A Fuzzy Knowledge-Based Approach for End-2-End Behavioural Analysis of Wormhole Attacks on Mobile Ad-Hoc Networks

Imeh Umoren, Ekemini Okpongpong and Ifreke Udoeka
Department of Computer Science, Faculty of Physical Sciences
Akwa Ibom State University, Mkpato Enin, Nigeria
Email: imehumoren@aksu.edu.ng

Abstract

Mobile Ad hoc Networks (MANETs) involve series of travelling nodes communicating with each other without a fixed Set-up. Certainly, MANETs are networks that utilize communication peripatetic nodes such as; Personal Digital Assistants (PDAs), mobile phones, laptops which enable wireless transmission across an area and forwarding data packets to the other nodes resulting in frequent change in topology. MANETs are exposed to several communication assaults such as *active attack* and *passive attack*. The active attack disrupts network operations while the passive attack obtains information without upsetting normal networks operation. Wormhole is a typical case of active attack. Indeed, an attacker receives packets at one end of the network, tunnels them to another end of the network, and then replays them into the networks from that point resulting in a collapse in communication across wireless setups. This research work simulates and models a typical wormhole attack in MANET using Network Simulator (NS-2.35) and Fuzzy Inference System (FIS). The *End-2-End* behavioural analysis of wormhole attacks on the transmitting networks layer of MANET was realized. To detect the level of wormhole attack in the network several parameters such as *Packet Delivery Ratio*, *Packet Forwarding Probability* and *Packet Dropping Probability* were considered by determining the degree of severity of wormhole attack which may upset the Quality of Service (QoS) delivery. The aim of this research paper is in the direction of Network security optimization.

Keywords: *Wormhole attack, Mobile Adhoc Networks, Fuzzy Inference System, Packet Node*

1. Introduction

The term “Ad hoc” is a Latin phrase which means “for this purpose”, therefore ad hoc networks are used for a particular purpose. Ad hoc networking can be applied where there is little or no communication infrastructure. There are various types of ad hoc networks such as; Vehicular Ad hoc Network, Mobile Ad hoc Network, Smartphone Ad hoc Network, Wireless Sensor Network, etc. Among these various types of ad hoc networks, this project will focus on the Mobile Ad hoc Network (MANET). [7] defines Mobile Ad hoc Network (MANET) as an autonomous system which consists of a collection of self-configurable mobile nodes connected through wireless links. MANETs that may require secure communication network include but is not limited to the following areas: military or police communication network, safety operations in oil drilling platforms, critical business application, safety operations in hospital (emergency), warzone, etc. MANET has some challenges which makes it vulnerable to attacks which are; absence of centralized infrastructure, dynamic topology, lack of resource constraints such as; power capacity, memory. The nodes in a MANET are free to move in any direction independently, they leave and join the network randomly. Compared to wired networks, MANET has more security issues and many types of attacks can be initiated on such networks, these attacks can be either passive or active. [13] stated that in passive attacks, the attacker obtains information without disturbing normal network operation and is difficult to detect since the operation of network is not affected while in an active attack, an attacker can be internal (within the network) or external (outside the network) and can disturb network operation by

modifying or deleting information, injecting a false message or impersonating a node. A typical example of an active attack is known as a **wormhole attack**.

A wormhole attack is usually performed by two or more malicious nodes. [1] defined wormhole attack as the most frequently occurring attack in ad hoc networks in which one malicious node tunnels the packets from its location to other defective nodes.

[19] described wormhole attack as where an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two attackers are called wormhole. The wormhole attack is difficult to detect because the attackers can launch the attack without revealing their identity.

This end-2-end behaviour of wormhole is due to the fact that the tunnel formed by the wormhole is from one end of the network to the other end of the network (i.e. from source to destination). In this research project, the focus is on the study of wormhole attack, some detection methods and techniques to prevent occurrences of attack in mobile ad hoc networks. The remainder of this paper is structured as follows: Section 2 provides a review of related literature on typical wormhole attack in MANET. Section 3 presents the materials and method employed in the research. Section 4 presents the results obtained from the study. Section 5 discusses the results with reference to existing literature. Section 6 concludes on the paper and points to future research direction.

