International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 10-No.4 (2024) pp. 1584-1593
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Characterization of Destructive Nodes and Analysing their Impact in Wireless Networks

Srinivas Aluvala[1,2]*, V. Srikanth[3]

[1]Department of CSE, KL University, Guntur, India
[2]Department of CS & AI, SR University, Warangal, India
* **Corresponding Author Email:** srinu.aluvala@gmail.com - **ORCID:** 0000-0002-9864-8184

[3]Department of CSE, KL University, Guntur, India
Email: vsrikanth@kluniversity.in - **ORCID:** 0000-0002-0623-9691

Article Info:

DOI: 10.22399/ijcesen.726
Received : 04 December 2024
Accepted : 19 December 2024

Keywords :

Security,
MANET,
Destructive Node Characterization,
Secure Communications,
Protocol Dynamics.

Abstract:

Mobile Ad hoc Networks (MANETs) are being used to meet new requirements for efficiency and coordination in a variety of new public and residential contexts. Certain essential functions, including as resource management among network nodes, trust-based routing, and security for network maintenance, are not performed as well as they should because of the dynamic nature of wireless networks. Ad-hoc networks can also be attacked from different tiers of a network stack, and they are susceptible to secure communications. Destructive nodes have the ability to alter or reject routing parameters. They may also provide bogus routes in an attempt to intercept source data packets and pass them through. To handle the complexity arising from secure data exchange, some protocols have been developed. However, not all attack types can be detected and eliminated by a secure protocol in every scenario. Since security is not a feature that is built into MANETs, new secure wireless protocols need to concentrate on these issues. Thus, the analysis of destructive nodes' characteristics and effects on wireless networks in this research paper examined the behaviour of multiple attacks, their activities through neighbour selection, the establishment of paths from sources to destinations, and the dissemination of attack presence detection information to regular devices during path discovery and data transmission mechanisms. In order to categorize as legitimate, nodes must be constructed with safe transmission knowledge to provide trustworthy communication, validation, honesty, and privacy.

1. Introduction

A MANET is a grouping of different wireless devices, referred to as nodes, that fervently connect and exchange data with one another. These nodes may be Bluetooth-enabled laptops, desktop computers with wireless local area network cards, smartphones, tablets, PDAs, or other types of wireless communication devices. Nodes that are able to communicate with one another across wireless channels make up a MANET. Depending on the type of network that is accessible, it is also possible to establish communication with different nodes within a static architecture. MANETs can be utilized in a variety of scenarios, such as information sharing between industrial and environmental partners during disaster relief efforts, official meetings and education, earthquakes, hurricanes, defence personnel communication, and other types of information exchange in a battle zone. The definition of mobile ad-hoc is shown in figure 1, which also depicts the infrastructure and infrastructure-less model of the MANET communication structure. Generally speaking, a node is a computing device that broadcasts data over the air. According to the description, the node can be attached to a person, a moving object, or a roadside car to enable communication between them. A route between two nodes in this environment could have one or more MANET hops. Finding and maintaining pathways in a wireless network is a big problem since node mobility can lead to dynamic changes. For several reasons, protecting MANETs is more difficult than defending traditional networks.

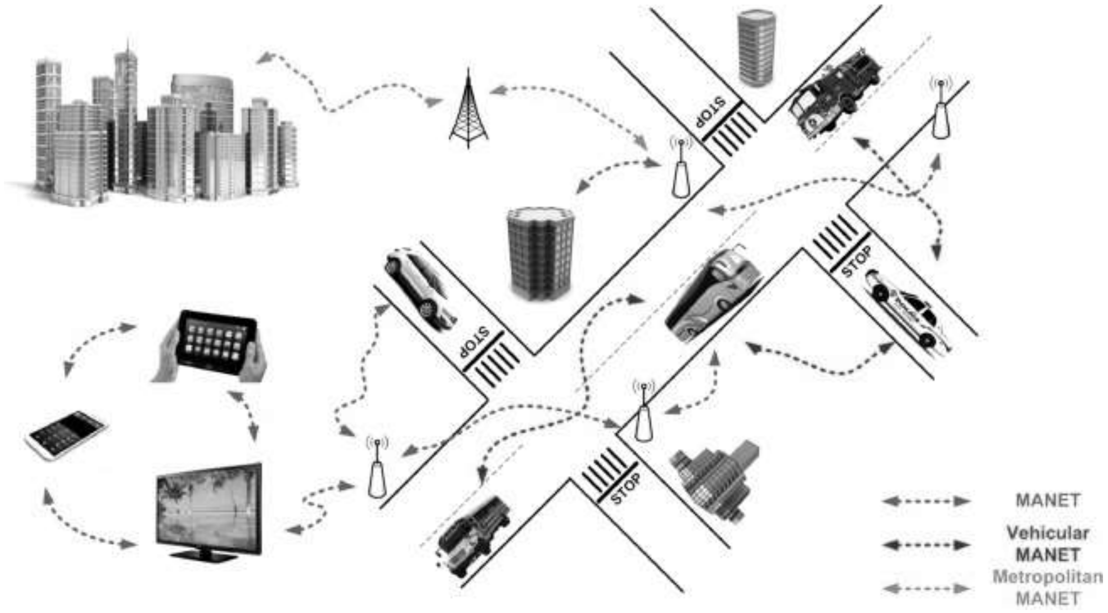

Figure 1: *Illustrates communication scenarios among MANETs*

Table 1: *Various benefits of wireless networks*

Benefit	Description
Dynamic Network Configuration	Network topology variables, such as the number of nodes, coverage, geography, and traffic counts, as well as packet size and rate, are incredibly simple to change.
Minimum deployment Cost	MANETs may be installed at a convenient location without the need for costly infrastructure like cables, connections, or towers. Manage wireless connections in a very short amount of time.
Battery Powered	Nodes can continue to operate on battery power even in the absence of a power source.
Connection	Through a wireless connection, anyone can join and leave at any moment.
Relocation	Nodes are able to move at any time from one area to another.

