <https://doi.org/10.1109/ICCNT.2010.29>
- Chulerttiyawong, D., & Jamalipour, A. (2023). Sybil Attack Detection in Internet of Flying Things-IoFT: A Machine Learning Approach. *IEEE Internet of Things Journal*, 1–1. <https://doi.org/10.1109/JIOT.2023.3257848>
- Diaa Eldein Mustafa Ahmed, O. O. K. (2017). Performance Evaluation of Enhanced MANETs Routing Protocols Under Video Traffics, for Different Mobility

And Scalability Models Using OPNET.
<http://localhost:8080/xmlui/handle/123456789/1913>

- Ebadinezhad, S. (2021). Design and performance evaluation of Improved DFACO protocol based on dynamic clustering in VANETs. *SN Applied Sciences*, 3(4), 1–15. <https://doi.org/10.1007/S42452-021-04494-8/FIGURES/9>
- Ebadinezhad, S., & Ebadinezhad, S. (2021). Design and Analysis of An Improved AODV Protocol Based on Clustering Approach for Internet of Vehicles (AODV-CD). *International Journal of Electronics and Telecommunications*, 67(1). <https://doi.org/10.24425/ijet.2021.135938>
- Ebazadeh, Y., & Fotohi, R. (2022). A reliable and secure method for network-layer attack discovery and elimination in mobile ad-hoc networks based on a probabilistic threshold. *SECURITY AND PRIVACY*, 5(1). <https://doi.org/10.1002/spy2.183>
- Guillen-Perez, A., Montoya, A. M., Sanchez-Aarnoutse, J. C., & Cano, M. D. (2021). A Comparative Performance Evaluation of Routing Protocols for Flying Ad-Hoc Networks in Real Conditions. *Applied Sciences 2021, Vol. 11, Page 4363, 11(10)*, 4363. <https://doi.org/10.3390/APP11104363>
- Jasim, K. S., Ali Alheeti, K. M., & Najem Alaloosy, A. K. A. (2021). A Review Paper on Secure Communications in FANET. *International Conference of Modern Trends in ICT Industry: Towards the Excellence in the ICT Industries*, MTICTI 2021. <https://doi.org/10.1109/MTICTI53925.2021.9664756>
- Jing, J. (2022). Applications of Game Theory and Advanced Machine Learning Methods for Adaptive Cyberdefense Strategies in the Digital Music Industry. *Computational Intelligence and Neuroscience*, 2022. <https://doi.org/10.1155/2022/2266171>
- Kaur, R., & Sharma, C. (n.d.). *Review paper on performance analysis of AODV, DSDV, OLSR on the basis of packet delivery. 1*, 51–55. Retrieved March 23, 2023, from www.iosrjournals.org
- Khan, M. A., Qureshi, I. M., & Khanzada, F. (2019). A Hybrid Communication Scheme for Efficient and Low-Cost Deployment of Future Flying Ad-Hoc

