Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/130515

FSSAM: Detecting Wormhole Occurrence Using Five-Stage Security Analysis Model in MANET

S. Muthukumar[1,*] *and K. Ruba Soundar*[2]

[1] Department of Computer Science and Engineering, Sree Sowdambika College of Engineering, Aruppukottai, Tamilnadu, India.
[2] Department of Computer Science and Engineering, P.S.R. Engineering College, Sivakasi, Tamilnadu, India.

Received: 23 Jan. 2019 , Revised: 16 Apr. 2019, Accepted: 19 Apr. 2019
Published online: 1 Sep. 2019

Abstract: The mobile ad-hoc network is a wireless network in which the nodes communicate with each other through wireless channels. Security in this network is the crucial aspect to protect from the fraudulent actions. Due to the fraudulent actions the data is lost, the route gets a failure and data route diversion takes place. The data transmission in the network also gets failure and this work is aimed to model and implement a Five Stage Security Analysis Model (FSSAM) to detect the wormhole attacks in MANET. For that, the proposed model collects and analyzes the information about all the nodes, routing paths and other communication details in the network. Network Simulation-2 tool is used for simulating the proposed FSSAM and the performance is evaluated.

Keywords: Security, MANET, Malicious Activity, Wormhole Attack, Route Discovery, Route Failure.

1 Introduction

A large number of mobile nodes connected as a temporary network, not depending on any existing infrastructure is termed as MANET. All the nodes in the network behave as a host as well as a router. Hence it provides all the nodes to get connected within the network and to communicate with one another. But MANET gets struck due to lack of security issues such as open medium, lack of central monitoring and management, changing its topology dynamically and no cleared defense mechanism. The nodes inclusion and exclusion in the network without any constraints at any time is described in [1]. One of the security issues is the wormhole attack and it disturbs the entire communication in the network [2]. The wormhole attack is represented in Fig. 1, in which A, B, C and G are some of the nodes taken in the network to describe the wormhole attack [3]. The nodes A and B are treated as a normal node and C and G are treated as malevolent nodes in the network. Because C and G communicate in private route which does not belong to the common route in the network. B chooses the first route because it is the shortest and fastest route, thus the transmission between the nodes depends upon the relay node and a large number of routing protocols is currently proposed. The wormhole attackers aggregate all the data packets and transmit them in a normal route.

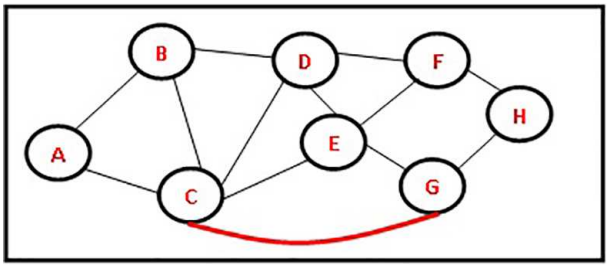

Fig. 1: Scenario of wormhole attack

In Fig. 1, S, D, M1 and M2 are the source, destination, malicious-node-1 and malicious node-2 respectively.

Therefore the resulting route has a less number of hops in the usual routes. Thus, those attackers who use the wormhole could easily calculate the prioritized route in MANET in order to perform packet modification and eavesdropping [3]. A wormhole link is created by connecting a high-speed channel link with the data route in the network is explained in [4]. The wormhole attack consists of two different modes, called ”Exposed” and

* Corresponding author e-mail: muthukumarphd@mail.com

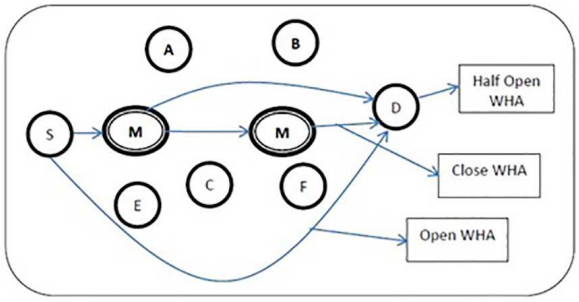

Fig. 2: Open, half-open and closed wormhole scenarios

'Hidden" modes. The two different modes can be identified by the packet header [2].

