Fuzzy enhanced Intrusion Prevention System for Ad Hoc Networks

Mr. R. Rajavarman, Assistant Professor in K.Ramakrishnan College of Technology, India.
Dr. T. AvudaiappanAssistant Professor in K.Ramakrishnan College of Technology, India,
E-mail: rajavarmanrrr@gmail.com & avudaiappanmecse@gmail.com

Article Info
Volume 83
Page Number: 6023 - 6028
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 01 April 2020*

Abstract:

Mobile nodes in the MANET are randomly moving and it is easily compromised by the external attackers. Previous schemes were not able to find the intruders efficiently. In this research work, Fuzzy enhanced Intrusion Prevention System for detecting and isolating attackers in ad hoc network. It contains two phases. In first phase, broadcast routing is established from source to sink node. Fuzzy mechanism is established in the routing to obtain any malfunction present in the network. Fuzzy decision mechanism takes the crisp values as input variables such as trust threshold vector and packet arrival rate. In second phase, intrusion prevention system is established to isolate the attackers in the network. Based on the extensive simulation results, FIPS achieves more network performance in terms of intrusion detection ratio, throughput, delay and packet arrival rat.

Keywords: Fuzzy estimation, Intrusion prevention system, Fuzzy decision mechanism, multicast route discovery and packet arrival rate

I.INTRODUCTION

In recent years, Mobile ad hoc network are adaptable and meet the various types of applications. Initially MANETs are very effective and suitable for military applications. Based on optimal link transfer mechanism, MANET become vulnerable and safe less network. Intrusion Prevention Scheme plays a crucial role in ad hoc network environment to detect and isolate any attacks from the network. It is a software system where as many schemes introduced like signature based detection system, anomaly based detection system and character based detection system.

II. PREVIOUS WORK

Nigahat and Dinesh Kumar [1] reviewed various surveys on black hole attack in ad hoc network. The security threats and objectives were defined in a periodical manner. Different categories of black hole attacks were discussed in this work. In this paper, we have analyzed the security threats an ad-hoc network faces and presented the security objective that need to be achieved. Various types of algorithms, protocols and schemes were analyzed in this section to improve the detection ratio and to avoid the attackers in future communication.

Anish Kumar Khare et.al [2] proposed the fuzzy enhanced trust estimation method to detect wormhole, black hole attack and denial of service attack. On demand vector routing was applied to solve the problem of long path issue. The shortest paths were easily found to reduce the packet losses. The trust value of each node is applied as zero to update the neighbor node with forward threshold factor value. Every node in forwarding path and reverse path has the capability of identifying the attackers in nearby hop based on the sequence number identification.

David Samuel bhatti et.al [3] reviewed the protocols and mechanisms on wormhole detection. The graph theory algorithms were done for isolating the legitimate nodes. Synchronization mechanisms were deployed for the minimization of delay and jitter. Existing trust based mechanisms are not enough for implementation of path due to certain conditions. The better security approaches were not useful for fulfilling expected security requirements.

Zaid Abdulkader [4] introduced the misbehaving node identification and protection scheme in Vehicle Ad hoc Networks The genuine routes were found for packet transmission using this mechanism for better transmission. The best performance was produced by this mechanism in terms of delay, delivery ratio, packet loss and delay. The key management scheme was included with this protection scheme for the managing the key in the network,

Shiva Shamaei, and Ali Movaghar [5] proposed a two phase wormhole attack detection scheme based on selection of paths. Tunnel was used for confirming the wormhole existence and finding malicious node location. In this paper, a two-phase detection scheme is proposed to detect and prevent wormhole attacks. Allkind of attacks were found i.e. in band and out band nodes without the hidden terminal or exposed terminal problem.

Sandeep Singh and Rajinder Singh [6] introduced a new methodology to monitor the behavior of worm hole attack in MANET. A Novel technique was used for the analysis of attacks. Here the threshold vector was used to identify the attacks.

Chitvan Gupta et.al [7] proposed the network and transport layer issues in MANET. The network performance was degraded due to the presence of the attacks. The attacks are detected and removed from the network based on the security analysis. There are several ways to prevent worm hole detection. The existing attacks knowledge is determined based on intrusion activities in ad hoc network. Due to dynamic environment, attackers are found based on worm hole detection.

Luong Thai Ngoc and Vo Thanh Tu [8] introduced a new method for detecting routing attacks in MANET. Data packets are dropped due to the presence of worm hole attacks. Based on the simulation result analysis, the routing protocol outperforms well than existing schemes.

Neelima singh and Ramanjeet Singh [9] proposed the hop count reverse trip clock based link length to detect the wormhole tunnels in the network. Based on hop count, worm hole attacks were identified and isolated from the network. The link length was estimated during route discovery phase to detect the lifetime of the routes. Using path length, worm hole attacks were identified based on network length.