2. Literature Review

In [20] paper presented an approach for detecting and defending against wormhole attacks called packet leashes, and the specific protocol called TIK (TESLA with Instant Key disclosure) that implements leashes. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Packet leashes provide a way for a sender and a receiver to be certain that a wormhole attacker is not causing the signal to propagate further than the specified normal transmission distance. There are two types of leashes; geographical leashes and temporal leashes. These two types of leashes can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet travelled further than the leash allows.

To implement temporal leashes, they presented the design and performance analysis of a protocol called TIK, which provides authentication of received packets. TIK enables the receiver to detect a wormhole attack. They observed that a receiver can verify the TESLA security condition as it receives the packet this fact allows the sender to disclose the key in the same packet. They described the stages of the TIK protocol in detail: sender setup, receiver bootstrapping, and sending and verifying authenticated packets.

[17] proposed a Handover Manageability and Performance Model for Mobile Communication Networks then formulated a model for soft handoff in CDMA networks by initiating an overlap region between adjacent cells which facilitating the derivation of handoff manageability performance model. The paper employed an empirical modeling approach to support their analytical findings, measure and investigated the performance characteristics of a typical communication network over a specific period in an established cellular communication network operator.

[9] focused on detecting irregular behavior using timing analysis of routing traffic within the network. In this research work, they showed how to identify intruders based on the protocol

irregularities that their presence creates once they begin to drop traffic. They identified the existence of the wormhole, before the intruders began the packet-dropping phase of the attack, by applying signal-processing techniques to the arrival times of the routing management traffic. This is done by relying on a property of proactive routing protocols that the stations must exchange management information on a specified, periodic basis. For the simulation, a MANET test bed was set up and they programmed an active wormhole and the results showed that an intruder was actively dropping systems and this was shown when they monitored the HELLO message intervals. This approach can be used in MANETs that use a proactive protocol that relies on regular protocol messages.

[8] described an end-to-end mechanism that can detect wormholes on a multi-hop route. This mechanism used geographic information to detect irregularity in neighbour relations and node movements. They presented a scheme, Cell-based Open Tunnel Avoidance (COTA), to manage the information. Wormhole attacks can be divided into three groups: closed, half open, and open and their mechanism is detected all the groups of wormholes. Simulations and experiments on real devices showed that the proposed mechanism can be combined with existent routing protocols to defend against wormhole attacks.

In a research paper [10] a novel trust-based schemes for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic mean. Their main goal was to design a protocol that not only prevents wormhole attacks but also avoids using strict clock synchronization.

They implemented the random way point movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity chosen between 0 m/s and the maximum simulation speed. Performance of the proposed scheme is evaluated based on the metrics such as Throughput, Packet Loss By malicious node.

By using Trust Based Model, Packet Dropping was reduced by 15% without using any cryptography mechanism and throughput is increased up to 7-8%. This was because the trust level of any node was not capable of sustaining the required traffic flow. In the case of detection of a wormhole by an intermediate node, all packets leading towards the tunnel are dropped and a corresponding route error packet is generated. At higher speeds the number of interactions with the nodes creating the wormhole increase considerably. This helps to spread trust information in the network at a higher rate. According to their results, up to 60% of the nodes executing the trust based DSR protocol were able to correctly identify at least one end of the wormhole.

[3] in their paper analyzed the effects of wormhole attack in ad hoc wireless networks by using a simple wormhole algorithm called hybrid routing algorithm which combines three different techniques; Hop Count Based Detection (Alternate Route), Anomaly Based Detection (Route Reply Decision Packet), Neighbour List Based Detection. Their paper focused on combining three techniques based on hop count, decision anomaly, and neighbor list count methods to detect and isolate wormhole attacks in ad hoc networks. They implemented an Ad hoc On-demand Distance Vector (AODV) protocol that simulates the behaviour of wormhole attack in Network Simulator 2. The simulation was performed in terms of average end-to-end delay, routing overhead, packet delivery ratio. This algorithm has better performance than the techniques being used individually (Hop count, Anomaly based, Neighbor list methods) to detect and isolate wormhole attacks in ad hoc networks. The solution detects the malicious

nodes and isolates it from the active data forwarding.