The network is inherently the least secure because to its unique features, which include unpredictability, channel listening, energy loss, mobility, security concerns, diversified device communication, channel scarcity, collision, congestion, noise, and interferences. In addition, MANETs have far less secure architecture because of their dynamic link connections, which are dependent on node migrations, network growth, application modifications, temperature, and other factors. Consequently, it is difficult to accurately describe activity that is legal. Therefore, due of the unexpected happenings, it is sometimes difficult to distinguish between malevolent and regular character. Within the network, a node can serve as the source for packet generation, the ultimate destination, or a forwarding intermediary for the transfer of data packets.

When a node forwards data, it functions as a routing device that receives and retransmits data to its neighbouring node, which is then directed towards the target. Occasionally, changes in the environment can cause the nature of a network to alter. Numerous benefits come with these wireless networks as shown in table 1. Wireless networks like MANETs have their challenges too. Every node in a MANET effectively functions as a router since all of the nodes that have been deployed help each new node send packets. The main issue with wireless routing is this. This puts networks' routing at risk.

The status of the clients can be maintained without the requirement for a fixed or centralized server. This raises the question of client loyalty. The dynamic nature of the network enables it to adapt to changing situations. As a result, protocols created for these kinds of settings need to be flexible enough to adapt to changes in the network. Due to their continuous interactions, the nodes that are positioned in unfavourable terrain and run on batteries have high energy power requirements. The main concern in this network is energy saving. Maintaining node identification (ID) is also a major issue in MANETs; duplication of IDs might be problematic because of open contact. Any MANET architecture requires a widely used method of ID allocation. Long route communication can lead to network and node delays. An extended delay can also be attributed to the routing loop. Another factor is buffer overloads, which cause packet waiting times. It is possible for unknown nodes to utilize the channel with the purpose of preventing other nodes from using it.

Attackers can create a bypass route to prevent legitimate communication. This significantly reduces the data loss. Thus, the results of throughput, packet delivery ratio, and overhead can have a significant impact, which reduces the overall performance of the network. It might be seen as legal or illegitimate because each node takes part in the route creation. Owing to dense networks, there is a possibility of network collapse, which suggests a change in each node's communication range. High network load can result in high congestion, energy loss, updating neighbours and the routing path, and high bandwidth use. Concurrent communication between several nodes causes a lot of noise and disturbance inside the network. The non-legitimate nodes have the ability to share bogus resource information with other nodes. This impacts the network greatly. Because of this, there may be a network jam in an emergency.

Because of their unique characteristics, MANETs are vulnerable to several assaults. Some attackers are difficult to identify because they operate in a public setting where all nodes cooperatively broadcast control and data packets throughout the network. As a result, designing a secure system for wireless communication is more difficult than for static cable networks. This study analyses a MANET's security objectives. Here, we explore several sample attack scenarios that pose security threats. The remainder of this document is formatted as follows: Section 2 covered the relevant literature. Section 3 outlines the several intriguing assaults on MANETs. The examined paper's conclusion is expressed in Section 4.

2. Related Work

This section reviews literature on different aspects of wireless networks particularly characterization of destructive nodes. A MANET is a wirelessly linked network of mobile routers that configures itself. The routers have unrestricted mobility and self-organization [1-4]. Thousands or even hundreds of mobile agents get an attack instruction from a DDoS "master program," and they use that information to execute flooding assaults against the target [1]. Wireless networks are especially vulnerable to radio signal interference because of their broadcast architecture, which prevents regular network connections. Jamming can occur by interference or collision at the receiver side, and it can interfere with wireless transmission and reception [5,6]. An attack that prevents authorized users from accessing the service provider or compromises service availability is known as denial of service [2]. Attackers are allowed to replace routes in any overheard packets while employing authentication and end-to-end authentication, and we presume that maliciously composed routes may only be included in messages sent by attackers [9]. When there is a little change in the protocols, the problem with the Internet is that it modifies the information that is necessary or mandatory. The foundation of the Internet architecture includes the creation of distributed denial-of-service [5]. Alpha-beta filtering can identify collusive assaults by malevolent nodes since it adapts its algorithm to the changing dynamics of the network [7,8]. This approach supports a larger working zone at the expense of increased physical layer complexity. Malicious nodes can use broadcasts that are forwarded by every node in the network to flood it with signals in an attempt to find the destination node that is out of range. Because nodes transmit packets in an ad hoc network, power consumption is higher [9,10]. The most serious kind of active assault jeopardizes the availability of broadband wireless networks, whereas passive attacks often affect secrecy and active attacks endanger integrity [3]. An adversarial or cloned node propagates the original node's node key or id, generating more copies of that node with the same id in the current network. This node has the potential to bring down the entire network [7].