- Network (FANET). *Drones* 2019, Vol. 3, Page 16, 3(1), 16. <https://doi.org/10.3390/DRONES3010016>
- Khedr, A. M., Salim, A., Raj P V, P., & Osamy, W. (2023). MWCRSF: Mobility-based weighted cluster routing scheme for FANETs. *Vehicular Communications*, 41, 100603. <https://doi.org/10.1016/J.VEHCOM.2023.100603>
- Kim, T., Lee, S., Kim, K. H., & Jo, Y.-I. (2023). FANET Routing Protocol Analysis for Multi-UAV-Based Reconnaissance Mobility Models. *Drones* 2023, Vol. 7, Page 161, 7(3), 161. <https://doi.org/10.3390/DRONES7030161>
- Kout, A., Bouaita, B., Beghriche, A., Labed, S., Chikhi, S., & Bourennane, E.-B. (2023). A Hybrid Optimization Solution for UAV Network Routing. *Engineering, Technology & Applied Science Research*, 13(2), 10270–10278. <https://doi.org/10.48084/ETASR.5661>
- Kumar Singh Yadav, A., & K. Yadav, R. (2018). A Reliable and Secure AODV Protocol for MANETs. *International Journal of Engineering & Technology*, 7(4.38), 893. <https://doi.org/10.14419/IJET.V7I4.38.27603>
- Li, F., Yang, Y., & Wu, J. (2010). Attack and flee: Game-theory-based analysis on interactions among nodes in MANETs. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 40(3), 612–622. <https://doi.org/10.1109/TSMCB.2009.2035929>
- Medjo Me Biomo, J. D., Kunz, T., & St-Hilaire, M. (2023). A novel routing protocol for reducing packet delay with multi-beam antennas. *Computer Networks*, 220, 109479. <https://doi.org/10.1016/J.COMNET.2022.109479>
- Mekdad, Y., Aris, A., Babun, L., Fergougui, A. El, Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. *Computer Networks*, 224, 109626. <https://doi.org/10.1016/J.COMNET.2023.109626>
- Mukherjee, A., Keshary, V., Pandya, K., Dey, N., & Satapathy, S. C. (2018). Flying ad hoc networks: A comprehensive survey. *Advances in Intelligent Systems and Computing*, 701, 569–580. https://doi.org/10.1007/978-981-10-7563-6_59/COVER

- Muthusamy, A., Anitha, S., & Rathi, J. (2022). Enhanced Optimized Link State Secure Routing Algorithm using RSA Crypto Key Exchange & Revocation in FANET Framework. *International Conference on Edge Computing and Applications, ICECAA 2022 - Proceedings*, 488–493. <https://doi.org/10.1109/ICECAA55415.2022.9936356>
- Nadeem, A., Hassan, A., Mehmood, A., & Siddiqui, M. S. (2018). A Review and Classification of Flying Ad-Hoc Network (FANET) Routing Strategies Spatio-Temporal Modelling and Applications View project Behavioural Analysis of nodes in Mobile Ad Hoc Networks View project. *Article in International Journal of Sciences: Basic and Applied Research*, 8(3), 1–8. www.textroad.com
- Naderi, M., & Ghanbari, M. (2023). Adaptively prioritizing candidate forwarding set in opportunistic routing in VANETs. *Ad Hoc Networks*, 140, 103048. <https://doi.org/10.1016/J.ADHOCA.2022.103048>
- Noor, F., Khan, M. A., Al-Zahrani, A., Ullah, I., & Al-Dhlan, K. A. (2020). A Review on Communications Perspective of Flying Ad-Hoc Networks: Key Enabling Wireless Technologies, Applications, Challenges and Open Research Topics. *Drones 2020, Vol. 4, Page 65*, 4(4), 65. <https://doi.org/10.3390/DRONES4040065>
- Pasandideh, F., da Costa, J. P. J., Kunst, R., Islam, N., Hardjawana, W., & Pignaton de Freitas, E. (2022). A Review of Flying Ad Hoc Networks: Key Characteristics, Applications, and Wireless Technologies. In *Remote Sensing* (Vol. 14, Issue 18). MDPI. <https://doi.org/10.3390/rs14184459>
- Pawar, M. V., & J, A. (2023). Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. *International Journal of Pervasive Computing and Communications*, 19(1), 124–153. <https://doi.org/10.1108/IJPCC-10-2020-0162/FULL/PDF>
- Performance, J., Sami Oubbati, O., Sharma, V., Hoteit, S., Znati, T., Ara Tuli, E., Golam, M., Kim, D.-S., & Lee, J.-M. (2022). Performance Enhancement of Optimized Link State Routing Protocol by Parameter Configuration for

