electronics

Article

Impact Analysis of Security Attacks on Mobile Ad Hoc Networks (MANETs)

Iain Baird, Isam Wadhaj *, Baraq Ghaleb and Craig Thomson

School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh EH10 5DT, UK; i.baird2@napier.ac.uk (I.B.); b.ghaleb@napier.ac.uk (B.G.); c.thomson3@napier.ac.uk (C.T.)
* Correspondence: i.wadhaj@napier.ac.uk

Abstract: Mobile ad hoc networks (MANETs) offer a decentralized communication solution ideal for infrastructure-less environments like disaster relief zones. However, their inherent lack of central control and dynamic topology make them vulnerable to attacks. This paper examines the impact of various attacks on mobile nodes within two network types: randomly and uniformly distributed stationary networks. Four types of attacks are investigated: delay, dropping, sinkhole (alone), and a combined black hole attack (dropping + sinkhole). The effects of these attacks are compared using the packet delivery ratio, throughput, and end-to-end delay. The evaluation results show that all single attacks negatively impacted network performance, with the random network experiencing the most significant degradation. Interestingly, the combined black hole attack, while more disruptive than any single attack, affected the uniformly distributed network more severely than the random network.

Keywords: MANET; delay attack; dropping attack; sinkhole attack

check for updates

Citation: Baird, I.; Wadhaj, I.; Ghaleb, B.; Thomson, C. Impact Analysis of Security Attacks on Mobile Ad Hoc Networks (MANETs). *Electronics* **2024**, *13*, 3314. https://doi.org/10.3390/electronics13163314

Academic Editor: Christos J. Bouras

Received: 14 July 2024
Revised: 13 August 2024
Accepted: 16 August 2024
Published: 21 August 2024

1. Introduction

Mobile ad hoc networks (MANETs) were originally conceptualized by the U.S. DOD in the 1970s with the introduction of the Packet Radio Network [1]. However, technological limitations at the time, such as bulky equipment and power constraints, hindered their practical implementation. Recent advancements in WiFi technology and the proliferation of WiFi-enabled devices have fueled the resurgence of interest in infrastructure-less networks like MANETs [2].

WiFi has become an essential part of modern life, facilitating a wide range of daily activities. Mobile ad hoc networks (MANETs), which harness the versatility of WiFi, are particularly effective in scenarios where traditional infrastructure is lacking, power resources are constrained, and rapid communication is critical. These networks are invaluable in disaster recovery efforts and military operations, where they enable real-time coordination. Beyond these high-stakes environments, the flexibility of MANETs has also led to their widespread use in civilian contexts. Examples include Smartphone Ad Hoc Networks (SPANs) for peer-to-peer communication, Vehicular Ad Hoc Networks (VANETs) for intelligent transportation systems, and Flying Ad Hoc Networks (FANETs) for drone-based applications. Additionally, MANETs are increasingly being deployed in smart cities, remote sensing, and outdoor events, showcasing their broad potential in both urban and rural settings [3].

The dynamic and flexible nature of MANETs introduces a larger attack surface compared to traditional WLANs [4]. This vulnerability makes it challenging to prevent attackers from disrupting network operations and maintaining data availability, confidentiality, and integrity [5]. Understanding these attack methods and their impact on MANETs is crucial for developing effective countermeasures.

This paper investigates and presents the effects of various attacks on mobile ad hoc networks. To achieve this, the Open Modeling and Network Simulation Tool (OMNeT++) discrete event simulator will be used to create a network simulation [6]. The Network Emulator for Threat Assessment (NETA) framework will be employed to launch attacks and gather data on network performance under different scenarios [7].

Problem Statement

While the flexibility and infrastructure-less nature of mobile ad hoc networks (MANETs) offer significant advantages, their dynamic topology and decentralized architecture render them highly susceptible to a variety of security threats, including denial-of-service (DoS), sinkhole, and delay attacks. The consequences of these attacks can be catastrophic, leading to data breaches, financial losses, and even loss of life in critical applications such as disaster recovery, military operations, and intelligent transportation systems. Despite ongoing research efforts, existing security solutions for MANETs often face challenges in terms of overhead, scalability, and resilience against emerging threats. Therefore, developing robust and efficient security mechanisms to safeguard the integrity and confidentiality of MANET communications is imperative.

Despite numerous studies addressing security issues in MANETs, a comprehensive understanding of the impact of various attacks, particularly considering the dynamic nature of the network, remains elusive. Existing research often lacks detailed empirical data on how attacker mobility influences critical performance metrics such as the packet delivery ratio and end-to-end delay. This scarcity of knowledge hinders the development of effective, lightweight countermeasures capable of adapting to diverse attack scenarios. The remainder of this paper is organized as follows:

Section 2 reviews recent research on MANET security. Section 3 covers mobile ad hoc networks (MANETs), introducing their key characteristics, functionalities, and applications. It also reviews routing protocols with a focus on AODV and explores security issues and vulnerabilities in MANETs.

Section 4 analyzes prevalent MANET attacks such as sinkhole and delay attacks. Section 5 details the testing procedures, including the network simulator, parameters, and attack strategies. Section 6 presents simulation results and analyzes the impact of attacker movement on two network typologies using metrics like the packet delivery ratio and end-to-end delay. Finally, Section 7 summarizes key findings, discusses the significance of attacker movement in DoS attacks, and suggests directions for future research.

2. Related Work

Al-Rubaiei et al. conducted a performance analysis of black hole and wormhole attacks on MANETs using the Network Simulator 2 (NS2) and the Ad hoc On-Demand Distance Vector (AODV) routing protocol [8]. Their study examined the impact of these attacks on the packet delivery ratio, end-to-end delay, and network load normalization. It is noteworthy that NS2 lacks built-in functionalities for simulating malicious attacks. Therefore, the authors modified the AODV protocol to simulate these attacks. The study concluded that black hole attacks had a more significant impact on the network compared to wormhole attacks, primarily due to higher packet loss. However, black hole attacks resulted in better network performance in terms of end-to-end delay.

Al-Shareeda et al. investigated the impact of Man-in-the-Middle (MitM) attacks on MANETs using OMNeT++ and the NETA framework [5]. They employed the Ad hoc On-Demand Distance Vector (AODV) routing protocol and measured the effects of the attacks on the packet delivery ratio and end-to-end delay. Unlike the previous study, OMNeT++ with NETA allows for native simulation of network attacks. Their findings demonstrate that both message delay and message dropping variants of the MitM attack significantly impact the network, causing substantial increases in end-to-end delay and packet loss.

Deepika et al. evaluated the performance of AODV and Dynamic Source Routing (DSR) protocols under Jellyfish Delay Variance attacks in a simulated MANET using NS2 [9]. The simulation involved fifty nodes with random waypoint mobility and a varying number of attacker nodes. End-to-end delay and throughput were measured. The paper proposes a method for detecting and removing Jellyfish attackers. This method utilizes node self-detection and neighbor detection. Each node stores trust attributes for its neighbors, which are updated before every transmission. The study concluded that both AODV and DSR experience significant improvement in end-to-end delay under attack when mitigation is implemented compared to no mitigation strategies. However, with an increasing number of attackers, throughput decreases significantly even with mitigation, although some improvement remains. However, the paper does not address the potential resource overhead associated with this trust-based approach, which is a crucial consideration for resource-constrained MANETs.

Sivanesh et al. investigate the impact of black hole and rushing attacks on mobile ad hoc networks (MANETs) utilizing the AODV routing protocol [10]. Employing the NS2 simulator, the study meticulously analyses network performance under these attacks, considering metrics such as the packet delivery ratio, end-to-end delay, throughput, and packet loss. The findings reveal that black hole attacks pose a more severe threat, resulting in a drastically reduced packet delivery ratio and increased packet loss compared to rushing attacks. While black hole attacks exhibit lower end-to-end delay due to diminished routing overhead, this advantage is offset by a significant compromise in network reliability. Ultimately, this research underscores the vulnerabilities inherent in the AODV protocol, which malicious nodes can exploit to disrupt normal network operations. It is important to note that the scope of this study is limited to two specific attack types, with other potential threats to AODV performance remaining unexplored. Additionally, the reliance on NS2 simulations may not fully encapsulate the complexities of real-world attacks as the previously discussed NS2 lacks a built-in functionality to simulate malicious attacks.