Chen et al. [11] suggested detection approach enhances security by combining HHT with trust assessment. WSN's routing protocol is vulnerable to LDoS attacks. Grebremariam et al. [12] improved accuracy and efficient routing attack detection, hybrid machine learning supports safe localization in wireless sensor networks (WSNs). Chen et al. [13] suggested channel-based machine learning achieves an 84% authentication rate without the need for human labelling, making it perfect for industrial equipment in detecting clone and Sybil assaults. Nguyen et al. [14] attacked on LPW networks in the Internet of Things deplete device batteries. Research is required for strong remedies because the current defences are not flawless. Bendale and Prasad [15] presented fresh security issues brought on by D2D, mMIMO, and IoT. Future networks need to concentrate on intrusion detection. Ahmad et al. [16] used a specialized clustering approach, hybrid anomaly detection in WSN for misdirection and black hole attacks yields excellent accuracy. Yang et al. [17] While UWSNs are becoming more and more popular due to technological developments, this survey examines their susceptibility to security concerns.

Wu et al. [18] suggested a trust model for WSNs that takes energy, data trust, and communication into account to successfully fend against internal assaults. Aliady et al. [19] used energy-preserving techniques, the suggested solution detects wormhole assaults in WSNs with huge accuracy for 4-hop tunnels without the need for additional hardware. Ojha et al. [20] proposed SEIQRV model significantly reduces malware proliferation in WSNs while improving performance by combining vaccination and quarantine. Zhang et al. [21] observed that through experiments and simulations, their FORMAT framework demonstrates greater efficacy in detecting and mitigating cross-layer assaults in wireless networks through Bayesian learning. Islam et al. [22] enhanced WSN design with enhanced security, several DoS attacks and countermeasures are explored. In industries such as traffic monitoring, healthcare, and the military, wireless sensor networks collect critical data, but their lack of resources presents security risks. Xie et al. [23] due to resource constraints, wireless sensor networks, which are used in industries such as traffic monitoring, healthcare, and the military, are vulnerable to security breaches. Different DoS attacks and countermeasures are explored to help improve the security of WSN design.

Yuan et al. [24] explored an efficient SF-APIT method which is suggested to address Sybil assaults in WSNs' APIT localization techniques. With a high degree of accuracy and little overhead, SF-APIT uses Received Signal Strength (RSS) to detect and prevent Sybil attacks. Zhang et al. [25] investigated and observed through the use of sparse compressive matrices and asymmetric semi-homomorphic encryption, a secure data collecting system based on compressive sensing (SeDC) increases WSN security while improving privacy and lowering computing costs. Zhao et al. [26] assessed node trust through behavioural observation, exponential trust distribution, and indirect trust to successfully fend off internal assaults, the exponential-based Trust and Reputation Evaluation System (ETRES) improves WSN security. Moudni et al. [27] suggested ANFIS-PSO technique efficiently and with low false alarm rates detects black hole attacks in MANETs. Kalidoss et al. [28] presented the Secured QoS-aware Energy Efficient Routing Protocol for Wireless Sensor Networks. It uses cluster-based routing and trust modelling with authentication for secure communication. In simulations, the suggested SQEER algorithm enhances packet delivery, network longevity, and security. Poongodi et al. [29] investigated on security as well as speed of wireless networks. Routeing is interfered with by selective drop attacks, which target these networks. Defence is provided by RSDA, which integrates with AODV and ECDSA authentication to provide dependable routing. Fang et al. [30] observed that for WSNs, LEACH-TM is a trust-based hierarchical routing system that boosts security and energy economy. To extend the lifetime of the network and lessen the impact of rogue nodes, it makes use of trust management and dynamic cluster head selection. The literature has revealed the need for exploring destructive nodes and their characterization.

3. Characterization of Destructive Nodes

This section explores different kinds of destructive nodes or source of attacks or attack causing agents.

3.1 Attackers in Wireless Networks

Routing disruption attacks and resource wasting attacks are two frequent categories for non-legitimate routing assaults. When it comes to resource expenditure attacks, certain disruptive nodes may attempt to inject fake information in order to use the network resources; in the routing interruption model, the attacks aim to disrupt the routing mechanisms by redirecting packets of erroneous pathways.

As presented in table 2, different kinds of attacks and their characterization dynamics are provided. This information provides required knowhow on the attack space in wireless networks that are prone to various security risks.

3.2 Data Modifier Attack (DMA)

DMA attack involves the alteration of a small number of control packet fields in the data transmitted between nodes, which can lead to packet transmission errors, lost packets, or altered data. A handful of these malevolent attacks are covered in the next sections.

Erroneous sequence numbers for packets Sqn: In order to display a new path, attackers can alter the Sqn in path request or path reply messages. Attackers who misbehave occasionally get a path request (PREQ) intended for destination D from source S or intermediate I. When the attackers have the path reply PREP, they unicast to the next node, which has a maximum destination Sqn greater than the last Sqn that D announced. After agreeing to the PREP, node S sends the data packets to D via A. If the destination Sqn is less than the one broadcast by M when the initial PREP from D reaches S, S will reject that packet as a stale entry. Until an appropriate PREP with a maximum Sqn greater than that of A is received by source S, the state will remain unchanged. **False hop count:** By structuring a PREQ's hop count (HC) field differently from the minimum hop count, an attacker of this type can maximize the possibility that they are united in a freshly created path. Comparably, the HC field in the routing messages is altered to draw in the data