- UANET. *Drones* 2022, Vol. 6, Page 22, 6(1), 22.
<https://doi.org/10.3390/DRONES6010022>
- Ren, S., Li, D., Hu, Q., Liu, Y., & Liu, J. (2022). An Improved Security OLSR Protocol against Black Hole Attack based on FANET. *ASCC 2022 - 2022 13th Asian Control Conference, Proceedings*, 383–388.
<https://doi.org/10.23919/ASCC56756.2022.9828257>
- Sawafi, Y. Al, Touzene, A., & Hedjam, R. (2023). Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks. *Journal of Sensor and Actuator Networks* 2023, Vol. 12, Page 21, 12(2), 21.
<https://doi.org/10.3390/JSAN12020021>
- Shafi, S., Mounika, S., & Velliangiri, S. (2023). Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET. *Procedia Computer Science*, 218, 2309–2318.
<https://doi.org/10.1016/J.PROCS.2023.01.206>
- Singh, A., Singh, G., & Singh, M. (2018). Comparative study of OLSR, DSDV, AODV, DSR and ZRP routing protocols under blackhole attack in mobile ad hoc network. *Advances in Intelligent Systems and Computing*, 624, 443–453.
https://doi.org/10.1007/978-981-10-5903-2_45/COVER
- Singh, K., & Gupta, R. (1 C.E.). SO-AODV: A Secure and Optimized Ad-Hoc On-Demand Distance Vector Routing Protocol Over AODV With Quality Assurance Metrics for Disaster Response Applications. *Https://Services.Igi-Global.Com/Resolvedoi/Resolve.aspx?Doi=10.4018/JITR.2021070106*, 14(3), 87–103. <https://doi.org/10.4018/JITR.2021070106>
- Souza, J., Jailton, J., Carvalho, T., Araújo, J., Francês, R., & Kaleem, Z. (2019). A Proposal for Routing Protocol for FANET: A Fuzzy System Approach with QoE/QoS Guarantee. *Wireless Communications and Mobile Computing*, 2019. <https://doi.org/10.1155/2019/8709249>
- Swain, S., Senapati, B. R., & Khilar, P. M. (1 C.E.). Evolution of Vehicular Ad Hoc Network and Flying Ad Hoc Network for Real-Life Applications: Role of VANET and FANET. *Https://Services.Igi-*

Global.Com/Resolvedoi/Resolve.Asp?Doi=10.4018/978-1-6684-3610-3.Ch003, 43–73. <https://doi.org/10.4018/978-1-6684-3610-3.CH003>

- Thuneibat, S., Al-Sharaa, B., & Al Sharaa, B. (2023). Dynamic source routing protocol with transmission control and user datagram protocols Network simulator Quality of service Routing protocol Transport layer Wireless network Dynamic source routing protocol with transmission control and user datagram protocols. *Indonesian Journal of Electrical Engineering and Computer Science*, 30(1), 137–143. <https://doi.org/10.11591/ijeecs.v30.i1.pp137-143>
- Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. In *Ad Hoc Networks* (Vol. 133). Elsevier B.V. <https://doi.org/10.1016/j.adhoc.2022.102894>
- Yadav, D., & Chaubey, N. K. (2022). Performance Analyses of Black Hole Attack in AODV Routing Protocol in Vanet Using NS3. *Communications in Computer and Information Science*, 1760 CCIS, 118–127. https://doi.org/10.1007/978-3-031-23095-0_9/COVER
- Yang, H., Pu, C., Wu, J., Wu, Y., & Xia, Y. (2023). Enhancing OLSR protocol in VANETs with multi-objective particle swarm optimization. *Physica A: Statistical Mechanics and Its Applications*, 614, 128570. <https://doi.org/10.1016/J.PHYSA.2023.128570>

Appendixes

Appendix A: Codes

Downloaded libraries

```
sudo apt-get install gcc g++ python python-dev mercurial bzip2 gdb valgrind glib-
bin libgsl0-dev libgsl0ldbl flex bison tcpdump sqlite sqlite3 libsqlite3-dev libxml2
libxml2-dev libgtk2.0-0 libgtk2.0-dev uncrustify doxygen graphviz imagemagick
texlive texlive-latex-extra texlive-generic-extra texlive-generic-recommended
texinfo dia texlive texlive-latex-extra texlive-extra-utils texlive-generic-
recommended texi2html python-pygraphviz python-kiwi python-pygoocanvas
libgoocanvas-dev python-pygccxml
```