In [14] the objective was to find out the malicious node that performs the wormhole attack in network. They have assumed that the MANET consists of group of nodes. They proposed an algorithm in which intrusion detection is done in a group-based manner to detect the wormhole attacks. The group-based approach was used to reduce the load of processing on each group heads and also reduce the risk of a group head being compromised. The entire network into divided in groups. The group may be overlapped or disjoint. Each group has its own group head and a number of nodes designated as member nodes. Member nodes pass on the information only to the group head. The group head is responsible for passing on the information to all its members. The group head is elected dynamically and maintains the routing information. In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security threats including the wormhole attack.

[11] implement a system that successfully detects the wormhole present in the MANET using network and physical layer parameters. The various network parameters such as throughput, average end-to-end delay, packets dequeued are used to detect the presence of wormhole in the network. In addition, the physical layer parameters such as signals transmitted and signals received and forwarded to MAC layer are considered in the detection process. Various MANETs are simulated using the Qualnet 5.0 network simulator. The system carries out a cross layer detection of wormhole which is done using the Fuzzy Inference System (FIS).

The study in [6] resulted to a number of routing protocols which can be classified as non-Location based routing protocols and Location-based routing protocols. Non-Location based routing protocol uses the traditional routing concept such as maintaining a routing table while the Location- based routing protocol uses the geographical location of the mobile nodes to route the packets from source to destination. In their paper, they performed and analyzed the wormhole attack at location-based protocol ALERT (Anonymous Location Based Efficient Routing Protocol). In location-based routing protocols, the nodes use the information about the geographical position of other nodes to route packets to their destinations. When sending a packet to a destination, the source node gets the position of the destination node by the location service and adds this information in the header of the packet. Then, each intermediate node that receives the packet gets the location information of the destination from the packet and uses it to forward the packet comparing with its own location.

One of the efficient location-based routing protocol is the ALERT protocol which provides protection to source, destination and routes. It assumes the where the nodes in a network are randomly spread. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder). In the ALERT routing, each source node executes the hierarchical zone partition. It checks whether itself and destination are in the same zone. If so, it divides the zone in the horizontal and vertical directions. The node repeats this process until itself and destination nodes are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF). The Network Simulator tool (NS-2) was used to evaluate the performance of different location based routing protocols in mobile ad-hoc networks. The wormhole attack was implemented on varying number of nodes in network and consequently isolated the wormhole attack using isolator to know the effectiveness of routing protocols. They compared the ALERT protocol and Stateless Routing (GPSR) protocol with wormhole attack

based on the performance of routing protocols which was analyzed by; throughput, end-to-end delay, packet delivery ratio (PDR) and normalized routing load (NRL). Throughput; Throughput is the average rate of successful packet delivery over a network in per unit time. From the results, the throughput was decreased in the presence of wormhole attack for ALERT because wormhole receives packet from one location and tunnels it to another network.

In [7], the paper analyzed the nature of black hole attack and wormhole attack in Mobile Ad hoc Networks (MANETs). They proposed a mechanism called Advanced Optimized Link State Routing (AOLSR) protocol in order to analyse the attacks and this AOLSR is an improvement of the OLSR routing protocol, which will be able to detect the presence of malicious nodes in the network. In the solution, the AOLSR protocol senses the nodes in the network by broadcasting the behavior of the nodes. It monitors the number of broadcasts, inactive time period of nodes, data handover and log. If any suspicious activity is done by the malicious nodes during the transmission of data, those malicious nodes will be detected and an alert will be sent to source and destination. In the simulation, 35% of malicious nodes out of the normal nodes was used to launch the attack. The traffic load is simulated using 15 user datagram protocol-case based reasoning (UDP-CBR) connections generating traffic of 5 kb UDP packets (data payload 512 Bytes) with an inter departure time of 1s. Their experimental results showed that the proposed protocol achieved routing security with 22% increase in packet delivery ratio, 27% reduction in packet loss rate, 42% increase in throughput and 69% reduction in packet end to end delay than standard OLSR.