Table 2: *Different attacks and characterization*

Attackers	Types of Attacks	Characterization
Active Attacks	Data Modifier	This assault alters the valid data structure and attempts to make illegal changes to the data
	Denial of service	Prevent the normal usage of the channel by sending constant fake packets.
	Playback Attack	A playback attack involves reproducing the same data repeatedly or attempts to delay the delivery of the data.
	Duplication	Attempt to misuse the network resources Node ID duplication is a significant corruption technique involving duplication of nodes. Repeated data can be stored in memory to take up memory space.
Passive Attacks	Man in the Middle Attack	Attacks are positioned between two nodes and passively intercept the communication of messages.
	Packet analyser Attack	Examines the node's position based on the packet flows between nodes, Retrieve packet from encrypted format Knows the frequency and length of the packet
Adaptation	Misrouting Packet attackers	Redirect the data packet from its initial route to the wrong directions
	spoofing attacks	Spoofing attacks involve impersonating another node by intercepting IP, AR, or server activities. It has the ability to take data, circumvent network control, and distribute malware throughout the network
Grabbing	Wormhole attacks	In the wormhole attack, a worm node intercepts the packets at one location and transfers them to another location, where it may either partially or totally discard the packets.
	Black hole attacks	Packets are frequently dropped from an unreliable network; the black hole attack is difficult to detect and prevent. It raises its destination sequence number and behaves as a destination at times. It can randomly drop packets at random intervals.
Untruth Attack	Deficiency attacks	The primary goal is to utilize a significant amount of resources such as energy and bandwidth by keeping them active without any valid reason.
	Path rescue attacks	Data packets may fail to reach the intended destination due to the wireless nature, link loss, or the presence of an attacker.
Breaking attacks	Packet droppers	The packet droppers have the ability to directly disrupt the control packets.
	Flooding attacks	Challenger could disrupt the normal transmission process by sending an excessive amount of unnecessary packets to the destination.
	Non-Cooperative attacks	Lack of cooperation from the neighbours and routing nodes to complete the network operations initiated by the attackers

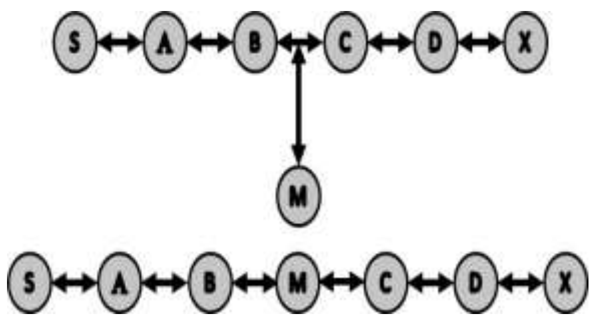

Figure 2: *Illustrates path collapse attack scenario*

packet, just like in the Sqn path-changing attack.

False route: The route collapse attack behaviour depicted in figure 2 makes it evident that the shortest path was found to connect S and D. It is also presumed that nodes C and X cannot hear one another, nor can B and D hear one another. Node M is an unruly node that is attempting to launch a denial of service (DOS) assault. Assume that S delivers data along the path S-A-B-C-D to D. This data packet is sent to B and C is removed from the routing list if M intercepts it. Since B cannot hear D, it is unlikely that B will convey this to D. Thus, M has successfully initiated a denial-of-service attack on D in an attempt to bring down the network.

3.3 Denial of Service

Similar to figure 3, the goal of this kind of attack is to stop authorized and legitimate users from using the network's services. Nodes were unable to communicate with a system during the DOS

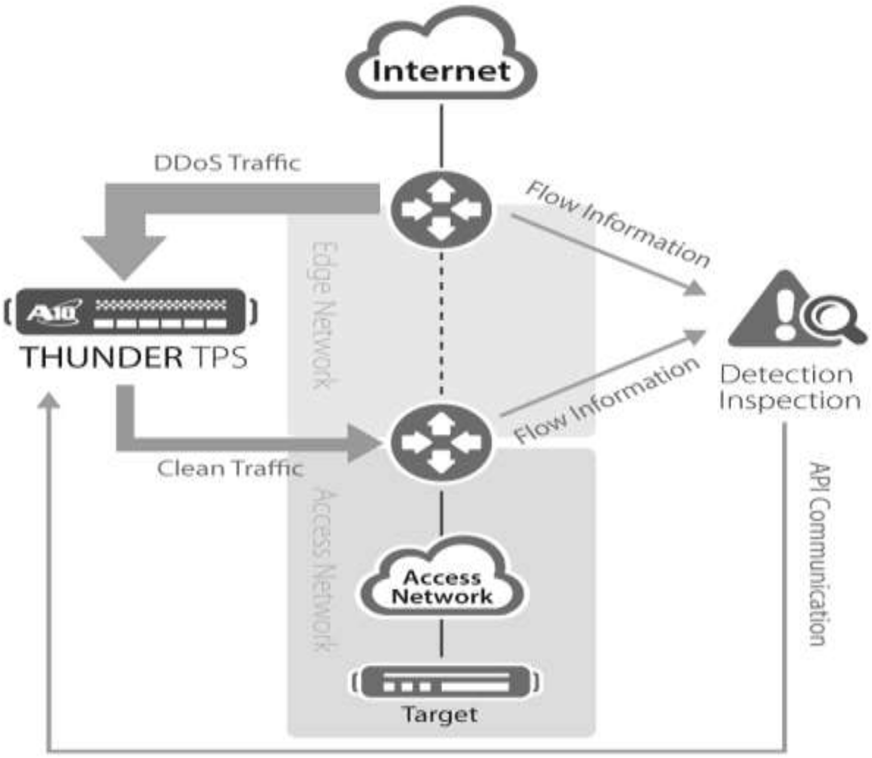

Figure 3: *Illustrates modus operandi of DoS attack*

assault. Current DOS attacks have left many websites unreachable to users for a period of time, resulting in important reputation, economists and some other losses.The behaviour of DOS attacks discussed below. The utilization of restricted resources, including network connectivity and capacity. Information on high sequence number configuration devastation or change. Potential harm or modifications to the network infrastructure. A defence against DoS assaults can be provided by the following real-world occurrences such as identification and removal, prompt protocol revision, separation of nodes and networks monitoring of flow.