Wormhole attacks: the three different forms of wormhole attacks are:
- –Open
- –Half Open
- –Closed

Open wormhole: Between the source (S) and Destination (D) nodes, malicious nodes (M1, M2) are available in the network. The node on the traversal path A and B are hidden and these nodes are involved with attackers automatically in the header by subsequent route finding method. The nodes are fraudulent-aware nodes in the data route of the network and thus it limits the fraudulent nodes stating that they are direct neighbors.

Half-open wormhole: In the given scenario, consider two different malicious nodes such as visible and hidden. One node closer to the source is visible and the other malicious node closer to the destination is hidden. The attacker doesn't modify the data packet. Finally, they club the end of the wormhole and then re-broadcast the packets.

Closed wormhole: All the intermediate node's identities are kept as hidden from S to D. Fake neighbors are created, since the S and D hop just one-half for away from each other shown in Fig. 2.

2 Research Background

Indirect communication is created using a multi-hop connection by all the nodes helping one another as neighborhood nodes. Differentiating the neighbor nodes from the entire nodes help to find out and communicate with the non-neighbors. The routing protocols play a vital role in the network. Wormhole influences several routing protocols that include DSR, OLSR, AODV, TBRPF and DSDV etc. [5–7]. In order to detect and prevent the wormholes, the theory of temporal packet is applied in [7]. With the help of topographical information, the receiver node is available within a predefined space from the sender node. The directional antennas [8] are also used in the prevention of wormhole attacks. Every node distributes their secret key with another node in the network and it also keeps a list of its updated neighbors. LITEWORP [7]—a light weighted counter measure–is used in the wormhole attack. Local monitoring is carried out, where the node tracks the traffic cost based on the distance among their neighboring nodes. Also, it uses their data structure of the first two neighbors. LITEWORP eliminates fraudulent nodes. To identify the wormhole attack, TTM attacks are created [9]. At the time of route setup procedure, TTM identifies the wormhole attacks by stating the transmission time of every two consecutive nodes on its recognized paths. In order to detect the wormhole attacks, two new mechanisms such as RTT-TC and topological comparisons are also incurred [10].

For preventing the network from wormhole attacks in WSN, a protocol is designed by using cryptographic mechanisms and also on the basis of GPS. The nodes get distinguished among themselves as GPS nodes and non-GPS nodes [11]. An efficient algorithm is developed in the proposed approach, rather than TTM. Packet Travel Time (PTT)-a new state is provided in this algorithm [12], where this state permits each device to monitor its neighbor behavior. In order to provide security against wormhole attacks, a method is newly adopted with the help of honeypot [13]. The determination of honeypot is to find out the actions of intruders, who try to have unauthorized access over the network and to improve the network security.

3 Existing System

3.1 Earlier IDS' Limitations

As the IDS technique is applied in MANET, certain problem is obtained because of its specific nature. Some factors that affect network performance are:

3.1.1 Congestion

Certain IDS tries to locate fraudulent nodes, in order to send special packets to all or any other node involved in the route. The network topology frequently gets changed in MANET. As the nodes move freely, many messages are poured into the network, which creates congestion. This produces a negative issue on the network. Thus the congestion also increases FPR of the IDS, where wormhole attacks are detected by time calculations.

3.1.2 Routing Delay

The consumed time for routing a data is used to calculate the delay which is obtained from route discovery and also

verify the routes before the actual data is sent. If the path is established, then the IDS takes a minimum amount of time, to evaluate the path between S and D nodes. Hence, it causes a delay in routing, which directly affects network performance.

3.1.3 Resource Overuse

It means that the additional use of resources used by a node for any activity rather than transmitting the data and finding its route. The mobile node also contains limited resources in the form of processing power, storage memory and life of a battery. Memory usage is larger when IDS gets involved.