Anjali Soni et.al [10] proposed the worm hole attack detection based on reliable, security and scalable network. The main purposed of the study was to determine the detection of attacks. The number of nodes was varied based on worm hole attack in ad hoc networks. From the analysis of network simulation, detection of worm hole attack was done based on node variation.

III.PERFORMANCE OF FIPS

In this section, the concept of fuzzy decision mechanism is deployed to detect the worm hole attack based on crisp values. The packet dropping attack was measured based on the fuzzy output metric. The problem in the fuzzy scheme was not overcome by existing schemes. The exact output is done by deleting the various issues to implement the fuzzy logic technique. Three measures are calculated to find the dropping ratio of network.

First measure is higher dropping rate than threshold value. Second measure is packet dropping by the node which is near to the destination node and it is greater than threshold value. Third measure is packet dropping by the node which is near to the source node. Based on network characteristics and attacker behavior, the threshold value is set to identify the attackers.

Measures of the nodes are varied from M1, M2, ….. N. The misbehaving nodes or attackers are represented as, A1, A2, …. AN. The number of nodes participating in the dynamic topology is represented as L1, L2, …. Ln. Based on these values, the matrix is formed.

3.1 Estimation of Fuzzy

Fuzzy estimation is based on the matrix T1, T2, … TM. From the threshold values U and U1, the matrix values are estimated. Based on the node number and member function, the matrix value is defined. The trapezoidal membership model is used for determining the membership function. The membership function in the matrix is defined as follows.

Value of node membership = $(A-x)/(B-x)$

A denotes threshold value, B denotes the packet dropping rate. x indicates the packet forwarding rate.

• 3.2 Fuzzy enhanced Intrusion Prevention System

Fuzzy enhanced intrusion detection system sends the periodical message to all nodes in the cluster region within the set. Once all nodes received the hello message for confirming the route, it will send the reply packets.

During reception period, the genuine node replies with correct packet sequence number corresponding to the route request node. If any wormhole attack is present, only the wrong information will be replied to the source node. If any node is sending a status packet with high sequence number, it is considered as genuine packet. If any node sends the average number of sequence number and more packet dropping , it is considered as black hole attack. The misbehaving nodes drop more compared to genuine nodes and the information reachability is not possible at the receiver end.

Congestion occurs due to worm hole and black hole attack. Instead of forwarding packets next to neighbor node, packet dropping will be done by the malicious node. Each mobile node has the equal traffic and allocated to threshold trust vector table. If any node violates the traffic load or consumes more power for packet dropping, it is immediately identified by fuzzy based intrusion detection approach. The source node rejects the malicious attacks and it will be added to black list table. Immediately the source node block the message from attacker node to forward it to neighbor node.

The following block shows the prevention of attackers in the network. The range of attackers is categorized based on the fuzzy matrix and threshold valuation. Figure 1 shows the illustration of fuzzy based intrusion prevention mechanism.

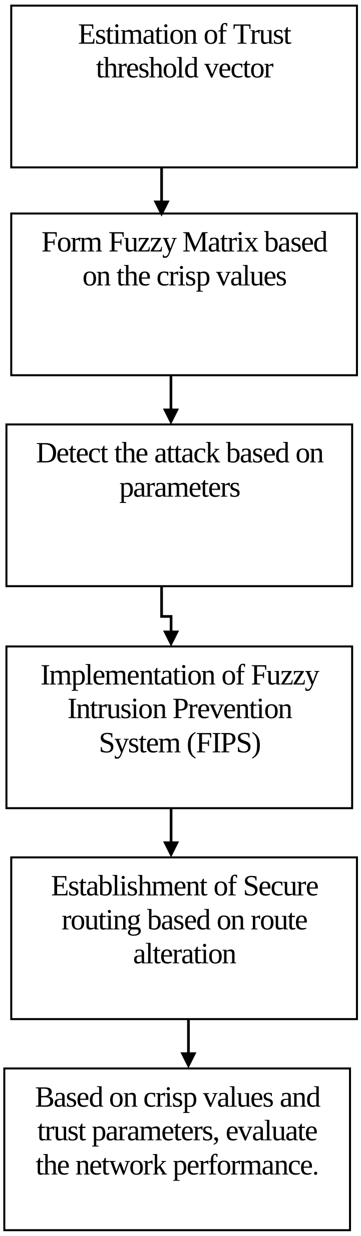
Estimation of Trust threshold vector
Form Fuzzy Matrix based on the crisp values
Detect the attack based on parameters
Implementation of Fuzzy Intrusion Prevention System (FIPS)
Establishment of Secure routing based on route alteration
Based on crisp values and trust parameters, evaluate the network performance.