Elshaikh et al. investigate the impact of black hole attacks on the performance of MANETs utilizing the AODV routing protocol [11]. By employing the OMNET++ simulator, the authors simulated various network scenarios with different numbers of nodes and black hole attackers. The paper indicates that nodes move randomly, but does not specify the exact mobility model employed, including whether the movement pattern of attacker nodes differs from that of regular nodes. The study focuses on key performance metrics such as the packet delivery ratio, throughput, and end-to-end delay to assess the severity of the attacks. The research methodology involves conducting multiple simulation runs under controlled conditions to analyze the behavior of black hole attacks. While the paper provides valuable insights into the impact of these attacks on network performance, it has certain limitations. The study's primary focus on black hole attacks restricts its scope. Additionally, the absence of detailed information about the mobility model and the lack of statistical analysis to support the findings weaken the overall strength of the conclusions. Despite these limitations, the paper offers a foundation for understanding the effects of black hole attacks on MANETs. The use of simulation and clear performance metrics strengthens the research. However, future studies could benefit from a broader exploration of different attack types, a diverse range of mobility models, including specific characterizations for attacker movement, and robust statistical analysis to enhance the overall contribution to the field.

This study introduces a novel approach to evaluating the impact of various attacks on MANETs. Unlike previous research, we focus on a scenario where normal nodes are stationary while attackers exhibit mobility. By employing both random and uniform distribution topologies, we provide a comprehensive analysis of network resilience under different spatial arrangements. This research investigates the effects of four distinct attack types: dropping, delay, sinkhole, and a combined black hole attack (incorporating dropping and sinkhole). Through this comparative analysis, we aim to identify vulnerabilities in an effort to enhance the robustness of MANETs against malicious threats.

3. Mobile Ad Hoc Networks

Mobile ad hoc networks (MANETs) are a type of wireless network that is both adaptive and self-organizing. Unlike traditional WiFi networks in offices or homes that rely on base stations or access points, MANETs operate in an infrastructure-less manner, and a comparison example between the infrastructures can be seen in Figure 1. Unlike the left image, which portrays an infrastructure-less MANET with all nodes functioning as routers, the right image depicts a traditional WiFi network featuring centralized base stations.

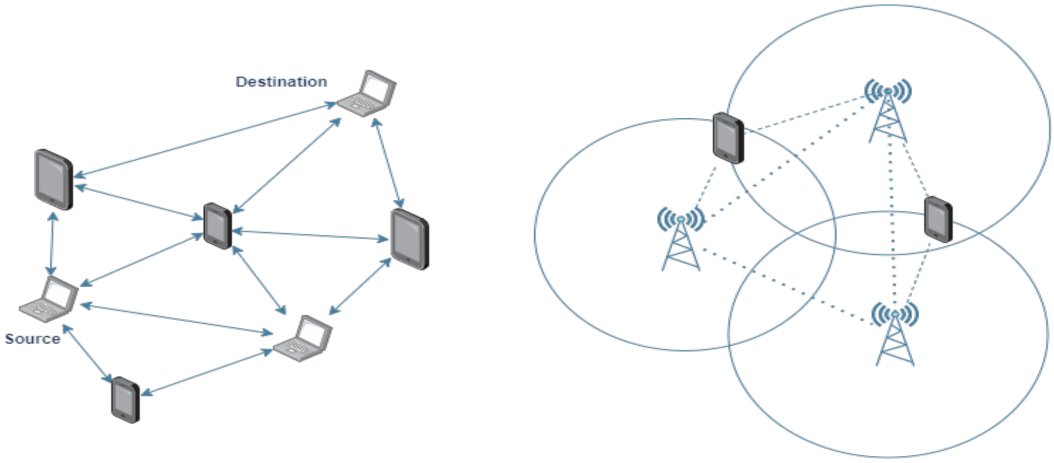

Figure 1. Ad hoc infrastructure comparison.

Due to dynamic topologies where nodes freely move in and out, the network's multi-hop structure constantly changes. To adapt to this, MANETs operate as self-configuring infrastructures, and this means they can discover new devices and have all nodes function as both routers and hosts. In MANETs, nodes constantly move in and out of each other's broadcast range. To find the most efficient routes, they use a network discovery method. This method allows new nodes to announce their presence and all nodes to dynamically update the routing information. This continuous discovery process makes MANETs highly scalable, enabling the network to seamlessly grow as new nodes join [12].

3.1. Routing in MANETs

Similar to traditional routing protocols, MANET routing aims to establish and maintain optimal paths between source and destination nodes. This process prioritizes minimizing delay and packet loss. However, MANET routing protocols face unique challenges compared to traditional networks due to several factors [13,14]:

- Decentralized network: Unlike centralized networks, there is no single entity managing routing in a MANET. Each node acts independently.
- Limited resources: Nodes in a MANET often have limited battery power and processing capabilities. Routing protocols need to be efficient to minimize resource consumption.
- Control overhead: Routing protocols generate control packets to discover and maintain routes. Excessive control overhead can lead to network congestion.
- High node mobility: As nodes move, the network topology constantly changes. Routing protocols need to adapt quickly to these changes and incorporate new network discovery mechanisms to locate nodes entering or leaving the network.

There are three main categories of topology-based routing protocols classified based on their approach to acquiring routing information for packet forwarding: proactive, reactive, and hybrid. A selection of example protocols can be seen in Figure 2 [15,16].

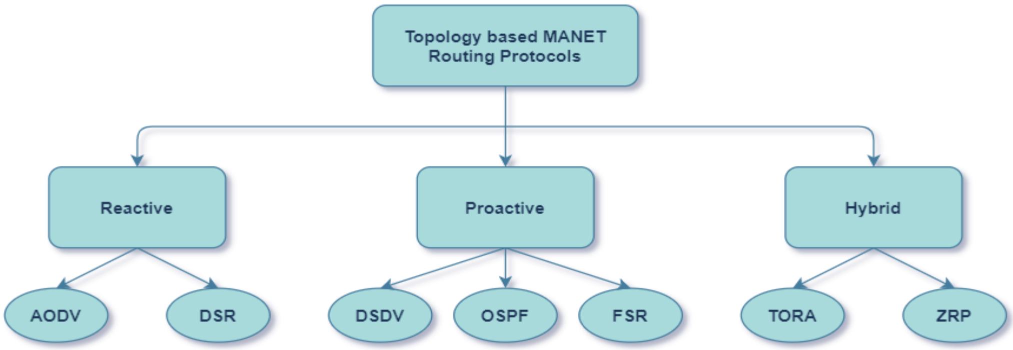

Figure 2. Topology-based MANET routing protocols.

3.1.1. Proactive Routing Protocol

Commonly known as Table-Driven routing, this method involves each node in the network keeping a table of all possible destinations. As the network topology continuously changes, periodic updates are used to maintain these tables. The primary advantage of this routing approach is its ability to reduce end-to-end delay [17].

3.1.2. Reactive Routing Protocol

Reactive routing protocols, also known as on-demand routing, are resource-efficient. Unlike proactive protocols, they do not require nodes to maintain extensive routing tables. Instead, they discover routes only when needed, reducing memory and bandwidth consumption. However, this reactive approach introduces a delay as nodes need to actively find a route before forwarding data packets [18].

3.1.3. Hybrid Routing Protocols

Hybrid routing protocols, as the name suggests, attempt to leverage the strengths of both proactive and reactive approaches. They establish proactive routing zones around each node, where routing information for frequently accessed destinations is readily available, minimizing delay for local communication. However, when a node needs to send data packets outside its zone (similar to a reactive protocol), it initiates a route discovery process to find the optimal path to the destination. This hybrid approach offers a balance between the route maintenance overhead of proactive protocols and the potential delays inherent in reactive protocols [19].