3.1.4 Special Hardware

More utility of hardware is required rather than the hardware, which is generally required for the data transfer and routing. Hence this special hardware could be in various forms such as special devices like directional antennas, GPS devices and special nodes with additional features. Network cost is reduced by resource re-usability.

3.1.5 Node Mobility

This is said to be the most important of the property of MANET, which means that each node in the network can move anywhere in the network. The IDS blocks the fraudulent nodes by transferring the block or trust information. Because of mobility, False Positive Rate (FPR) could be increased.

Wormhole attack detection methodology, where the transmission depends on the range of the neighborhood without using extra tools was proposed in [14]. The simulation results denote that the proposed system could detect the wormhole attack efficiently in WSN. In this work, a well-known algorithm of Transmission Range-based Method (TRM) is used. Due to the presence of wormhole, a new topology is demolished and the roots are misled. Specialized hardware is not used anywhere, even though a large amount of data gets transmitted, this algorithm prevents wormholes by permitting the neighborhood function to detect whether the network topology is an original or fake one. An analytical evaluation is provided for this algorithm in order to correct the simulation experiment which states its efficiency.

The wormhole attack in the existing system is denoted only by investigating and verifying the communication route. Wormhole attack is created by very few fraudulent nodes, where they act like a normal node and hence transfer the data in their private route. Thus this paper is permitted to detect the methodology of Worm Hole Attack (WHA), by analyzing the entire network in terms of location, neighborhood, route and time of communication within the network.

4 Proposed System

Various stages for WHA detection of the proposed approach is discussed below.

4.1 Route Analysis

The protocol AOMDV-is utilized to discover the various routing path from the source node to the destination node in each route. This protocol is an annex of AODV protocol. In this, the protocol is checked with the route table, either the route is available or not for transferring the data between nodes. An RREQ packet is broadcasted in all the available routes and investigates the nodes including destination node. If the destination receives the RREQ, then it immediately sends back an RREP packet in the same path. Even though a various number of RREQ packets comes from different data paths, they are all aggregated and transmitted in a single path to the source node. All the available routing paths that are known by the source node are updated in the routing table. In this manner, the paths are obtained [2]. The perspective view of AOMDV is at the time of route discovery procedure, it provides multiple paths to avoid link failure. AOMDV creates various paths and it will choose the key path for the transferring of data. Using AOMDV protocol this paper detects the wormhole attack. The entire information of the proposed model is explained below.

Source node S establishes RREQ packet with sending time t1, it sends the respective RREP packet to S and further also receives the time of a packet. In case many RREP packets are received then it must keep track of the related time t2_*i* of every RREP packet. By using these values we estimate the round trip time t3_*i* of the broadcast route [8]. The round trip time of every route t3_*i* is divided by each of its hop counts. The average of round trim time of all routes is calculated by the value ts_*i*. The value occurred in threshold is round trip time th. Once the threshold value is compared with each round trip time th_*i*, in such a case, if total round trip time ts_*i* is less than the threshold round trip time th_*i* (ts_*i* $<$ th_*i*) and the hop count of the particular *i*th route is equivalent to 2 then the closest/first neighbor node is considered as wormhole node. Fig. 3 shows that the neighbor node M1 is wormhole node and sends a dummy RREP message to M2 and the time difference is calculated. Considering M1 as the wormhole node, M2 replies to M2, hence M2 is also detected as wormhole node. Now both M1 and M2 are eliminated and the data is transmitted through another routing path. The usage of AOMD protocol in this proposed mechanism is that it minimizes the outlay and delay.

4.2 Node Location Analysis

Location of the particular node acts as a crucial role in wormhole attack. When the current location of the mobile

node is known, then it is used to build a track on the network. Certain special nodes contain a GPS receiver at a specific location to get the location of neighboring nodes. With the help of special antennas, the relative location is collected. This GPS device decreases the battery time of the node. The relative location is used as the detection failure in order to increase the False Positive Rate (FPR).