Figure 1. Fuzzy enhanced Intrusion Prevention System

IV. SIMULATION RESULTS

The proposed FIPS is simulated using the network simulation tool (NS 2.35). The traffic used here is constant bit rate traffic. Dynamic source routing protocol (DSR) is used for the network overhead analysis.It provides overhead reduction and centralized route gathering in ad hoc environment. The number of nodes used here for simulation is 250 nodes. The packet rate used here is 4 packets/sec. The mobility model used here is random walk model.

Table 1.
Simulation and Setting Parameters of FIPS

No. of Nodes	250
Area Size	1200 X 1200 sq.m
Mac	802.11
Radio Range	250 meter
Simulation Time	100 sec
Traffic Source	Constant Bit Rate
Packet Size	128 bytes
Mobility Model	Random Walk
Protocol	Dynamic Source Routing

The following parameters are used to analyze the performance ofproposed intrusion prevention system.

Intrusion detection ratio: It is the ratio of detected intruders to the total number of nodes available in the network.

Queuing delay: It is delay occurred due to heavy traffic congestion.

Packet arrival rate: It is the rate at which number of packets arrived at the destination in the presence of dynamic network environment.

Throughput: It is the number of packets received per time.

Intrusion detection time: It is the time for detecting intruders in the present link during route maintenance.

Figure 2 shows the performance of FIPS over existing schemes in terms of intrusion detection ratio. The proposedscheme achieves high ratio than existing schemes.

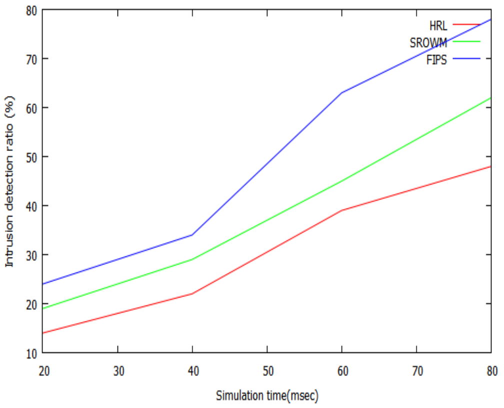

Figure 2. Intrusion detection ratio Vs Simulation time

Figure 3 shows the analysis of queuing delay while varying time in x axis. The performance of FIPS is varied based on simulation time. It achieves less queuing delay compared to existing
Scheme.

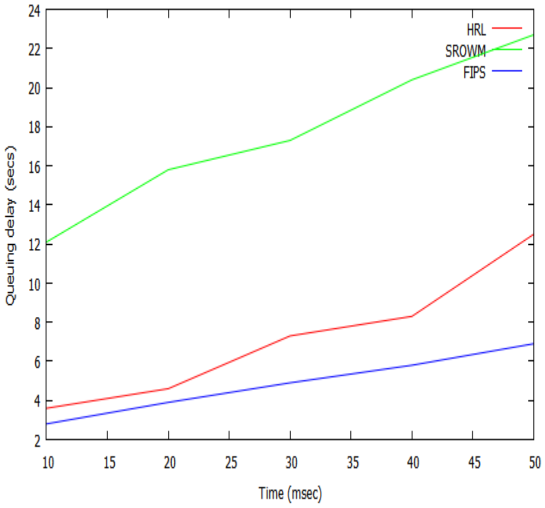

Figure 3. Queuing delay Vs Time

Figure 4 illustrates the performance of packet arrival rate while varying number of packets in x axis. From the results, FIPS achieves high packet arrival rate than existing schemes.

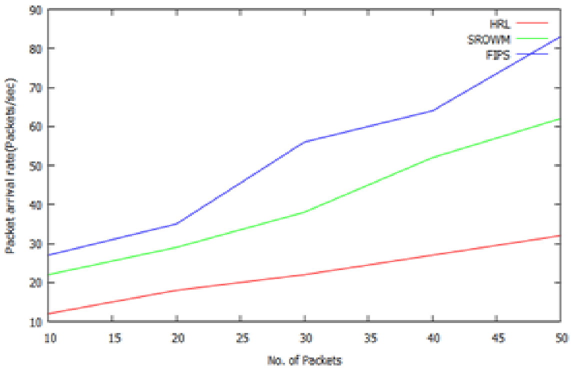

Figure 4. Throughput Vs No. of links

Figure 5 illustrates the performance of throughput while varying the number of links. The FIPS produces more throughput than existing schemes..