Codes:

```
#include "ns3/point-to-point-module.h"
#include "ns3/ipv4-global-routing-helper.h"
#include <fstream>
#include <string>
#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/applications-module.h"
#include "ns3/mobility-module.h"
#include "ns3/config-store-module.h"
#include "ns3/wifi-module.h"
#include "ns3/aodv-helper.h"
#include "ns3/internet-module.h"
#include "ns3/netanim-module.h"

using namespace ns3;
NS_LOG_COMPONENT_DEFINE("Mob");

void BlackholeAttack(Ptr<Node> attackerNode, Ptr<Node> victimNode)
// Get the victim node's Ipv4StaticRouting helper
Ptr<Ipv4> ipv4 = victimNode->GetObject<Ipv4>();
Ptr<Ipv4RoutingProtocol> routingProtocol = ipv4->GetRoutingProtocol();
Ptr<Ipv4StaticRouting> staticRouting =
DynamicCast<Ipv4StaticRouting>(routingProtocol);
// Create a new route with a next hop pointing to the attacker node
Ipv4StaticRouting::RouteToHostAttributes routeAttributes;
routeAttributes.destination = Ipv4Address::GetBroadcast();
routeAttributes.gateway = attackerNode->GetObject<Ipv4>()->GetAddress(1,
0).GetLocal();
routeAttributes.outputInterface = 1;
staticRouting->SetHostRoute(routeAttributes);}
```

```

int main(int argc, char *argv[])
{ CommandLine cmd;
  cmd.Parse(argc, argv);
  NodeContainer c;
  c.Create(20); //20 wireless nodes
  WifiHelper wifi;
  wifi.SetStandard(WIFI_PHY_STANDARD_80211b);
  WifiMacHelper mac;
  mac.SetType("ns3::AdhocWifiMac");
  wifi.SetRemoteStationManager("ns3::ConstantRateWifiManager",
                               "DataMode", StringValue("OfdmRate54Mbps"));
  YansWifiPhyHelper wifiPhy = YansWifiPhyHelper::Default();
  YansWifiChannelHelper wifiChannel = YansWifiChannelHelper::Default();
  wifiChannel.SetPropagationDelay("ns3::ConstantSpeedPropagationDelayModel");
  wifiChannel.AddPropagationLoss("ns3::FriisPropagationLossModel");
  wifiPhy.SetChannel(wifiChannel.Create());
  NetDeviceContainer cDevices = wifi.Install(wifiPhy, mac, c);
  AodvHelper aodv;
  InternetStackHelper internet;
  internet.SetRoutingHelper(aodv);
  internet.Install(c);
  Ipv4AddressHelper ipAddr;
  ipAddr.SetBase("192.168.0.0", "255.255.255.0");
  Ipv4InterfaceContainer cInterfaces;
  cInterfaces = ipAddr.Assign(cDevices);
  MobilityHelper mobility;
  mobility.SetMobilityModel("ns3::GaussMarkovMobilityModel",
                           "Bounds", BoxValue(Box(0, 100, 0, 100, 0, 100)),
                           "TimeStep", TimeValue(Seconds(0.5)),
                           "Alpha", DoubleValue(0.85),
                           "MeanVelocity",
  StringValue("ns3::UniformRandomVariable[Min=800|Max=1200]"),
                           "MeanDirection",
  StringValue("ns3::UniformRandomVariable[Min=0|Max=6.283185307]"),
                           "MeanPitch",
  StringValue("ns3::UniformRandomVariable[Min=0|Max=0]"),
                           "NormalVelocity",
  StringValue("ns3::NormalRandomVariable[Mean=0.0|Variance=0.0|Bound=0.0]"),
                           "NormalDirection",
  StringValue("ns3::NormalRandomVariable[Mean=0.0|Variance=0.2|Bound=0.4]"),
                           "NormalPitch",
  StringValue("ns3::NormalRandomVariable[Mean=0.0|Variance=0.02|Bound=0.04]"));
  mobility.SetPositionAllocator("ns3::RandomBoxPositionAllocator",
                               "X",
  StringValue("ns3::UniformRandomVariable[Min=0|Max=100]"),
                               "Y",
  StringValue("ns3::UniformRandomVariable[Min=0|Max=100]"),
                               "Z",
  StringValue("ns3::UniformRandomVariable[Min=0|Max=100]"));
}