4.3 Time Analysis

The average time taken by the wormhole attack route is more than the usual routing. In order to calculate the difference in routing time among normal route and wormhole route, the synchronization method is connected with all the hop nodes in the route. It can also be calculated in another form where the S node drives a lightweight message to the node D in the order it maintains the sent time of a packet. When a HELO message is received by the destination node, it, in turn, replies with the HELO-RPLY message. The minimum time of every hop is obtained. Implementation of the synchronized clock is expensive in MANET. In simple time difference method, it is hard to find out the location in order to identify the fraudulent nodes. During the route discovery, the obtained route information is stored in a routing table. Each time the routing table is verified individually whether any wormhole node is presented in the path or not. If it is present then it eliminates that path and chooses another which doesn't have any wormhole attacks.

4.4 Hop Count Analysis

The number of hops and the network congestion more by wormhole route is less and high than the normal route respectively in shortest path routing. In order to detect a wormhole attack, the hop count process is also considered. The minimum time for one hop communication is calculated by splitting the total number of hop by the entire time it takes. When a minimum hop time is higher than a normal hop, the fraudulent node is present. In order to obtain a minimum time or a distance GPS device or a synchronized clock is required.

4.5 Neighborhood

One of the significant features helps to detect wormhole attack is that it has only two neighbor nodes in its route. So, a wormhole could be detected when it fetches the data that is related to its neighboring nodes. This kind of problems arises in a larger network where every node has many neighbors. Hence more memory storage and power are required. Because of these techniques, the neighbor list gets changed frequently and it also increases FPR.

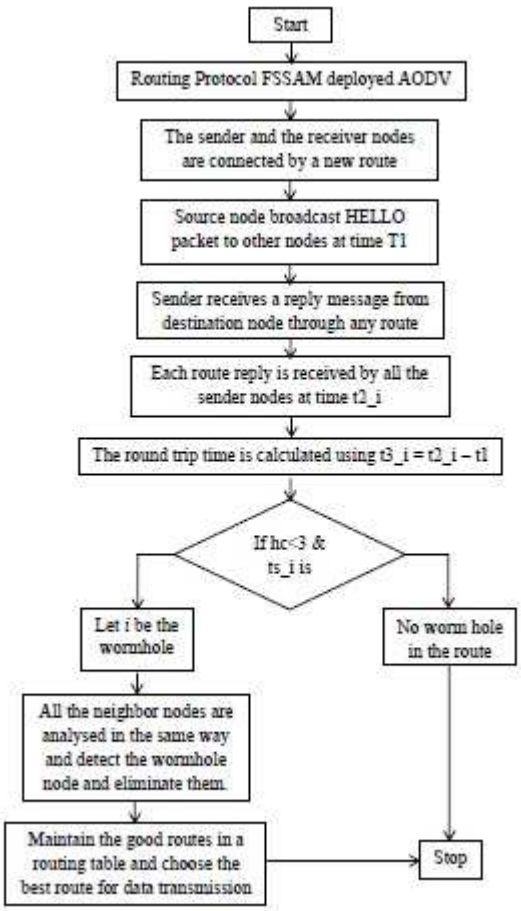

Fig. 3: Route analysis-based WHA detection

4.6 Data Packets

Certain intrusion detection technique detects the node in wormhole by manipulating the proportion of packets sent and received. The nodes in the network are to track the number of packets sent and received by its nearby nodes and persisted in a routing table, so that they could ascertain the states of its neighbors. This technique works efficiently in a larger network with a higher rate of mobility.