3.2. Ad Hoc On-Demand Distance Vector (AODV)

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is classified as a reactive protocol for MANETs [20]. However, it exhibits characteristics of both the reactive and proactive approaches. The AODV shares similarities with reactive protocols like Dynamic Source Routing (DSR) in its route discovery and maintenance mechanisms [21]. However, before flooding the network with route request messages, the AODV consults its cached routing table, similar to a proactive protocol like the Destination Sequenced Distance Vector (DSDV). This cached information helps the AODV avoid unnecessary route discovery overhead in scenarios where the route might already be known [22]. As a result, the AODV can be viewed as a hybrid protocol that leverages aspects of both reactive and proactive approaches. This routing decision process can be seen in Figure 3.

The AODV initiates route discovery by broadcasting route request (RREQ) packets when no cached route exists. These packets propagate through the network until the destination is found or an intermediate node has a valid route. Upon receiving an RREQ, the destination or a suitable intermediate node responds with a route reply (RREP); see Figure 4. The source node selects the best route based on the sequence number and hop count and starts data transmission. The AODV also employs route maintenance using periodic Hello messages and Route Error (RERR) packets to detect and repair broken links, triggering route discovery when necessary [23].

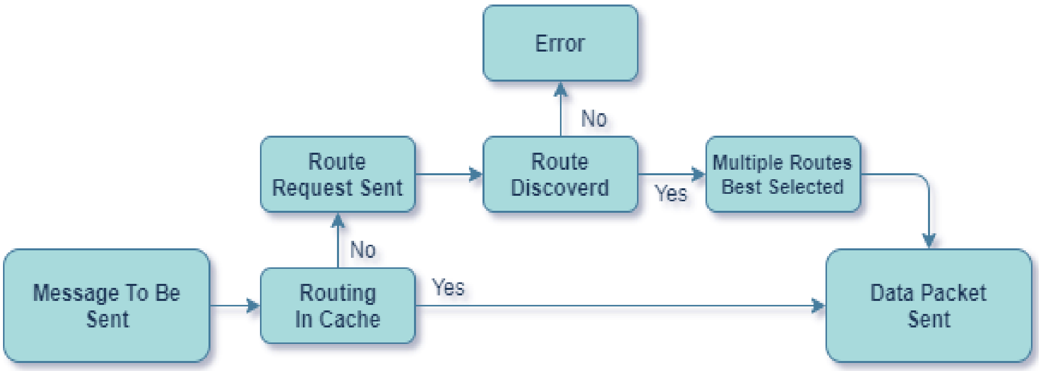

Figure 3. AODV routing process.

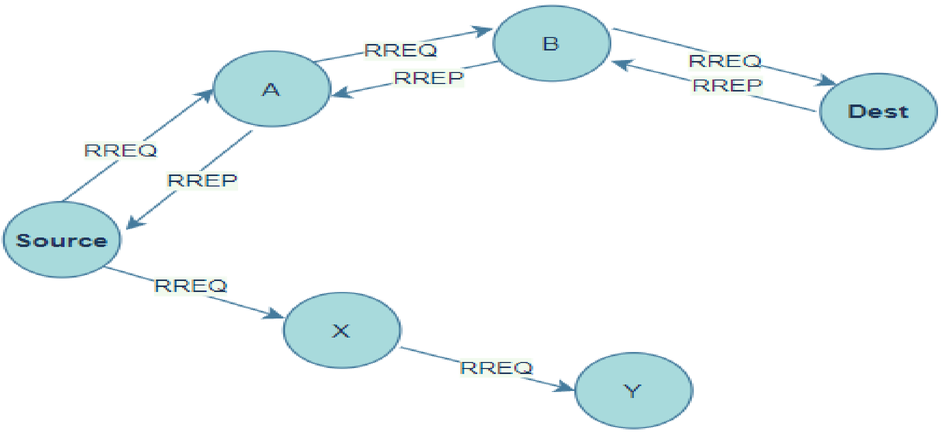

Figure 4. Route request transmission and route reply.

3.3. Security Issues in MANETs

Security requirements in MANETs differ slightly from traditional networks. While the core principles remain the same, MANETs necessitate additional considerations due to the following [24,25]:

- Resource constraints and security trade-offs: Unlike traditional wired networks, nodes in a MANET have limited battery life, processing power, memory, and bandwidth. Implementing robust security measures can significantly strain these already limited resources. Therefore, it is crucial to find a balance between security requirements and resource availability to ensure optimal network performance and expected lifetime.
- Vulnerability of wireless medium: Compared to wired networks with a clear physical layer boundary, MANETs are inherently more vulnerable. All nodes communicate wirelessly, eliminating the need for physical access to launch attacks. This vulnerability necessitates additional security measures beyond what is typically employed in wired networks.
- Challenges of centralized management: Security in wired networks often relies on centralized management for tasks like data encryption with key distribution. However, MANETs lack a central authority. While partial or selective encryption techniques can be implemented to reduce resource consumption, the absence of a central repository for key management presents a significant challenge [26].
- Impact of mobile topologies: The dynamic nature of MANETs, with nodes freely moving in and out of the network, creates challenges for both routing and security. Detecting malicious nodes becomes difficult due to the constant changes in the network topology caused by legitimate node mobility

4. Common Attacks within MANETs

This section explores various security threats targeting MANETs. Due to their open, accessible, and mobile nature, MANETs are particularly susceptible to a wide range of attacks. These attacks can be categorized in several ways, including the following [27,28].

4.1. Active vs. Passive

Attacks can be passive (aiming to eavesdrop on or analyze network traffic without disrupting operations) or active (disrupting network functionality or manipulating data).

4.2. Internal vs. External

Depending on the origin of the attacker, threats can be internal (launched by compromised nodes within the network) or external (launched from outside the network).

The following sections explore some of the most prevalent attacks targeting MANETs [29].

4.3. Sinkhole Attack

Reactive routing protocols, such as the AODV, rely on a query–response mechanism for route discovery. When a source node requires a route to a destination, it broadcasts a route request (RREQ) packet through the network. Intermediate nodes forward this RREQ, incrementing a hop count to track the path length. Upon receiving an RREQ, the destination node or a node possessing a fresh route to the destination responds with a route reply (RREP) packet, which is traced back to the source via the reverse path established by the RREQ. The source selects the optimal route based on metrics such as hop count and route freshness, indicated by a sequence number. A sinkhole attack exploits this process by maliciously crafting a RREP message that falsely advertises a shorter path and a higher sequence number. This deceptive information lures the source node into redirecting traffic through the attacker, effectively creating a "sinkhole" that absorbs incoming packets [30].

Once a sinkhole attack is successfully executed, the malicious node gains control over the network traffic destined for the targeted destination. The attacker can then manipulate this traffic in various ways. A common tactic is to simply drop the packets, effectively launching a black hole attack, as illustrated in Figure 5. This results in complete data loss for the intended recipients [31]. However, the malicious node's capabilities extend beyond this, allowing for a range of other malicious activities, such as eavesdropping, data modification, or launching further attacks on the network [32].

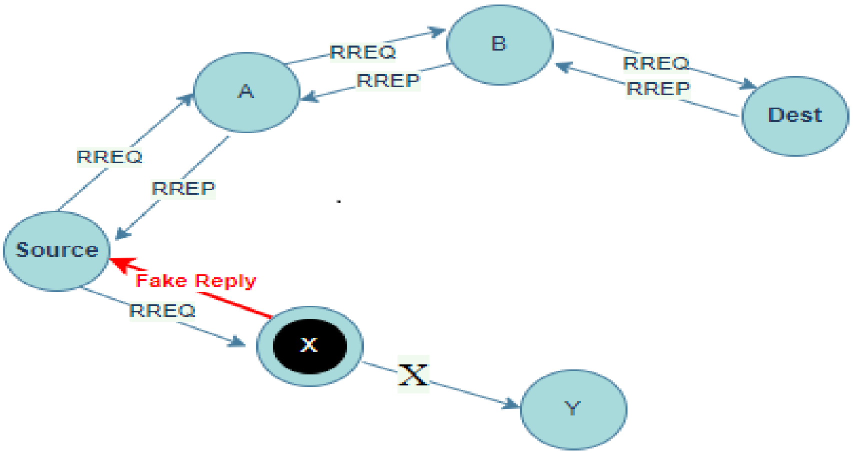

Figure 5. Black hole attack.