```

```
mobility.Install(c);
UdpEchoServerHelper echoServer(9);
ApplicationContainer serverApps = echoServer.Install(c.Get(0));
serverApps.Start(Seconds(1.0));
serverApps.Stop(Seconds(10.0));
UdpEchoClientHelper echoClient(cInterfaces.GetAddress(0), 9);
echoClient.SetAttribute("MaxPackets", UIntegerValue(1));
echoClient.SetAttribute("Interval", TimeValue(Seconds(1.0)));
echoClient.SetAttribute("PacketSize", UIntegerValue(1024));
ApplicationContainer clientApps = echoClient.Install(c.Get(1));
clientApps.Start(Seconds(2.0));
clientApps.Stop(Seconds(10.0));
wifiPhy.EnablePcapAll("Fanet3D");
AnimationInterface anim("Fanet3D.xml");
AsciiTraceHelper ascii;
wifiPhy.EnableAsciiAll(ascii.CreateFileStream("Fanet3D.tr"));
Ptr<Node> attackerNode = c.Get(2);
Ptr<Node> victimNode = c.Get(3);
BlackholeAttack(attackerNode, victimNode);
Simulator::Stop(Seconds(10.0));
Simulator::Run();
Simulator::Destroy();
return 0;}
```

Appendix B**Ethical Committee Approval Letter****BİLİMSEL ARAŞTIRMALAR ETİK KURULU**

04.09.2023

Dear NURUDEEN BODE AYANSINA

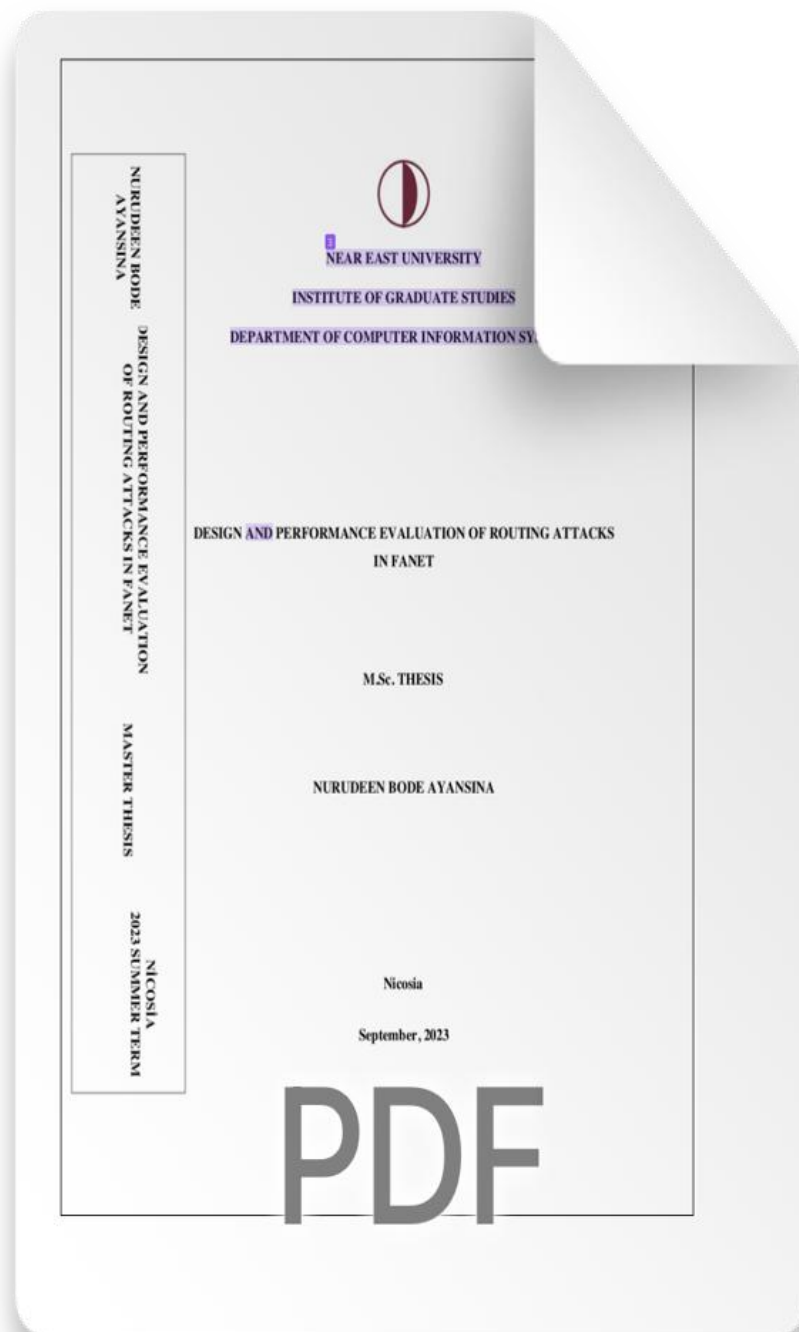
Your project **“A SYSTEMATIC LITERATURE REVIEW OF DESIGN AND PERFORMANCE EVALUATION OF ROUTING ATTACKS IN FANET”** has been evaluated. Since only secondary data will be used the project it does not need to go through the ethics committee. You can start your research on the condition that you will use only secondary data.