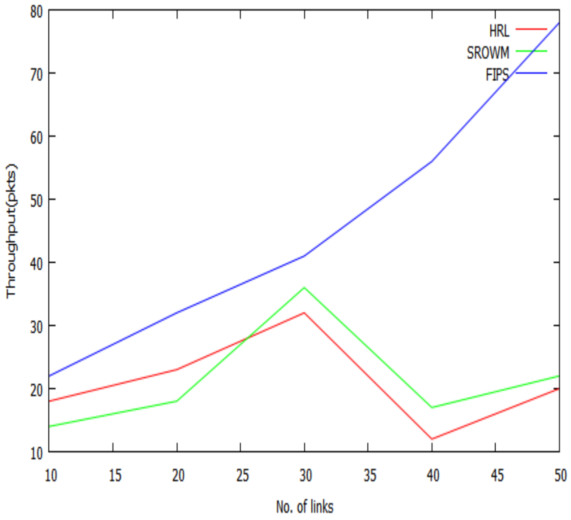

Figure 4. Packet arrival rate Vs No. of Packets

Figure 6 shows the results of intrusion time while varying speed in x axis. It is seen that detection time of FIPS is less compared to existing schemes.

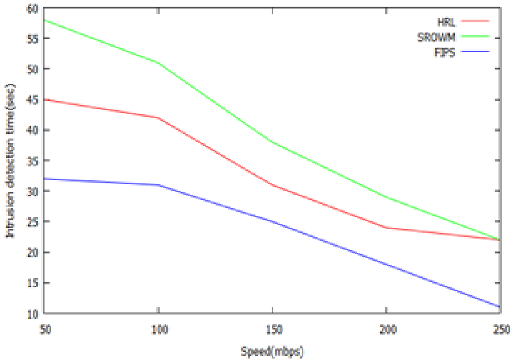

Figure 6. Intrusion detection time Vs Speed

V.CONCLUSION

Intrusion detection is a major concern while producing efficient network performance in ad hoc networks. Balancing intruders and links are very important in the network. In this research work, Fuzzy enhanced Intrusion Prevention System is proposed to achieve high detection ratio than existing schemes. Fuzzy membership functions are the key indicators for determining the attackers during dynamic network environment. In future, it is planned to add the cross layer based fuzzy intrusion detection system.

REFERENCES

[1] Nigahat and Dinesh Kumar, “A Review On Black Hole Attack In Mobile Ad-Hoc Networks (Manet) International Journal Of Engineering Sciences & Research Technology, Volume 6, Issue 3, 2017 , pp.556-561.

[2] Ashish Kumar Khare, Rana and Dr. R. C. Jain “Detection of Wormhole, Blackhole and DDOS Attack in MANET using Trust Estimation under Fuzzy Logic Methodology”, I. J. Computer Network and Information Security, Vol.7, Issue 1, 2017, pp.29-35.

[3] David Samuel Bhatti, Shehla Saeed, Muhammad Asad Ullah, Naila Samar Naaz, Syed Saqib Raza Rizvi, Syed Taha Ali, “SRoWM: Smart Review on Wormhole Mitigation”, IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.12, December 2017, pp. 178-187.

[4] Zaid Abdulkader, “Malicious Node Identification Routing and Protection Mechanism for VANET against

[5] Various Attacks”, Journal of Information Security Research, Volume 8, Number 4, 2017,pp.161-177.

[6] Shiva Shamaei, and Ali Movaghar “ATwo-PhaseWormholeAttack Detection Scheme in MANETs”. The ISC Int'l Journal of Information Security, Volume 6, Issue 2, 2014, pp.183-191.

[7] Sandeep Singh, Rajinder Singh, “Detection and Isolation of Selective Packet Drop Attack in MANET”, International Advanced Research

Journal in Science, Engineering and Technology, Vol.4, Issue 7, 2017, pp.94-99.

[8] Chitvan Gupta, Dr. Prashant Singh, Dr. Rajdev Tiwari, “Network and Transport Layer Attacks in Ad-hoc Network”, International Journal of Advanced Research in Computer and Communication Engineering, Volume 6, No.2, 2017, pp.38-42.

[9] Luong Thai Ngoc, Vo Thanh Tu, “Whirlwind: A New Method to Attack Routing Protocol in Mobile Ad Hoc Network”, International Journal of Network Security, Vol.19, No.5, PP.832-838.

[10] Neelima Singla and Ramanjeet Singh “Wormhole Attack Prevention and Detection in MANETs Using HRL Method”, International Journal of Advance Research, Ideas and Innovations in Technology, Volume-3, Issue-2, 2017, pp.196- 200.

[11] Anjali Soni, Shivendu Dubey, Jyoti Gupta, “Varying Number of Nodes Based Implementation of Wormhole Attack Based on Manet Using NS3”, IJSART, Volume 3, Issue 4, 2017, pp.152-155.