4.4. Delay Attack

The Jellyfish Delay Variance attack is another sophisticated exploit that leverages the vulnerabilities found in the route reply (RREP) mechanism, commonly targeted in sinkhole attacks. While similar in its goal of disrupting network traffic, the Jellyfish attack provides the attacker with a broader set of strategies to achieve this disruption, thereby offering greater flexibility and making detection more challenging. In particular, the Jellyfish attack can employ three distinct tactics [33]:

- Jellyfish reorder attack: In this method, the malicious node deliberately rearranges the order of packets as they pass through the network. This reordering disrupts the intended sequence of data transmission, which can lead to issues such as out-of-order packet delivery, degraded application performance, and increased error rates in protocols that rely on sequential data, such as TCP.
- Jellyfish periodic dropping attack: Here, the attacker periodically drops packets rather than continuously. This intermittent loss of data packets degrades network performance by causing delays in communication, repeated re-transmissions, and reduced throughput. The periodic nature of the packet dropping also makes the attack harder to detect, as it mimics the natural packet loss that can occur in a congested or unstable network.
- Delay variance attack: This tactic involves introducing variable delays to the packets as they are forwarded through the malicious node. By causing inconsistencies in packet delivery times, the attacker increases overall network latency, which can severely impact time-sensitive applications. The unpredictable nature of these delays further complicates the detection and mitigation of the attack, as it can be mistaken for network congestion or other benign issues; see Figure 6.

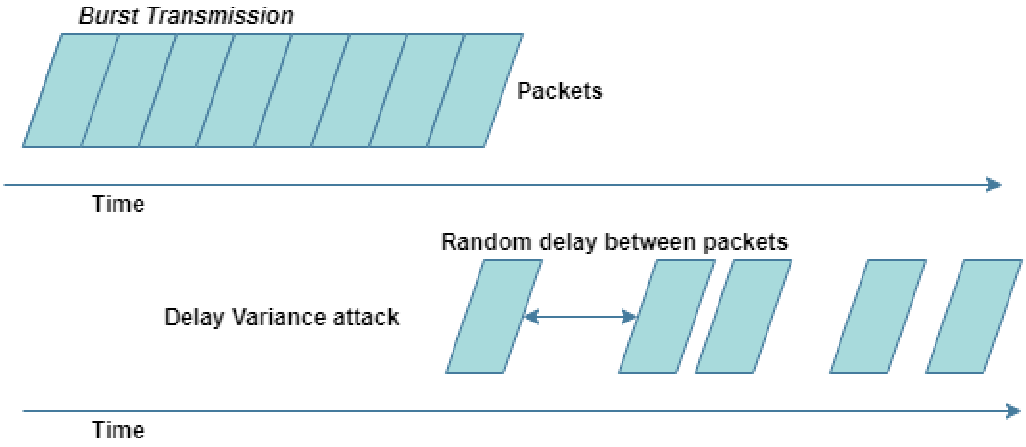

Figure 6. Delay variance attack.

Collectively, these tactics allow the attacker to subtly and effectively degrade the performance and reliability of the network, all while remaining hidden within the legitimate traffic flow. The Jellyfish Delay Variance attack, with its multiple approaches, presents a significant challenge in ensuring the security and stability of MANETs and other wireless networks.

4.5. Wormhole Attacks

Wormhole attacks, also referred to as tunnel attacks, exploit a vulnerability similar to that in sinkhole attacks. The attack is initiated by having two malicious nodes establish a covert tunnel (wormhole) among them. The attack is then launched by capturing packets at one end of the wormhole, transmitting them through the out-of-band connection, and re-injecting them at the other end. This can trick legitimate nodes into believing the wormhole route is shorter, leading to disrupted traffic flow, potential data manipulation, and degraded network performance [34].

4.6. Selfish Nodes

Selfish nodes pose a significant challenge to MANETs. Unlike malicious nodes that actively disrupt the network, selfish nodes prioritize their own benefit over network goals. They selectively participate in routing protocols, forwarding packets only when it serves their needs. This behavior often involves dropping other packets to conserve resources like battery power. While selfish nodes may not directly target specific users, their actions harm the entire network by increasing overall overhead and reducing efficiency. Network performance suffers as other nodes must work harder to compensate for dropped packets and find alternative routes [35,36].

4.7. Grey Hole Attacks

The grey hole attack, also known as a selective forwarding attack, shares similarities with the black hole attack. Both involve malicious nodes dropping packets. However, grey hole attacks are more sophisticated and unpredictable. Instead of dropping all packets like a black hole, grey hole nodes selectively drop them based on pre-determined criteria, such as packet types (e.g., dropping all UDP packets) or random intervals. This makes grey hole attacks challenging to detect because the malicious node can behave normally at times, masking its true nature. The unpredictable nature of packet dropping makes it difficult to identify the attacker and distinguish it from legitimate nodes [37].

4.8. Flood Attacks

Flooding attacks aim to disrupt network operations by overwhelming it with a large volume of packets, essentially a denial-of-service (DoS) attack. These attacks come in various forms, each targeting a specific network protocol or service [38]:

- Hello flood: Targets the Hello messages used by nodes to discover neighbors, exhausting bandwidth and node resources.
- RREQ flood: Spams the network with route request messages used in reactive routing protocols, overloading nodes and hindering legitimate route discovery.
- Data flood: Floods the network with irrelevant data packets, consuming bandwidth and hindering legitimate data transmission.
- ICMP/UDP flood: Targets specific protocols like ICMP (ping) or UDP to overwhelm resources.

4.9. Rushing Attack

Rushing attacks target route discovery mechanisms in on-demand routing protocols like the AODV and DSR. When a node receives a route request packet, a rushing attacker prematurely forwards it to the destination or intermediate nodes. This aims to suppress the original RREQ, tricking the destination or intermediate nodes into dropping it as a duplicate. The attacker can also employ rushing attacks on route reply messages [28].

By forwarding a fabricated RREP before the legitimate one arrives, the attacker increases their chances of being chosen as the preferred route for data forwarding. This allows them to inject themselves into the data path and potentially disrupt communication [39].

5. Methodology

This project delves into the impact of various attacks on the functionality and performance of mobile ad hoc networks (MANETs). The analysis focuses on three specific attack types: dropping attacks, which disrupt communication by discarding packets; sinkhole attacks, where a malicious node attracts and absorbs network traffic; and Jellyfish Delay Variance attacks, which introduce unpredictable delays into packet delivery. To comprehensively assess the potential damage, a combined scenario simulating a black hole attack, a fusion of sinkhole and dropping attacks, will also be investigated. These attack vectors were chosen due to their potential to severely compromise MANET operations, including disruption of critical communication, data loss, and degradation of network performance. By understanding the effects of these attacks, effective countermeasures can be developed to enhance the resilience and security of MANETs.

Our simulations will utilize two network configurations, each consisting of 25 nodes. The first configuration will employ a random distribution, where node placement is random within the simulation area. The second configuration will use a uniform distribution, where nodes are spread evenly throughout the area. In both scenarios, only the attacking nodes will be mobile; see Figure 7.