3.4 Hijacking Communication Session

Attackers first extract the destination or forwarding node's IP address in order to get the precise sequence number. After then, the victim is treated like a DOS by the attacker. The destination thus gets crowded for a while. Thus, using the other node as a valid object, the hijacker continues the session.

3.5 Resource Utilization Attack

Because wireless networks are dynamic and each node's coverage area is limited, security is a significant concern. The depletion of network resources, such as bandwidth, energy, and node queue, is achieved by the malicious node by persistent broadcasting of control packets, which is known as a denial-of-service attack (DOS). This decreases performance. Detection of this attack can be found through nodes exchanging resource information and track heavily resource-used nodes using a protocol.

3.6 Duplication Attacks

Attacks that replicate data in a network to violate privacy and sincerity. It is possible for an attacker to alter someone's perception of the network by copying the node address of another device. Figure 4. lists the following as possible attackers.

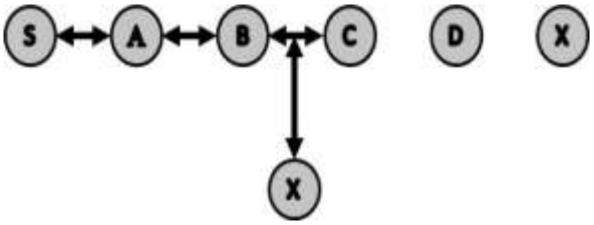

Figure 4: *Illustrates dynamics duplication attack*

Node S initiates a PREQ procedure with the intention of sending data to X. The misbehaving attacker M duplicates the destination ID X as misbehaving node ID X' since he is closer to S than X. S receives PREP from the misbehaving node. Without verifying the authenticity of the PREP, Source S starts sending data to the misbehaving node because it believes the path to the PREP. A route loop between a few network nodes may result from this sort of malicious activity.

3.7 Grabbing Attack

Grabbing attacks attempt to stop a process by injecting control packets or fake messages. These attacks are challenging to keep an eye on in a network as the data appears to the nodes distributing it as authentic communications. A fabrication assault is demonstrated in figure 5.

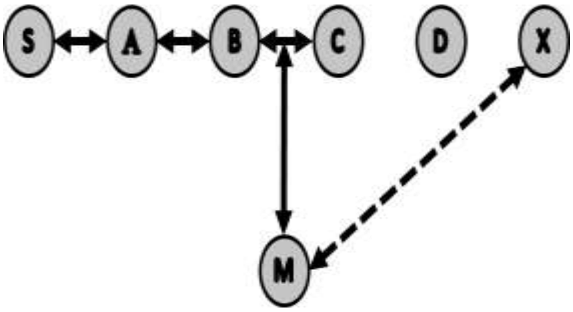

Figure 5: *Illustrates scenario of grabbing attack*

In order to receive the path to X, Source S must broadcast PREQ in order to convey data to X. Misbehaving node M sends PREP to the S while pretending to have a cached route to the X. Without verifying the PREP, the S node accepts it and begins sending data to M. Furthermore, misbehaving nodes may provide route errors that encourage a network's link to detach from a particular node.

3.8 Tunnelling Wormhole Attack

A severe kind of assault known as a "wormhole attack" allows two worm nodes to exchange packets via a private "tunnel" within the network, as illustrated in figure 6. A worm1 node accepts control and data packets at one location in the network and tunnels them to the next location, where they are transmitted out into the environment, while the worm is present in the network. Wormholes are the tunnelling between two linked attackers.

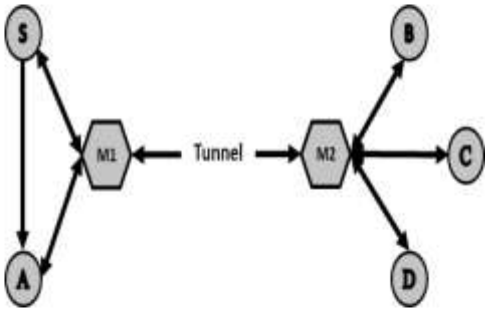

Figure 6: *Illustrates tunnelling wormhole scenario*

The two worm nodes in this instance, M1 and M2, join via a private link. Every packet that M1 receives from the source is then passed via a linked "worm node" called M2. A worm node uses tunnelling to stop routing and provides the shortest path. These kinds of malicious activity can severely disrupt node-to-node communication and are difficult to detect in a network. Detection of such attack can be done through the detection method of neighbour list analysis, detection based on hop counts, route-based detection based on time and location-based identification of worm nodes.