5 Results and Discussion

5.1 Simulation Settings

The network simulator is focused to be implemented and executed as a simulation model for FSSAM method. Set of the parameter with some value is shown in Table 1 in order to obtain a simulation environment. It also contains the network area, mobility speed, propagation delay. By initializing and assigning the parameters in network

Table 1: Simulation parameter settings

Parameter	Value
X, Y	1500, 1500
Routing Protocol	AODV
PROB	Radio Propagation
NN	100 to 500 Nodes
MAC	MAC/802.11
Energy Model	Energy-model = true
Mobility	Random
Moving Speed	2 m/s
Traffic	CBR
Bandwidth Link	2 Mbps
Propagation path loss model	Two-Ray ground Model
Propagation channel frequency	600 KHz
Propagation speed	1500 meter/sec
Propagation limit	111 dbm
Propagation path loss model	Free space
Transmit power	33 dbm
Receive sensitivity	98 dbm
Receive threshold	88 dbm
Data rate	100 kbps
Channel bandwidth	100 KHz
Antenna model	Omni-directional
Maximum transmission range	100 meters

simulator software it is able to calculate the relevant results in term of throughput, energy and so on.

Based on the control parameters like mobility, size of the network, number of nodes with load and certain performance values such as Packet Delivery Ratio (PDR), delay, throughput and so on are calculated in the simulation. The performance of FSSAM is evaluated by calculating various parameters. The total number of nodes is changed in each round of operation and performance is calculated. Throughput is calculated by the packets ratio that has been effectively received by the destination within the time duration. E-2-E delay calculates the quantity of time it takes to travel its data path. PDR is the ratio between the delivered packets to the total number of packets sent and it also determines the excellence of request in the form of congestion control and congestion is caused in the network because of routing overhead. The NS2 simulator comprises some parameters control and performance metrics such as network size, number of S and number D nodes, the load of the network, throughput, overhead, e-2-e delay and PDR.

In the existing algorithm, [14] obtained the simulation results such as wormhole detection rate and route failure rate. But in this paper, FSSAM method is verified in terms of various parameters like throughput, energy, delay taken for detecting wormhole attack, end-to-end delay, packet loss, and PDR.

According to the number of nodes deployed, QoS parameters are calculated. The nodes taken in each round of the simulation process is 100, 200, 300, 400 and 500. The outcome results are compared with the results mentioned by [15]. The throughput of both systems is

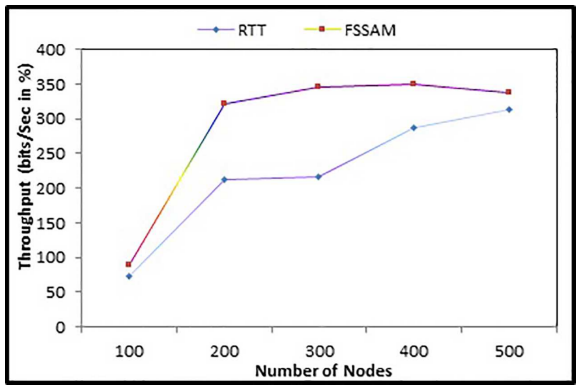

Fig. 4: Number of nodes versus throughput

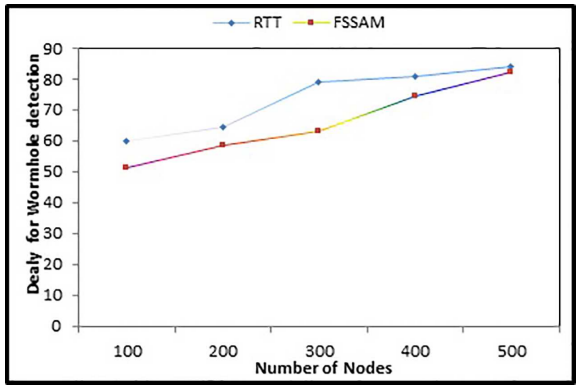

Fig. 5: Number of nodes versus delay taken for wormhole detection

calculated according to the number of nodes deployed in the network. The quantity of node decides the density of the network and it may or may not increase the number of intermediate nodes in the network. Also, the communication rate and transmission of data depend on the number of nodes communicating within a time of interval. The comparison results in terms of throughput using both existing (RTT) and proposed FSSAM systems are shown in Fig. 4 Throughput obtained using FSSAM is higher than the RTT at each round of network operations.