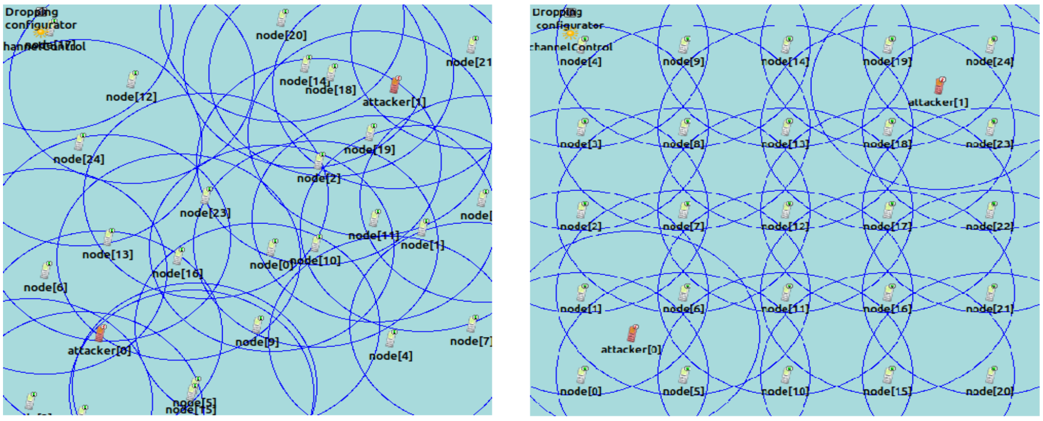

Figure 7. Random node and uniform node distributed networks.

The specific order in which the simulations were conducted is documented in Table 1.

Table 1. Simulation run order.

Random Then Uniform Distribution		
Simulation	**Attack**	**Number of Attackers**
1	Baseline (No Attack)	One Node
2	Delay	
3	Sinkhole	
4	Dropping	
5	Combined (Black Hole)	
6	Baseline (No Attack)	Two Node
7	Delay	
8	Sinkhole	
9	Dropping	
10	Combined (Black Hole)	

For consistent and repeatable attacker movement across multiple simulation runs, the Bonn motion mobility model was employed [40]. This approach enables for the definition of both the speed and direction of attacker nodes within the simulator. The Bonn motion mobility model utilizes text files, commonly referred to as trace files, to define attacker movement within the simulator. These trace files are referenced by a configuration file (.ini).

Each line in the trace file describes the motion of a single attacking node. The data are typically grouped into threes:

- x: X-coordinate (specifies the node’s horizontal position).
- y: Y-coordinate (specifies the node’s vertical position).
- t: Time in seconds (represents the time at which the node should be at the specified coordinates).

Optional

- z: (Optional) height coordinate (specifies the node's vertical position in 3D simulations).

This approach ensures consistent and repeatable attacker movement across multiple simulation runs, allowing for a reliable analysis of the attacks' impact.

5.1. Simulator

To streamline the simulation process, two frameworks within the OMNeT++ discrete event simulator will be utilized:

- INET framework: This framework provides essential components for building mobile ad hoc networks (MANETs) within the OMNeT++ environment. It offers pre-built modules for nodes, routing protocols, and network functionalities.
- Network attacks NETA framework: This framework simplifies the simulation of various attacks on MANETs. NETA integrates seamlessly with INET, allowing you to introduce and analyze the effects of different attack scenarios within your simulations.

The simulation configuration is defined within an initialization file (often referred to as an .ini file). This file allows us to specify various parameters that control the simulation run. Table 2 provides an overview of some common parameters used across all simulations.

Table 2. Common parameters to all simulations.

Parameter	**Value**
Simulation time	1661 s
Environmental size	1000 m × 1000 m
Packet size	512 bytes
Traffic type	UDP
Node number	25
Attackers	1, 2
Node mobility	Stationary
Attacker mobility	Bonn motion
Routing protocol	AODV

5.2. Performance Metrics

Three key performance metrics will be monitored to evaluate the impact of the attacks: packet delivery ratio (PDR), end-to-end delay (E2E), and throughput.

5.2.1. Packet Delivery Ratio

This metric measures the percentage of packets successfully delivered from the source to the destination. A lower PDR indicates increased packet loss due to the attacks. The PDR can be calculated by using the following Formula (1).

$$PDR = \frac{PacketsReceived}{PacketsSent} \tag{1}$$

5.2.2. End-to-End Delay

This metric measures the average time taken for a packet to travel from the source to the destination. Increased delays can be attributed to the attacks disrupting network communication.

5.2.3. Throughput

This represents the successful data rate achieved by the network, essentially the amount of usable data delivered per unit time. Throughput is the ratio of the total number of successfully transmitted and delivered packets to the total simulation time. Calculating the throughput can be accomplished using Formula (2).

$$Throughput = \frac{8 \times Packetsize\,(bytes) \times Packetsreceived}{Simulationtime\,(sec)} \tag{2}$$

6. Performance Evaluation and Discussions

To ensure the robustness of our findings and account for the inherent variability associated with random node placement within the OMNeT++ environment, a multi-run simulation approach was employed. Each simulation scenario was executed 10 times with a different random seed, introducing variation in the node positions to the random distribution scenario and network behavior. This approach allows us to capture a broader range of possible outcomes and generate more reliable average results, calculated with a 99% confidence level.

6.1. PDR Results

6.1.1. Random Node Distribution Results

The results clearly demonstrate the varying impact of different attack types on the PDR within the random distribution. Notably, delay and sinkhole attacks, as depicted in Figure 8, exhibit PDR values indistinguishable from the baseline scenario. This is attributed to the nature of these attacks, which primarily manipulate routing or introduce delays without necessarily preventing packets from ultimately reaching their destinations. In contrast, the baseline scenarios feature one and two mobile nodes operating exclusively as routers, free from malicious activities. By frequently establishing more efficient routes to the root compared to randomly distributed nodes or single-node configurations, two mobile routers contribute to the superior performance illustrated in Figure 8.

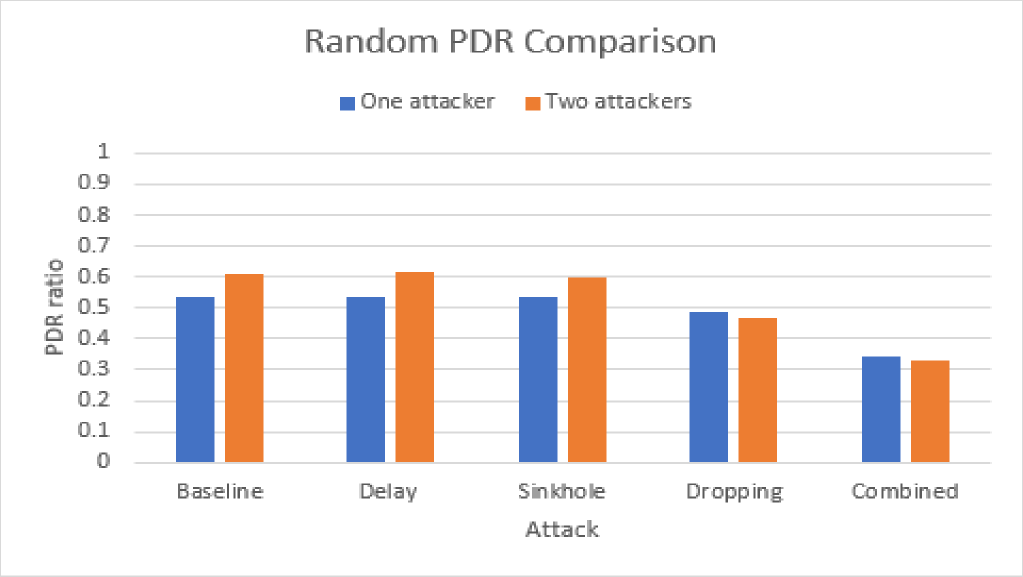

Figure 8. PDR results' random distribution for all attacks.

The dropping attack exhibits a distinct impact compared to delay and sinkhole attacks. Unlike the latter, which disrupt routing or delay packets, the dropping attack directly discards packets upon receiving them. This aggressive behavior leads to a significant reduction in the PDR. In the randomly distributed network, the average PDR plummets from a baseline of 0.607 to 0.467.