3.9 Black Hole Attack

By pretending to be a destination, the node tries to attract packets to itself in this attack. All nodes in the vicinity of the black hole must route data towards it since a node reports a zero value for each destination result. Any wireless protocol may be attacked by a black hole assault of this kind. In a flooding-based environment, a black hole attends to the route demands for the networks. The black hole enters the pathway to interact with the packets passing between it and, upon hearing a path request for a path to the destination, creates a reply with an incredibly short route. The steps for finding a black hole are listed below. Step 1: The destination sequence number is validated. Step 2: Distributing valid certificates between authorised nodes in order to safeguard the packet metrics. Step 3: Legitimate nodes keeping an eye on harmful purpose nodes. Step 4: By comparing them with the certificates that are contained in their directory and all path lengths, the source and destination verify the authenticity of the paths and documents.

3.10 Jamming Attack

When launching a jamming assault, the attacker begins monitoring the communication channel to see how frequently packets from the source are arriving at the target.

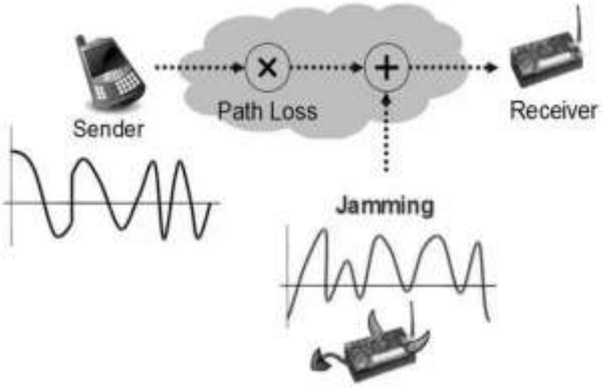

Figure 7: *Illustrates the scenario of jamming attack.*

As seen in figure 7, the attacker then begins to send the packets with that frequency, causing error-free reception at the destination to halt.

3.11 Vampire Attack

A challenger creates messages using deliberate launch routing loops in our vampire assault. Given that figure 2 illustrates how it distributes packets in a circular loop, we refer to it as the vampire attack. By creating limited confirmation of packet headers at forwarding nodes, it seeks to contaminate routing by permitting some packets to repeatedly flow via the same nodes. Additionally, as figure 8. illustrates, it lengthens the path to rapidly deplete the node's lifetime.

Numerous studies investigate various mitigating strategies to minimize vampire injury and discover that although the assault may be easily avoided with very little control overhead, the wider vampire attack remains extremely difficult. The first safety method we covered was routing, in which any intermediary node that knows a quick path to the destination might resend the data packet. We switch from detection to assurance that a packet travels over the network in the second validation. Every node ensures that the packet makes it across every hop that gets it closer to its final destination.

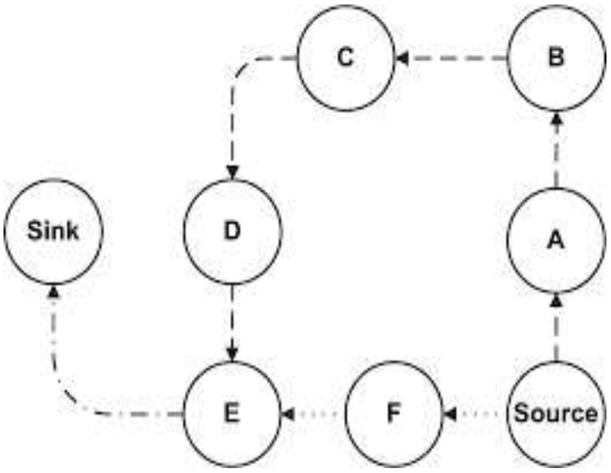

Figure 8: *Illustrates dynamics of vampire attack.*

The dynamic nature of wireless networks and the limited coverage areas of individual nodes provide significant security challenges. The effect of resource usage assault is similar to a denial-of-service attack (DoS) in which a malicious node continuously broadcasts control packets to lower network resources including bandwidth, energy, and node queue in an effort to limit performance. A number of other attacker behaviours are present in network communications. Several of these were covered previously. The next section covers two secure routing methods for ad hoc wireless networks. An attacker can depart from the regularity of the network by using similar behaviour and different ways of being present. Wireless communication is often considered to be very unsafe if the built-in protocol lacks security awareness. Every regular node should be constructed with a security monitoring knowledge protocol directed towards all neighbouring and route nodes. By doing this, network degradation and loss are avoided. Security is important and used in different works [31-40].

4. Conclusion and Future Work

With varying attackers and a large number of misbehaving nodes, the attackers may disrupt the network significantly. They are skilled at creating malicious scenarios and misbehaving nodes. The ultimate goal of a protocol is to transfer data from source to destination in an efficient manner; in this case, receiving packets from legitimate nodes is quite simple and there is no malicious node present. Once an attacker has established a variety of maladaptive settings inside the network, the impact of network damages may be verified by comparing the received packets with the previous packets, which can disclose the packet loss based on the overhead values. This occurs when data is sent in the wrong way by an attacker or unknown source; in certain situations, packets may be discarded as a result of inappropriate behaviour. This leads to the conclusion that routing methods need to be designed with knowledge of secure transmission while keeping an eye on network changes. The design of the wireless protocol could prevent different attacks requires further research. In future we intend to develop a secure protocol for wireless networks.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Qiang Huang, Hisashi Kobayashi, and Bede Liu. (2003). Modeling of Distributed Denial of Service Attacks Wireless Networks. *IEEE Pacific Rim Conference on Communications Computers and Signal Processing (PACRIM 2003)* (Cat. No.03CH37490), Victoria, BC, Canada, 1;41-44 doi: 10.1109/PACRIM.2003.1235714.