[12] proposed a fuzzy logic-based protection of wormhole and blackhole attack in mobile ad-hoc networks. The proposed method defines a set of rules to avoid wormhole and the blackhole attacks during communication. In this system, Sugeno model is employed and configured with three input linguistic variables namely; request forwarding probability (P1), reply forwarding probability (P2) and data dropping probability (P3) that characterize the quality of next hop neighborhood. After computing the probability of the nodes, the fuzzy process is invoked to detect the malicious nodes in the network. The performance of the proposed protocol was calculated by comparing it with a blackhole and wormhole of Secured Manet Transmission for Wormhole and Blackhole Attacks (SMTWB) using fuzzy inference system. The Efficiency of the proposed SMTWB protocol using FIS is analyzed on the basis of three performance metrics; throughput, packet delivery ratio and end-to-end delay, in the presence of different percentage of wormhole and blackhole nodes (1%, 2%, 3%, 4%, and 5%) in a network of 100 nodes.

[2] detected the existence of wormhole attack in MANET using Fuzzy Inference System. To detect the wormhole nodes in the system, they used measured parameters such as No. of dropped packets, Reply packets, Forwarded packets to collect the data for analysis. The wormhole nodes were identified by using soft computing algorithms such as Fuzzy Inference System (FIS) based on the above parameters.

In [18], A Machine Learning Framework for Length of Stay Prediction in Emergency Healthcare Services Department

3. Research Method

3.1 Architecture of the Proposed System

The architecture of the proposed analysis of wormhole attacks on MANET for potential optimization is shown in Figure 3.1.

Fig. 3.1: Architecture of the proposed system

4. Findings and Discussions

This research work adopted the fuzzy logic model which has three basic elements: fuzzifier, inference engine and defuzzifier. Fuzzifier: The fuzzifier maps crisp input data into values in the fuzzy logic space. This is done by using membership functions. Mathematically, a membership function associates each element $\mu_X(x)$ in the universe of discourse U with a number in the interval $[0, 1]$, as shown in equation (1)

$$\mu_A: X \rightarrow [0, 1] \quad (1)$$

Inference Engine: The number of rules depends on both the number of inputs and membership functions associated to each input. The general form of the l th fuzzy rule in the rule base is:

$$R^l: \text{if } (x_1 \text{ is } f_1^l) \text{ and } (x_2 \text{ is } f_2^l) \text{ and } \dots (x_n \text{ is } f_n^l) \text{ then } (y_1 \text{ is } P^l) \quad (2)$$

Defuzzifier: When the input data have been numerically processed by fuzzy reasoning, they are converted back to crisp values. There are several methods for doing so, and this research work used the algorithm called Centre of gravity, which computes in the simplest case the weighted average over all rule outputs.

$$COG = \frac{\sum \mu_A(x) \cdot x}{\sum \mu_A(x)}$$

Where $\mu_A(x)$ is the degree of membership of x in a set A .

4.1 Fuzzy Linguistic Variables

Linguistic Variables are non – numeric values which are used to facilitate the expression of rules and facts in Fuzzy Logic. The universe of discourse is shown in table 4.1.

Table 4.1: Fuzzy Linguistic Variables

VARIABLES		MEMBERSHIP FUNCTIONS	UNIVERSE OF DISCOURSE
Packet Delivery Ratio		Low (L)	0.0 - 0.25
		Medium (M)	0.25 - 0.55
		High (H)	0.55 - 1.0

Packet Forwarding Probability	Low (L)	0.0 - 0.25
	Medium (M)	0.25 - 0.55
	High (H)	0.55 - 1.0
Packet Dropping Probability	Low (L)	0.0 - 0.25
	Medium (M)	0.25 - 0.55
	High (H)	0.55 - 1.0
Wormhole Attack Level (Output)	Low (L)	0.0 - 0.25
	Medium (M)	0.25 - 0.55
	High (H)	0.55-1.0

4.2 Rule Base

Rules describe the relationships between input and output linguistic variables in words. A rule base is the set of rules for a fuzzy system. These rules have two parts, the rule antecedent (IF part) and the rule consequent (THEN part). The system rule base is shown in Table 4.2.