6.1.2. Uniform Node Distribution Results

In stark contrast with the random network, the uniformly distributed network exhibits remarkable resilience against the dropping attack. Here, even the dropping attack, known for its disruptive nature, has a minimal effect on the PDR. The average PDR for the uniform network only experiences a slight decrease, dropping from a near-perfect baseline of 0.999 to 0.982. See Figure 9.

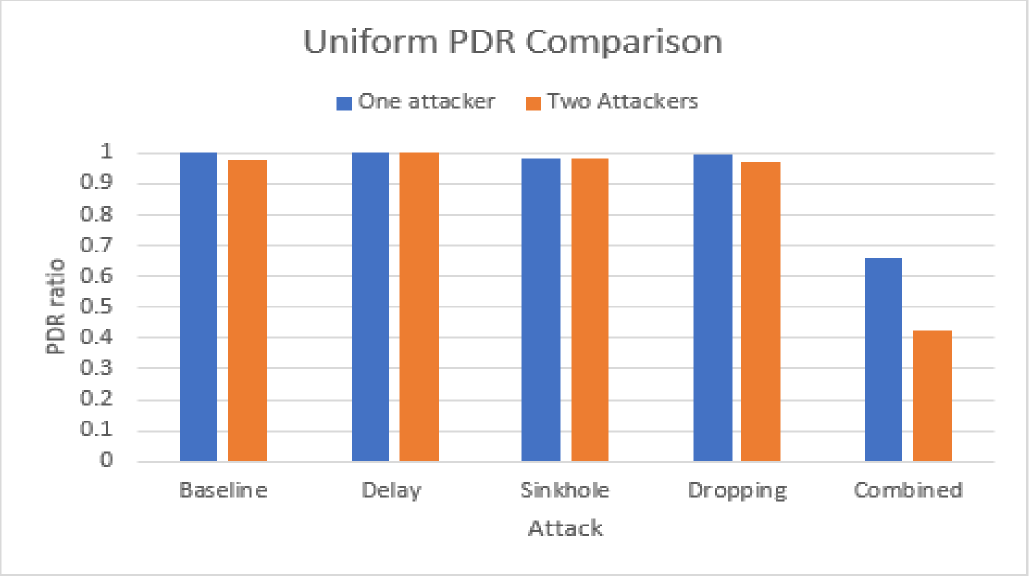

Figure 9. PDR results' uniform distribution for all attacks.

The combined attack, incorporating both dropping and sinkhole functionalities (black hole attack), demonstrates a significant impact on the PDR in both network distributions. However, the severity of the impact differs between the two network types:

- Random network: The random network experiences a substantial decrease in the PDR under the combined attack, with the average PDR dropping from a baseline of 0.607 to 0.307. This represents a decrease of approximately 50.16%.
- Uniform network: While the uniformly distributed network maintains a higher PDR compared to the random network even under attack (0.419 vs. 0.307), the combined attack has a proportionally larger effect on its performance. The uniform network's PDR suffers a decrease from a near-perfect baseline of 0.999 to 0.419, representing a decline of approximately 57.54%.

6.2. Throughput Results

6.2.1. Random Node Distribution Results

Similar to the observations for the packet delivery ratio (PDR), the impact of dropping attacks on the throughput exhibits a distinct pattern across network distributions, as seen in Figures 10 and 11.

The random network experiences a noticeable decrease in throughput when under a dropping attack. Throughput drops from a baseline of 22,371,978 bits per second to 17,200,434 bits per second, representing a decline of approximately 23%.

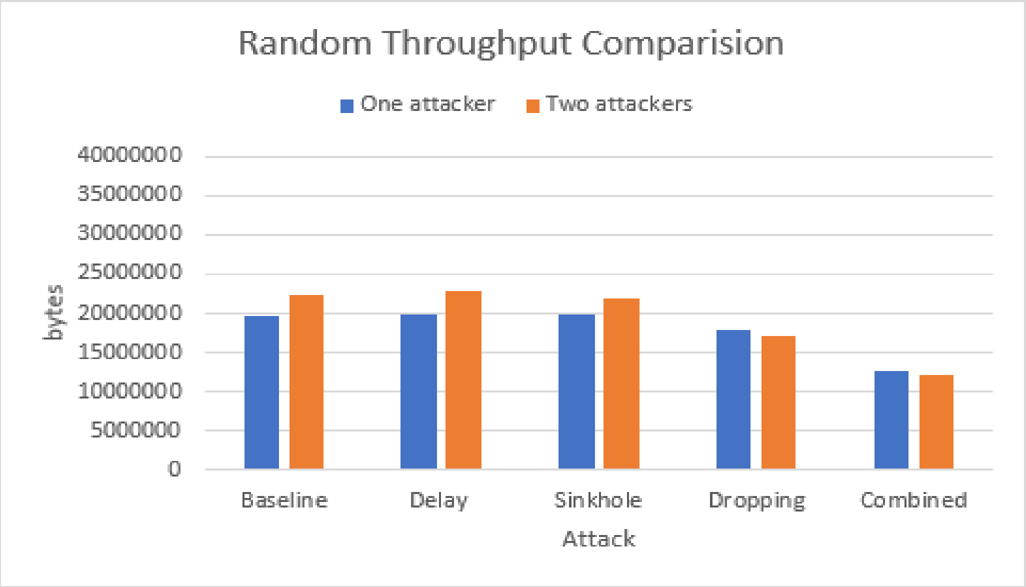

Figure 10. Throughput results' random distribution for all attacks.

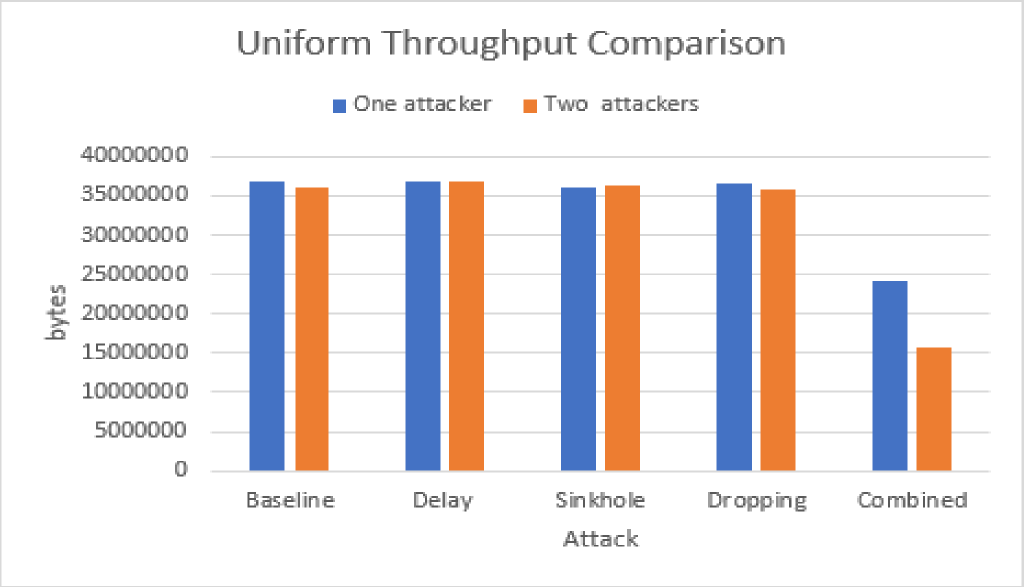

Figure 11. Throughput results' uniform distribution for all attacks.

6.2.2. Uniform Node Distribution Results

Once again, the uniformly distributed network demonstrates resilience. Unlike the random network, it shows minimal to no observable impact on throughput under the dropping attack. The significant decrease in throughput for the random network under attack can be attributed to the dropping attack's nature. By discarding packets, this attack disrupts successful data transmission, leading to a reduction in the overall network throughput. The uniform network, on the other hand, appears to be more adept at routing around dropped packets, potentially due to its inherent redundancy in node placement.