[2] Lawan A. Mohammed and BijuIssac. (2006). Detailed DoS Attacks in Wireless Networks and Countermeasures, *Int. J. Ad Hoc and Ubiquitous Computing,* 2(3):157-166 DOI:10.1504/IJAHUC.2007.012417

[3] Shafiullah Khan, Kok-Keong Loo1, Tahir Naeem, Mohammad AbrarKhan. (2008). Denial of Service Attacks and Challenges in Broadband Wireless Networks, *IJCSNS International Journal of Computer Science and Network Security*, 8(7);

[4] Sreedhar. C, Dr. S. MadhusudhanaVerma and Dr. N. Kasiviswanath. (2010). Potential Security Attacks on Wireless Networks and Their Countermeasure, *International journal of computer science & information Technology (IJCSIT)* 2(5) DOI:10.5121/ijcsit.2010.2506

[5] KuldeepTomar, and S.S Tyagi. (2014). Quantifying the Impact of Flood Attack on Transport Layer Protocol, *International Journal on Computational Sciences & Applications (IJCSA)* Vol.4, No.6.

[6] Pratibha S. Gaikwad, Prof. S. P. Pingat. (2015). Preventing Jamming and Replay Attack in Wireless Applications, *International Journal of Innovative Research in Computer and Communication Engineering*, 3(7). DOI: 10.15680/ijircce.2015. 0307024

[7]Megha Sharma, RajshreePurohit. (2015). Node Replication Attack Detection Technique in Wireless Sensor Network – A Survey, *International Journal of Electrical, Electronics and Data Communication*, 3(8).

[8] H. Khosravi, R. Azmi, and M. Sharghi. (2016). Adaptive Detection of Hello Flood Attack in Wireless Sensor Networks, *International Journal of Future Computer and Communication,* 5(2). DOI:10.18178/ijfcc.2016.5.2.452

[9] Devikarani Roy, ShilpaVerma. (2016). Vampire Attacks: Detection And Prevention, *International Journal of Computer Techniques* – 3(3).

[10] JasmeenMangat, Er. JaspreetKaur (2017). Review on the Flooding Attacks in Mobile Ad Hoc Networks, *International Journal of Advanced Research in Computer Science and Software Engineering,* 7(4). 390-392. DOI:10.23956/ijarcsse/V7I4/0218

[11] Chen, Hongsong; Meng, Caixia; Shan, Zhiguang; Fu, Zhongchuan; Bhargava, Bharat K. (2019). A novel Low-rate Denial of Service attack detection approach in ZigBee wireless sensor network by combining Hilbert-Huang Transformation and Trust Evaluation. *IEEE Access,* 7;32853–32866. doi:10.1109/ACCESS.2019.2903816

[12] Gebrekiros Gebreyesus Gebremariam, J. Panda, S. Indu b. (2023). Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning mode. *Alexandria Engineering Journal* 82(1);82-100 https://doi.org/10.1016/j.aej.2023.09.064

[13] Chen, Songlin; Pang, Zhibo; Wen, Hong; Yu, Kan; Zhang, Tengyue; Lu, Yueming. (2020). Automated Labeling and Learning for Physical Layer Authentication against Clone Node and Sybil Attacks in Industrial Wireless Edge Networks. *IEEE Transactions on Industrial Informatics,* pp.1–11. doi:10.1109/TII.2020.2963962.

[14] Nguyen, Van-Linh; Lin, Po-Ching; Hwang, Ren-Hung. (2019). Energy Depletion Attacks in Low Power Wireless Networks. *IEEE Access,* 7;51915–51932. doi:10.1109/ACCESS.2019.2911424

[15] Bendale, Shailesh Pramod; Rajesh Prasad, Jayashree. (2018). [IEEE 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN) - Lonavala, India *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN) - Security Threats and Challenges in Future Mobile Wireless Networks.* pp.146–150. doi:10.1109/GCWCN.2018.8668635.

[16] Ahmad, Bilal; Jian, Wang; Ali, Zain Anwar; Tanvir, Sania; Khan, M. Sadiq Ali. (2018). Hybrid Anomaly Detection by Using Clustering for Wireless Sensor Network. *Wireless Personal Communications*, pp.1 – 13. doi:10.1007/s11277-018-5721-6.

[17] Yang, Guang; Dai, Lie; Si, Guannan; Wang, Shuxin; Wang, Shouqiang. (2019). Challenges and Security Issues in Underwater Wireless Sensor Networks. *Procedia Computer Science,* 147;210–216. doi:10.1016/j.procs.2019.01.22.

[18] Wu, Xiaoling; Huang, Junjie; Ling, Jie; Shu, Lei. (2019). BLTM: Beta and LQI based Trust Model for Wireless Sensor Networks. *IEEE Access*, 4;1–12. doi:10.1109/ACCESS.2019.2905550

[19]Aliady, Wateen A.; Al-Ahmadi, Saad A. (2019). Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks. *IEEE Access,* 7;84132–84141. doi:10.1109/ACCESS.2019.2924283

[20]Ojha, RudraPratap; Srivastava, Pramod Kumar; Sanyal, Goutam; Gupta, Nishu (2020). Improved Model for the Stability Analysis of Wireless Sensor Network Against Malware Attacks. *Wireless Personal Communications,* pp.1–24. doi:10.1007/s11277-020-07809-x.