Table 4.2: The System Rule Base

S/NO	PDR	PFP	PDP	WORMHOLE ATTACK LEVEL
1	Low	Low	Low	Low
2	Low	Low	Medium	Medium
3	Low	Low	High	High
4	Low	Medium	Low	Low
5	Low	Medium	Medium	Low
6	Low	Medium	High	Medium
7	Low	High	Low	Low
8	Low	High	Medium	Low
9	Low	High	High	Medium
10	Medium	Low	Low	Low
11	Medium	Low	Medium	Medium
12	Medium	Low	High	High
13	Medium	Medium	Low	Medium
14	Medium	Medium	Medium	Medium
15	Medium	Medium	High	High
16	Medium	High	Low	Low
17	Medium	High	Medium	Medium
18	Medium	High	High	High
19	High	Low	Low	Low
20	High	Low	Medium	Low
21	High	Low	High	Medium
22	High	Medium	Low	Low
23	High	Medium	Medium	Medium
24	High	Medium	High	High
25	High	High	Low	Medium
26	High	High	Medium	High
27	High	High	High	High

4.3 Membership Function Plots

The type of membership function employed for this work is the triangular membership function. Triangular membership function is defined by three parameters: left, center and right. A triangular membership function is defined as follows;

$$f(x; a, b, c) = \begin{cases} 0, & x \leq a \\ \frac{x-a}{b-a}, & a \leq x \leq b \\ \frac{c-x}{c-b}, & b \leq x \leq c \\ 0, & c \leq x \end{cases}$$

4.3.1 Membership Function for Packet Delivery Ratio

$$\mu_l(x; 0, 0.125, 0.25) = \begin{cases} 0, & x \leq 0 \\ \frac{x-0}{0.125-0}, & 0 \leq x \leq 0.125 \\ \frac{0.25-x}{0.25-0.125}, & 0.125 \leq x \leq 0.25 \\ 0, & 0.25 \leq x \end{cases}$$

$$\mu_m(x; 0.25, 0.4, 0.55) = \begin{cases} 0, & x \leq 0.25 \\ \frac{x-0.25}{0.4-0.25}, & 0.25 \leq x \leq 0.4 \\ \frac{0.55-x}{0.55-0.4}, & 0.4 \leq x \leq 0.55 \\ 0, & 0.55 \leq x \end{cases}$$

$$\mu_h(x; 0.55, 0.775, 1) = \begin{cases} 0, & x \leq 0.55 \\ \frac{x-0.55}{0.775-0.55}, & 0.55 \leq x \leq 0.775 \\ \frac{1-x}{1-0.775}, & 0.775 \leq x \leq 1 \\ 0, & 1 \leq x \end{cases}$$

4.3.2 Membership Function for Packet Forwarding Probability

$$\mu_l(x; 0, 0.125, 0.25) = \begin{cases} 0, & x \leq 0 \\ \frac{x - 0}{0.125 - 0}, & 0 \leq x \leq 0.125 \\ \frac{0.25 - x}{0.25 - 0.125}, & 0.125 \leq x \leq 0.25 \\ 0, & 0.25 \leq x \end{cases}$$

$$\mu_m(x; 0.25, 0.4, 0.55) = \begin{cases} 0, & x \leq 0.25 \\ \frac{x - 0.25}{0.4 - 0.25}, & 0.25 \leq x \leq 0.4 \\ \frac{0.55 - x}{0.55 - 0.4}, & 0.4 \leq x \leq 0.55 \\ 0, & 0.55 \leq x \end{cases}$$

$$\mu_h(x; 0.55, 0.775, 1) = \begin{cases} 0, & x \leq 0.55 \\ \frac{x - 0.55}{0.775 - 0.55}, & 0.55 \leq x \leq 0.775 \\ \frac{1 - x}{1 - 0.775}, & 0.775 \leq x \leq 1 \\ 0, & 1 \leq x \end{cases}$$