Both network distributions experience a significant decline in throughput under the combined attack, which discards packets and disrupts routing functionalities. The random network's throughput plummets from a baseline average of 21.21 megabits per second to a new value of 12.66, representing a 40% drop under the combined attack. Similarly, the uniform network, despite its resilience to individual attacks, suffers a substantial decrease in throughput, dropping from its baseline average of 36.41 megabits per second to a new value of 19.77, a 46% drop in throughput.

6.3. End-to-End Delay Results

6.3.1. Random Node Distribution Results

The movement patterns of attacker nodes significantly influence their effectiveness in delaying packets within the randomly distributed network. Both single and double attacker scenarios exhibit a strategic initial movement: approaching the root node first.

It is crucial to recognize this initial starting movement pattern of the attackers when considering the impact on end-to-end delay from both dropping and combined attacks within the randomly distributed network. While one might expect delays to increase with attacker interference, the act of dropping packets removes them from the network entirely. This eliminates their contribution to the overall end-to-end delay calculation. Since the motion of the attackers primarily targets long-delay packets, their removal can lead to a reduction in the average end-to-end delay observed in the network, as seen in Figures 12 and 13.

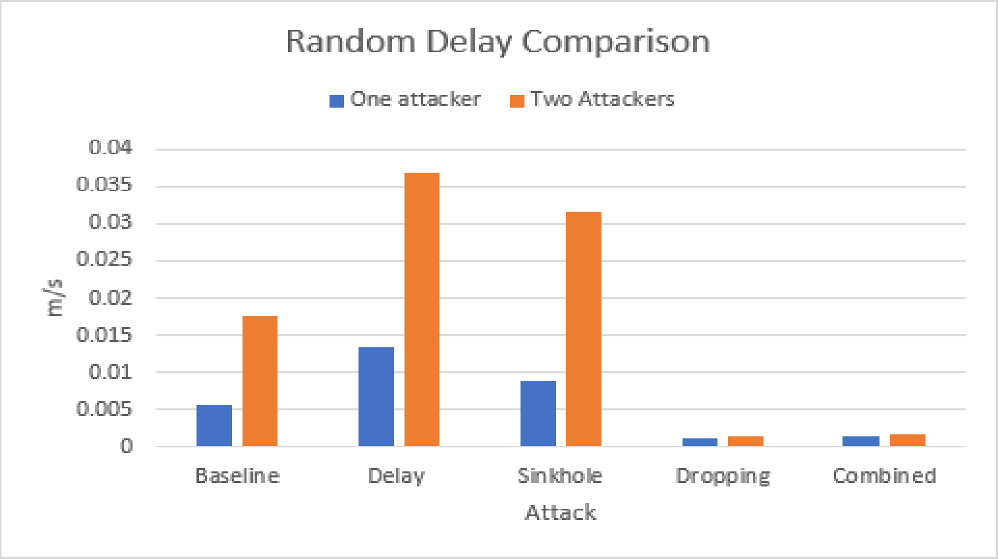

Figure 12. End-to-end results' random distribution for all attacks.

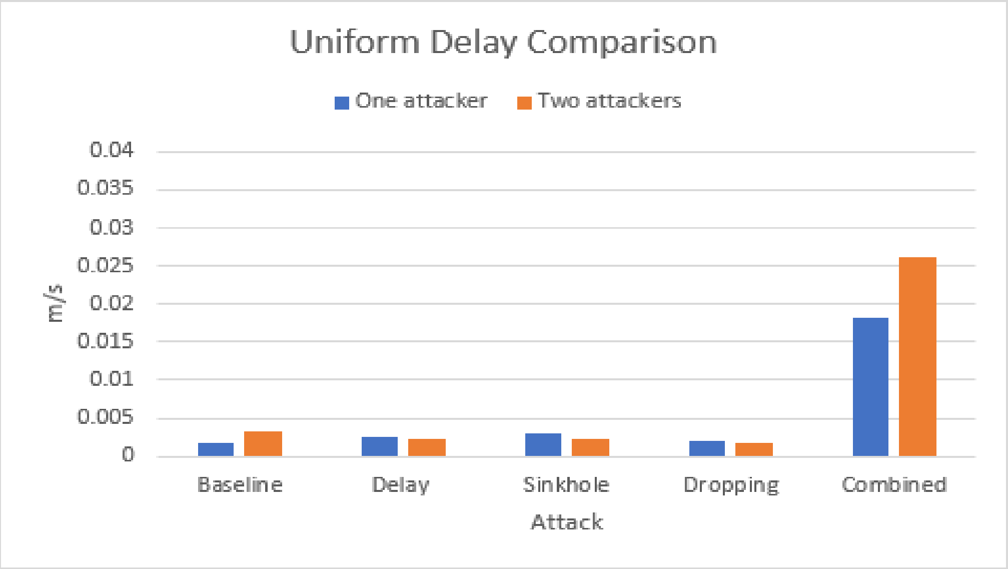

Figure 13. End-to-end results' uniform distribution for all attacks.

6.3.2. Uniform Node Distribution Results

This effect is not observed to the same extent in the uniformly distributed network with dropping attacks. This can be attributed to the decreased number of packets being dropped by the attack in the uniform network compared to the random network. The inherent redundancy in node placement within the uniform network may offer alternative routes for packets to bypass attackers, mitigating the impact of dropping attacks on end-to-end delay.

The uniform node distribution, while demonstrating resilience against individual dropping and sinkhole attacks, exhibits a significant increase in E2E delay when subjected to the combined attack. This unexpected behavior can be attributed to the interplay between the network topology, attacker mobility, and the combined attack's functionalities.

The presence of the combined sinkholes with dropping in the combined attack poses a significant threat to the uniform network's resilience. Strategically placed sinkholes, due to the network's inherent structure, can attract and discard a larger portion of packets compared to the random network. This effectively creates bottlenecks and increases E2E delay for packets that need to navigate around the sinkhole.

Overall, the combined attack's ability to disrupt both data transmission and routing exploits the uniform network's redundancy in a way that individual attacks cannot, leading to a noticeable increase in E2E delay.

7. Conclusions

This study investigates the impact of various attacks on MANETs through simulations. Two scenarios were explored involving stationary nodes under attack by mobile malicious nodes. The first scenario employed a random node distribution, while the second used a uniform distribution. Both scenarios evaluated network performance under dropping, delay, sinkhole, and combined sinkhole–dropping (black hole) attacks using the end-to-end delay, packet delivery ratio, and throughput metrics.

Our findings revealed that the network topology plays a crucial role in how MANETs are effected by attacks. While uniformly distributed networks may offer better resistance to individual attacks, they are more susceptible to sophisticated combined attacks like black hole attacks. Furthermore, our observations suggest that the movement patterns of attacking nodes within the network likely contribute to the observed effects.

Future Work

Future work should explore how variations in attacker movement patterns, such as initial positions, speed through the network, and potentially even 3D movement, influence the severity of attacks on different network topologies. Additionally, investigating the impact of varying node densities on attack effectiveness would provide valuable insights into network vulnerability. By examining these factors, more comprehensive security strategies and network configurations can be developed, ultimately enhancing resilience against diverse attack scenarios.