[21] Zhang, Liyang; Restuccia, Francesco; Melodia, Tommaso; Puldlewski, Scott. (2018). Taming Cross-Layer Attacks in Wireless Networks: A Bayesian Learning Approach. *IEEE Transactions on Mobile Computing,* pp.1–14. doi:10.1109/TMC.2018.2864155

[22] Islam, Mohammad NafisUl; Fahmin, Ahmed; Hossain, Md. Shohrab; Atiquzzaman, Mohammed. (2020). Denial-of-Service Attacks on Wireless Sensor Network and Defence Techniques. *Wireless Personal Communications,* pp.1–29. doi:10.1007/s11277-020-07776-3 .

[23]Xie, Haomeng; Yan, Zheng; Yao, Zhen; Atiquzzaman, Mohammed. (2018). Data Collection

for Security Measurement in Wireless Sensor Networks: A Survey. *IEEE Internet of Things Journal*, pp.1–22. doi:10.1109/JIOT.2018.2883403 .

[24] Yuan, Yali; Huo, Liuwei; Wang, Zhixiao; Hogrefe, Dieter. (2018). Secure APIT Localization Scheme against Sybil Attacks in Distributed Wireless Sensor Networks. *IEEE Access*, pp.1–8. doi:10.1109/ACCESS.2018.2836898

[25] Zhang, Ping; Wang, Shaokai; Guo, Kehua; Wang, Jianxin. (2018). A secure data collection scheme based on compressive sensing in wireless sensor networks. *Ad Hoc Networks*, 70;73–84. doi:10.1016/j.adhoc.2017.11.011

[26] Zhao, Jin; Huang, Jifeng; Xiong, Naixue. (2019). An Effective Exponential-based Trust and Reputation Evaluation System in Wireless Sensor Networks. *IEEE Access*, 7;33859–33869. doi:10.1109/ACCESS.2019.2904544

[27] Lyu, Chen; Zhang, Xiaomei; Liu, Zhiqiang; Chi, Chi-Hung. (2019). Selective Authentication based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things against DoS Attacks. *IEEE Access*, 7;31068–31082. doi:10.1109/ACCESS.2019.2902843

[28] Kalidoss, Thangaramya; Rajasekaran, Logambigai; Kanagasabai, Kulothungan; Sannasi, Ganapathy; Kannan, Arputharaj. (2019). QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks. *Wireless Personal Communications*, pp.1-22 –. doi:10.1007/s11277-019-06788-y

[29] Poongodi, T; Khan, Mohammed S.; Patan, Rizwan; Gandomi, Amir H.; Balusamy, Balamurugan. (2019). Robust Defence Scheme Against Selective Drop Attack in Wireless Ad Hoc Networks. *IEEE Access*,.1-11. doi:10.1109/ACCESS.2019.2896001.

[30]Weidong Fang; Wuxiong Zhang; Wei Yang; Zhannan Li; Weiwei Gao; Yinxuan Yang. (2021). Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. *Digital Communications and Networks*,pp.1–3. doi:10.1016/j.dcan.2021.03.005.

[31]El-Taj, H. (2024). A Secure Fusion: Elliptic Curve Encryption Integrated with LSB Steganography for Hidden Communication. *International Journal of Computational and Experimental Science and Engineering*, 10(3);434-460. https://doi.org/10.22399/ijcesen.382

[32]Prasada, P., & Prasad, D. S. (2024). Blockchain-Enhanced Machine Learning for Robust Detection of APT Injection Attacks in the Cyber-Physical Systems. *International Journal of Computational and Experimental Science and Engineering*, 10(4);799-810. https://doi.org/10.22399/ijcesen.539

[33]R, U. M., P, R. S., Gokul Chandrasekaran, & K, M. (2024). Assessment of Cybersecurity Risks in Digital Twin Deployments in Smart Cities. *International Journal of Computational and Experimental Science and Engineering*, 10(4);695-700. https://doi.org/10.22399/ijcesen.494

[34]M. Swetha, & G. Appa Rao. (2024). Hybrid Ensemble Lightweight Cryptosystem for Internet of Medical Things Security. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1528-1540. https://doi.org/10.22399/ijcesen.625

[35]Sushma Polasi, & Hara Gopal Venkata Vajjha. (2024). Secure Drone Communications using MQTT protocol. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1282-1289. https://doi.org/10.22399/ijcesen.685

[36]Rahul SHANDILYA, & R.K. SHARMA. (2024). ProTECT: A Programmable Threat Evaluation and Control Unit for Zero Trust Networks. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1372-1378. https://doi.org/10.22399/ijcesen.673

[37]MOHAMED, N. N., Yulianta SIREGAR, Nur Arzilawati MD YUNUS, & Fazlina MOHD ALI. (2024). Modelling the Hybrid Security Approach for Secure Data Exchange: A Proof of Concept . *International Journal of Computational and Experimental Science and Engineering*, 10(4)1475-1485. https://doi.org/10.22399/ijcesen.344

[38]Guven, M. (2024). A Comprehensive Review of Large Language Models in Cyber Security. *International Journal of Computational and Experimental Science and Engineering*, 10(3);507-516. https://doi.org/10.22399/ijcesen.469

[39]C, A., K, S., N, N. S., & S, P. (2024). Secured Cyber-Internet Security in Intrusion Detection with Machine Learning Techniques. *International Journal of Computational and Experimental Science and Engineering*, 10(4);663-670. https://doi.org/10.22399/ijcesen.491

[40]Kosaraju Chaitanya, & Gnanasekaran Dhanabalan. (2024). Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection in Wireless Sensor Networks. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1462-1474. https://doi.org/10.22399/ijcesen.613