4.3.3 Membership Function for Packet Dropping Probability

$$\mu_l(x; 0, 0.125, 0.25) = \begin{cases} 0, & x \leq 0 \\ \frac{x - 0}{0.125 - 0}, & 0 \leq x \leq 0.125 \\ \frac{0.25 - x}{0.25 - 0.125}, & 0.125 \leq x \leq 0.25 \\ 0, & 0.25 \leq x \end{cases}$$

$$\mu_m(x; 0.25, 0.4, 0.55) = \begin{cases} 0, & x \leq 0 \\ \frac{x - 0.25}{0.4 - 0.25}, & 0.25 \leq x \leq 0.4 \\ \frac{0.55 - x}{0.55 - 0.4}, & 0.4 \leq x \leq 0.55 \\ 0, & 0.55 \leq x \end{cases}$$

$$\mu_h(x; 0.55, 0.775, 1) = \begin{cases} 0, & x \leq 0 \\ \frac{x - 0.55}{0.775 - 0.55}, & 0.55 \leq x \leq 0.775 \\ \frac{1 - x}{1 - 0.775}, & 0.775 \leq x \leq 1 \\ 0, & 1 \leq x \end{cases}$$

4.3.4 Membership Function for Wormhole Attack level (Output)

$$\mu_l(x; 0, 0.125, 0.25) = \begin{cases} 0, & x \leq 0 \\ \frac{x - 0}{0.125 - 0}, & 0 \leq x \leq 0.125 \\ \frac{0.25 - x}{0.25 - 0.125}, & 0.125 \leq x \leq 0.25 \\ 0, & 0.25 \leq x \end{cases}$$

$$\mu_m(x; 0.25, 0.4, 0.55) = \begin{cases} 0, & x \leq 0 \\ \frac{x - 0.25}{0.4 - 0.25}, & 0.25 \leq x \leq 0.4 \\ \frac{0.55 - x}{0.55 - 0.4}, & 0.4 \leq x \leq 0.55 \\ 0, & 0.55 \leq x \end{cases}$$

$$\mu_h(x; 0.55, 0.775, 1) = \begin{cases} 0, & x \leq 0 \\ \frac{x - 0.55}{0.775 - 0.55}, & 0.55 \leq x \leq 0.775 \\ \frac{1 - x}{1 - 0.775}, & 0.775 \leq x \leq 1 \\ 0, & 1 \leq x \end{cases}$$

The graphical representation of the membership functions employed in this work are plotted and generated using MATLAB programming tool. The various plots are shown in Figure 4.1a - 4.1d.

Fig 4.1a: Membership Function for 'Packet Delivery Ratio'

Fig 4.1b: Membership Function for 'Packet Forwarding Probability'

Fig 4.1c: Membership Function for 'Packet Dropping Probability'.

Fig 4.1d: Membership Function for the ‘Wormhole Attack’ variable

5. Simulation Parameters

The proposed system uses Fuzzy Inference System (FIS) for ***End-2-End Behavioural Analysis of Wormhole Attack***. The system detects the existence of wormhole nodes which determines the rate of packet delivery, packet forwarding probability and packet dropping probability based on the simulation of the network. 10 nodes and 15 nodes were simulated respectively. However, 2 nodes acted as the wormhole nodes which generated output results as shown in Table 4.3.

Table 4.3 Simulation Results

Number of mobile nodes	Number of sent Packets	Number of Received Packets	Number of Forwarded Packets	Number of dropped Packets
10	10780	241	2759	10475
15	10780	1698	8826	8802

5.1 Simulation Analysis

The proposed system uses Fuzzy Inference System (FIS) for ***End-2-End Behavioural Analysis of Wormhole Attack***. The system detects the existence of wormhole nodes which determines the rate of packet delivery, packet forwarding probability and packet dropping probability based on the simulation of the network. 10 nodes and 15 nodes were simulated respectively. However, 2 nodes acted as the wormhole nodes which generated output results as shown in Table 4.3.