Prof. Dr. Aşkın KİRAZ

Rapporteur of the Scientific Research Ethics Committee

Appendix C

Similarity Report



DESIGN AND PERFORMANCE EVALUATION ATTACKS IN FANET

ORIGINALITY REPORT

13%	10%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	1%
2	www.mdpi.com Internet Source	1%
3	Submitted to Yakin Doğu Üniversitesi Student Paper	1%
4	docs.neu.edu.tr Internet Source	1%
5	Submitted to Heriot-Watt University Student Paper	1%
6	stax.strath.ac.uk Internet Source	<1%
7	www.scribd.com Internet Source	<1%
8	www.telecom.hk.hk Internet Source	<1%
9	Feng Li, , Yinying Yang, and Jie Wu. "Attack and Flee: Game-Theory-Based Analysis on	<1%

PDF

Interactions Among Nodes in MANET
Transactions on Systems Man and
Cybernetics Part B (Cybernetics), 20
Publication

10	Submitted to North West University Student Paper	
11	www.semanticscholar.org Internet Source	< 1 %
12	Dongkyun Kim, C.K. Toh, Hongseok Yoo. "The Impact of Spurious Retransmissions on TCP Performance in AD HOC Mobile Wireless Networks", 2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007 Publication	< 1 %
13	asset-pdf.scinapse.io Internet Source	< 1 %
14	etd.aau.edu.et Internet Source	< 1 %
15	Submitted to Cambridge Education Group Student Paper	< 1 %
16	Submitted to Vaasan yliopisto Student Paper	< 1 %
17	link.springer.com Internet Source	< 1 %
PDF		
dspace2.lib.nccu.edu.tw		