Author Contributions: Conceptualization, I.B.; Methodology, I.B.; Software, I.W.; Validation, I.B.; Investigation, I.B.; resources, I.W. and I.B.; data curation, I.B.; Writing—original draft preparation, I.B.; Writing—review & editing, I.W., B.G. and C.T.; Supervision, I.W.; project administration, I.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author/s.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ramanathan, R.; Redi, J. A brief overview of ad hoc networks: Challenges and directions. *IEEE Commun. Mag.* **2002**, *40*, 20–22. [CrossRef]
2. Mirza, S.; Bakshi, S.Z. Introduction to manet. *Int. Res. J. Eng. Technol.* **2018**, *5*, 17–20.
3. Ibrahim, K.L.; Azeez, L.I. Investigate the impact of three wormhole attacks on manet. In Proceedings of the 2021 13th IFIP Wireless and Mobile Networking Conference (WMNC), Virtual, 21–22 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 84–91.
4. Eltahlawy, A.M.; Aslan, H.K.; Abdallah, E.G.; Elsayed, M.S.; Jurcut, A.D.; Azer, M.A. A survey on parameters affecting MANET performance. *Electronics* **2023**, *12*, 1956. [CrossRef]
5. Al-Shareeda, M.A.; Manickam, S. Man-in-the-middle attacks in mobile ad hoc networks (manets): Analysis and evaluation. *Symmetry* **2022**, *14*, 1543. [CrossRef]
6. OMNeT++ Discrete Event Simulator. [Online]. Available online: https://omnetpp.org/ (accessed on 10 December 2023).
7. NESG-NETA. [Online]. Available online: https://nesg.ugr.es/index.php/en/neta-2 (accessed on 10 December 2023).
8. Al Rubaiei, M.H.; Jassim, H.S.; Sharef, B.T. Performance analysis of black hole and worm hole attacks in manets. *Int. J. Commun. Netw. Inf. Secur.* **2022**, *14*, 126–131. [CrossRef]
9. Deepika, D.; Saxena, S. Performance evaluation of aodv with self-cooperative trust scheme using jellyfish delay variance attack. In Proceedings of the 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 14–15 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1191–1196.
10. Sivanesh, S.; Dhulipala, V.S. Comparitive analysis of black hole and rushing attack in manet. In Proceedings of the 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW), Tiruchirappalli, India, 22–24 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 495–499.
11. Elshaikh, M. Black hole attack behavioral analysis general network scalability. *Indones. J. Electr. Eng. Comput. Sci.* **2019**, *13*, 677–682.
12. Sharma, A.K.; Noida, D.C.; Mishra, A. A study of energy optimization for manet. In Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 13–15 March 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 264–267.
13. Jain, B.; Soni, G.; Thapar, S.; Rao, M. A review on routing protocol of manet with its characteristics, applications and issues. *Int. J. Early Child. Spec. Educ.* **2022**, *14*, 2950–2956.
14. Singh, J.; Harsimran, K. A brief review: Routing protocols aodv and dsdv for manet. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 630.
15. Wali, S.; Ullah, S.I.; Khan, A.W.U.; Salam, A. A comprehensive study on reactive and proactive routing protocols under different performance metric. *Sukkur IBA J. Emerg. Technol.* **2018**, *1*, 39–51.
16. Kurkina, N.; Papaj, J. Performance analysis of AODV routing protocol and its modifications for MANET. In Proceedings of the 2023 World Symposium on Digital Intelligence for Systems and Machines (DISA), Kosice, Slovakia, 21–22 September 2023; pp. 140–144. [CrossRef]
17. Bai, Y.; Mai, Y.; Wang, N. Performance comparison and evaluation of the proactive and reactive routing protocols for manets. In Proceedings of the 2017 Wireless Telecommunications Symposium (WTS), Chicago, IL, USA, 26–28 April 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.
18. Shrivastava, P.K.; Vishwamitra, L. Comparative analysis of proactive and reactive routing protocols in vanet environment. *Meas. Sens.* **2021**, *16*, 100051. [CrossRef]
19. Kurode, E.; Vora, N.; Patil, S.; Attar, V. Manet routing protocols with emphasis on zone routing protocol–an overview. In Proceedings of the 2021 IEEE Region 10 Symposium (TENSYMP), Jeju, Republic of Korea, 23–25 August 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
20. Choudhary, S.; Narayan, V.; Faiz, M.; Pramanik, S. Fuzzy approach-based stable energy-efficient aodv routing protocol in mobile ad hoc networks. In *Software Defined Networking for Ad Hoc Networks*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 125–139.
21. Al-Dhief, F.T.; Sabri, N.; Salim, M.; Fouad, S.; Aljunid, S. Manet routing protocols evaluation: Aodv, dsr and dsdv perspective. In *MATEC Web of Conferences*; EDP Sciences: Les Ulis, France, 2018; Volume 150, p. 06024.
22. Deepak, S.; Anandakumar, H. Aodv route discovery and route maintenance in Manets. In Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 15–16 March 2019; pp. 1187–1191.
23. Hu, Y.; Luo, T.; Shen, J. An improvement of the route discovery process in aodv for ad hoc network. In Proceedings of the 2010 International Conference on Communications and Mobile Computing, Shenzhen, China, 12–14 April 2020; Volume 1, pp. 458–461.
24. Banerjee, B.; Neogy, S. A brief overview of security attacks and protocols in manet. In Proceedings of the 2021 IEEE 18th India Council International Conference (INDICON), Guwahati, India, 19–21 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
25. Yadav, N.; Chug, U. Secure routing in manet: A review. In Proceedings of the 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 14–16 February 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 375–379.
26. Nithyapriya, J.; Jothi, R.A.; Palanisamy, V. Protecting messages using selective encryption based esi scheme for manet. In Proceedings of the 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW), Tiruchirappalli, India, 22–24 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 50–54.
27. Meddeb, R.; Triki, B.; Jemili, F.; Korbaa, O. A survey of attacks in mobile ad hoc networks. In Proceedings of the 2017 International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia, 8–10 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–7.

28. Kumari, A.; Krishnan, S. Analysis of malicious behavior of black hole and rushing attack in manet . In Proceedings of the 2019 International Conference on Nascent Technologies in Engineering (ICNTE), Navi Mumbai, India, 4–5 January 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
29. Bharti, M.; Rani, S.; Singh, P. Security attacks in manet: A complete Analysis. In Proceedings of the 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 21–22 April 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 384–387.
30. Karthigha, M.; Latha, L.; Sripriyan, K. A comprehensive survey of routing attacks in wireless mobile ad hoc networks. In Proceedings of the 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 26–28 February 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 396–402.
31. Mankotia, V.; Sunkaria, R.K.; Gurung, S. DT-AODV: A dynamic threshold protocol against black-hole attack in MANET. *Sādhanā* **2023**, *48*, 190. [CrossRef]
32. Shrestha, S.; Baidya, R.; Giri, B.; Thapa, A. Securing black hole attacks in manets using modified sequence number in aodv routing protocol. In Proceedings of the 2020 8th International Electrical Engineering Congress (iEECON), Chiang Mai, Thailand, 4–6 March 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–4.
33. Pooja, B.P.; Manish, M.P.; Megha, B.P. Jellyfish attack detection and prevention in manet. In Proceedings of the 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS), Chennai, India, 4–5 May 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 54–60.
34. Alsafwani, N.; Ali, M.A.; Tahir, N.M. Evaluation of the mobile ad hoc network (manet) for wormhole attacks using qualnet simulator. In Proceedings of the 2021 IEEE 11th International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 6 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 46–49.
35. Shan, A.; Fan, X.; Wu, C.; Zhang, X.; Fan, S. Quantitative study on the impact of energy consumption based dynamic selfishness in manets. *Sensors* **2021**, *21*, 716. [CrossRef] [PubMed]
36. Kampitaki, D.G.; Economides, A.A. Selfishness in Mobile Ad-Hoc Networks: A Literature Review on Detection Techniques and Prevention Mechanisms. *IEEE Access* **2023**, *11*, 86895–86909. [CrossRef] [CrossRef]
37. Panda, N.; Pattanayak, B.K. Defense against co-operative black-hole attack and gray-hole attack in manet. *Int. J. Eng. Technol.* **2018**, *7*, 84–89. [CrossRef]
38. Mintu; Singh, G.; Gupta, P. To alleviate the flooding attack and intensify efficiency in manet. In Proceedings of the 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 15–17 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 87–94.
39. Kapu, V.K.; Karri, G.R. Efficient detection and mitigation of rushing attacks in VANET using RAID: A novel intrusion detection system. *J. Comput. Sci.* **2023**, *19*, 1143–1159. [CrossRef]
40. Aschenbruck, N.; Ernst, R.; Gerhards-Padilla, E.; Schwamborn, M. Bonnmotion: A mobility scenario generation and analysis tool. In Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques, Malaga, Spain, 15–19 March 2010.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.