Table 4.3 Simulation Results

Number of mobile nodes	Number of sent Packets	Number of Received Packets	Number of Forwarded Packets	Number of dropped Packets
10	10780	241	2759	10475
15	10780	1698	8826	8802

5.2 Evaluation and Discussion of Result

Figure 4.4a shows the Graph of Number of Packets Sent during the simulation.

Fig. 4.4a: Graph of Number of Packets Sent

Figure 4.4b shows the Graph of Number of Packets Forwarded during the simulation.

Fig. 4.4b: Graph of Number of Packets Forwarded

Figure 4.4c shows the Graph of Number of Packets Received during the simulation.

Fig. 4.4c: Graph of Number of Packets Received

Figure 4.4d shows the Graph of Number of Packets Dropped during the simulation.

Fig. 4.4d: Graph of Number of Packets Dropped

Figure 4.5 shows the Graph of Number of Packets Sent, Received, Forwarded and Dropped during the simulation.

Fig. 4.5: Graph showing the detailed Analysis

The simulation was carried out in NS-2, a total of 10780 packets were sent in the network. The graph represents the Packet analysis in a typical wormhole attack situation using the simulation of 15 nodes with two wormhole attacker nodes. It was observed that during the simulation, the number of packets dropped was more than the number of packets received. This is as a result of the wormhole attack, the attack forwards packets sent from the source and this makes the Time-To-Live (TTL) of a packet to elapse thereby causing a drop in the packet.

These results were fed into the fuzzy inference system based on three parameters; Packet Delivery Ratio, Packet Forwarding Probability and Packet Dropping Probability and the parameters can be calculated thus;

$$\text{Packet Delivery Ratio} = \frac{\text{Number of packets received}}{\text{Number of packets sent}}$$

$$\text{Packet Forwarding Probability} = \frac{\text{Number of packets forwarded}}{\text{Number of packets sent}}$$

$$\text{Packet Dropping Probability} = \frac{\text{Number of packets dropped}}{\text{Number of packets sent}}$$

Table 4.5: Parameters and Values Used for Analysis

Number of mobile nodes	Packet Delivery Ratio	Packet Dropping Probability	Packet Forwarding Probability	Fuzzy Analysis
10	0.0224	0.9717	0.2559	29.17% Low
15	0.1575	0.8165	0.8187	44.99% Low

Fuzzy Inference System Editor:

Rule Viewer:

Surface Viewer:

6. Conclusion

In this research paper, various types of wormhole detection algorithms in MANET were investigated. The work focused on detecting anomalous behaviour using Fuzzy Logic model. Particularly, security has become a primary concern in order to provide defense services in various communication networks; wireless as well as wired environments. Hence, the goal of

this research is to optimize networks security apparatus in order to guard against the routing paths of different packets thereby securing the packets from malicious attacks. This is accomplished by determining the *Packet Delivery Ratio (PDR)*, *Packet Forwarding Probability (PFP)* and *Packet Dropping Probability (PDP)*. Considering these network parameters, the system was capable of detecting the degree of severity of wormhole attack on MANET. This work is a genuine attempt to enhance the Quotient of Packet Delivery while minimizing the rate of Packet Drop for efficient Network QoS Provisioning.