- 18 Internet Source
-
- 19 thesis.univ-biskra.dz
Internet Source
-
- 20 Submitted to Brunel University
Student Paper
-
- 21 Idriss Moumen, Najat Rafalia, Jaafar Aouchabaka, Youssef Chatoui. "AODV-based Defense Mechanism for Mitigating Blackhole Attacks in MANET", E3S Web of Conferences, 2023
Publication <1%
-
- 22 E.O. Ochola, L.F. Mejaele, M.M. Eloff, J.A. van der Poll. "Manet Reactive Routing Protocols Node Mobility Variation Effect in Analysing the Impact of Black Hole Attack", SAIEE Africa Research Journal, 2017
Publication <1%
-
- 23 Submitted to Nottingham Trent University
Student Paper <1%
-
- 24 Taehwan Kim, Seonah Lee, Kyong Hoon Kim, Yong-Il Jo. "FANET Routing Protocol Analysis for Multi-UAV and Performance Mobility Models", Drones, 2022
Publication <1%
-
- 25 www.ijscce.org
Internet Source <1%

- | | | |
|----|--|------|
| 26 | www.ros.hw.ac.uk
Internet Source | |
| 27 | www.akceducation.org
Internet Source | |
| 28 | www.sfu.ca
Internet Source | |
| 29 | Submitted to Asia Pacific University College of Technology and Innovation (UCTI)
Student Paper | <1 % |
| 30 | Submitted to Higher Education Commission Pakistan
Student Paper | <1 % |
| 31 | Submitted to Staffordshire University
Student Paper | <1 % |
| 32 | Submitted to Victoria University of Wellington
Student Paper | <1 % |
| 33 | D. Djenouri, L. Khelladi, A.N. Badache. "A survey of security issues in mobile ad hoc and sensor networks", IEEE Communications Surveys & Tutorials, 2005
Publication | <1 % |
| 34 | Submitted to www.melaka.gov.my
Melaka
Student Paper | <1 % |
| 35 | ijcsmc.com
Internet Source | |

PDF

36	Submitted to /paperInfo.asp?oid=13 Student Paper	
37	Seyed Ali Hosseini, Hamid Farrokhi. "Impacts of network size on the performance of routing protocols in mobile ad-hoc networks", 2010 Second Pacific-Asia Conference on Circuits, Communications and System, 2010 Publication	
38	Submitted to University of Derby Student Paper	<1 %
39	Submitted to University of Greenwich Student Paper	<1 %
40	Submitted to International Islamic University Malaysia Student Paper	<1 %
41	Submitted to Middlesex University Student Paper	<1 %
42	V. A. Berezin, V. A. Kuzmin, I. I. Tkachev. "Black holes initiate false-vacuum decay", Physical Review D, 9, 11 Publication	<1 %
43	www.blm.gov Internet Source	<1 %

PDF

44	Submitted to Gulf University for Science and Technology Student Paper	
45	Su Mon Bo, Hannan Xiao, Aderemi A. Adewale, James A. Malcolm, Bruce Christianson Performance Comparison of Wireless Network Routing Protocols under Security Attack", Third International Symposium on Information Assurance and Security, 2007 Publication	
46	www.scilit.net Internet Source	<1 %
47	Chang-WuPing-JiaYen-Wen ChenSuChen. "Design of path-based multicast routing protocol in MANET", Proceedings of the 3rd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks - PM2HW2N 08 PM2HW2N 08, 2008 Publication	<1 %
48	etd.repository.ugm.ac.id Internet Source	<1 %
49	journals.nawroz.edu.krd Internet Source	<1 %
50	m.moam.info Internet Source	<1 %
	meral.edu.mm	

PDF

51	Internet Source	
52	Adam Gorine, Ayoade Adeyemo. "Performance of Vehicle Ad-Hoc Networks (VANETs) Operating in a Hostile Environment", SN Computer Science Publication	
53	Submitted to CSU, San Jose State University Student Paper	<1 %
54	cse.buffalo.edu Internet Source	<1 %
55	openarchive.usn.no Internet Source	<1 %
56	www.duo.uio.no Internet Source	<1 %
57	www.ist-runes.org Internet Source	<1 %
58	www.springerprofessional.de Internet Source	<1 %
59	"Smart Trends in Information Technology and Computer Communications", Springer Science and Business Media LLC, 2016 Publication	<1 %
60	1library.net Internet Source	<1 %

PDF