References

- [1] Aakanksha Kadam, Niravkumar Patel and Vaishali Gaikwad (2016). Detection and Prevention of Wormhole attack in MANET. International Research Journal of Engineering and Technology (IRJET) Volume: 03, Issue: 03, Page 388 – 393, (Mumbai, Maharashtra), India.
- [2] Abhijit Ghanshyam Raut and D. Vydeki (2017). Design and Analysis of Fuzzy Based Wormhole Detection in MANET. International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE), Vol. 4, Issue 5, (Chennai), India.
- [3] A. Vani and D. Sreenivasa Rao (2011). A Simple Algorithm for Detection and removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks, International Journal on Computer Science and Engineering (IJCSE), Vol. 3, No. 6, Page 2377- 2383, (Hyderabad, Andhra Pradesh), India.
- [4] Aditya Bakshi, A.K. Sharma and Atul Mishra (2013). Significance of Mobile Ad hoc Networks (MANETS), International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 2, Issue-4, Page 1-3.
- [5] Ankita Khanna, P. U. Dere (2016). Intrusion Detection of Wormhole Attack and Managing Security using DSR protocol in MANET, Proceedings of 59th IRF International Conference, (Pune), India.
- [6] Devendra Kumar and Deepak Kumar Xaxa (2014). Analysis of Effectiveness of ALERT Protocol against Wormhole Attack in MANETs, International Journal of Engineering Sciences & Research Technology (IJESRT) page 353-359.
- [7] K. Sivagurunathan, K. Manojkumar, D. Sounder and Midhun Sebastian (2015). Performance Evaluation of Advanced OLSR against Black Hole Attack and Wormhole Attack in MANET, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, page 2025 - 2034, (Puducherry), India.
- [8] L. Lazos, R. Poovendran, C. Meadows, P. Syverson and L. W. Chang (2005). Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. IEEE Communication Society, WCNC, (Seattle), Washington, DC.
- [9] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont and Ramiro Liscano (2006). Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis, In IEEE Military Communications Conference, Page 1-7.
- [10] P. Narendra Reddy, CH. Vishnuvardhan and V. Ramesh (2013). Routing Attacks in Mobile Ad Hoc Networks. International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 2, Issue 5, Page 360 – 367, India.

- [11] P. Revathi, M. M. Sahana & Vydeki Dharmar (2013). Cross Layer Detection of Wormhole in MANET Using FIS. ITSI Transactions on Electrical and Electronics Engineering (ITSI-TEEE), Volume -1, Issue 3, Chennai, India.
- [12] P. S. Hiremath, Anuradha and Prakash Pattan (2016). SMTWB - Secured MANET Transmission for Wormhole and Blackhole Attacks using Fuzzy Logic. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), Volume 23, Page 236 – 241, India.
- [13] Reza Fotohi and Shahram Jamali (2014). A Comprehensive Study on Defense against Wormhole Attack Methods in Mobile Ad hoc Networks, International journal of Computer Science & Network Solutions, Volume 2, No. 5, page 37 - 56 (Germi) Iran.
- [14] Sandeep Saxena, Nagendra Kumar and Shubham Omar (2013). Detecting wormhole attacks on wireless ad – hoc networks: A group based approach, International Journal of Computer Applications (0975 – 8887) Volume 69– No. 28, page 8 – 13, Noida.
- [15] Shalini Jain and Satbir Jain (2010). Detection And Prevention Of Wormhole Attack in Mobile Ad Hoc Networks, International Journal of Computer Theory and Engineering, Vol. 2, No. 1, (New Delhi), India.
- [16] Simon Coupland and Robert John (2007). Geometric Type-1 and Type-2 Fuzzy Logic Systems IEEE Transactions on Fuzzy Systems, Vol. 15, No. 1, (Leicester), U.K.
- [17] Imeh J. Umoren, Prince Asagba and Olumide Owolabi (2014). Handover Manageability and Performance Modeling in CDMA Mobile Communication Networks, International Institute for Science, Technology and Education (IISTEE) and Computing Information Systems Development Informatics and Allied research -Journal (CISDA). Vol 5 No. 1, ISSN: 2167 -1710, page 27-42.
- [18] Imeh J. Umoren, Daniel E. Asuquo, Onukwugha Gilean, Mfon Esang (2019). Performability of Retransmission of Loss Packets in Wireless Sensor Networks. Comput. Inf. Sci. 12(2): 71-86, Canada.
- [19] Weichao Wang, Bharat Bhargava, Yi Lu and Xiaoxin Wu (2006). Defending against Wormhole Attacks in Mobile Ad Hoc Networks, Wiley Interscience, Wireless Communication and Mobile Computing, (W. Lafayette), Indiana.
- [20] ih-Chun Hu, Adrian Perrig and David B. Johnson (2003). Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, IEEE InfoCom. International Journal for Scientific Research & Development (IJSRD), Vol. 1, Issue 3

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>)