For example, when the quantity of nodes is 500, the throughput obtained by RTT is 312.44 and by FSSAM is by 336.89. From the throughput value, it is decided that the proposed FSSAM method is better than the RTT method.

To verify the efficiency of the FSSAM, a number of wormhole attackers are created in the simulation and checked whether the FSSAM method detects them or not. If this happens, then the time taken for identifying the wormhole nodes in the network is estimated. The time duration taken for values obtained from simulation, for 5% of wormhole nodes is calculated as shown in Fig. 5 From the result, it is noticed that the time taken for detecting wormhole attack by FSSAM is very less than RTT. For example, time taken for detecting 5% of wormhole nodes out of 500 nodes by FSSAM is 81.99

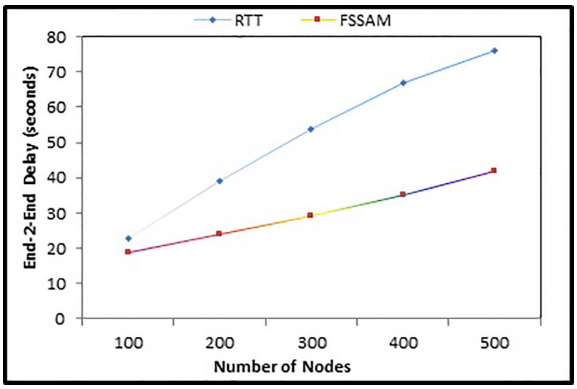

Fig. 6: Number of nodes versus remaining energy

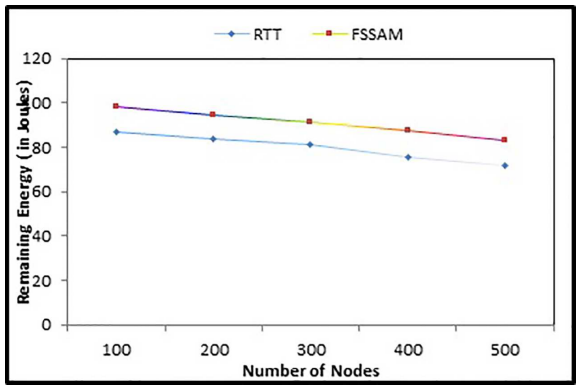

Fig. 8: Number of nodes versus packet loss

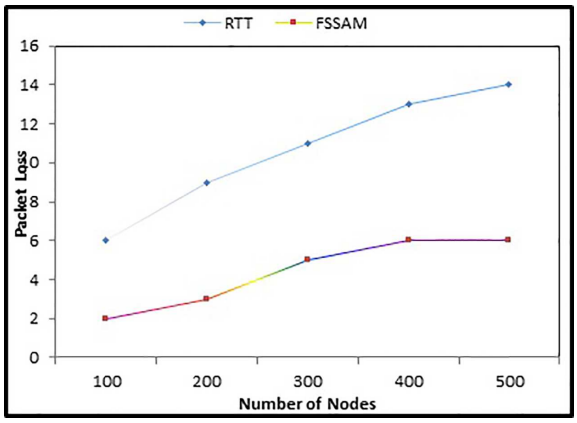

Fig. 7: Number of nodes versus end-2-end delay

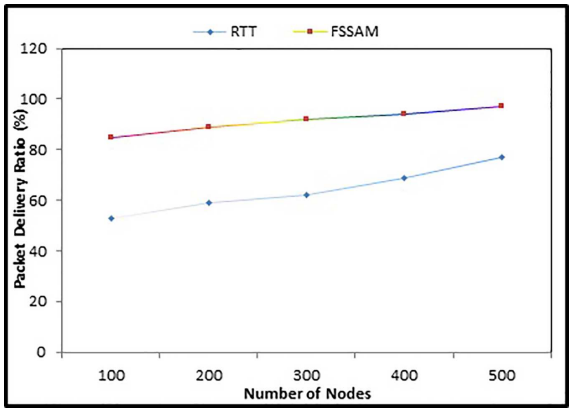

Fig. 9: Number of nodes versus PDR

seconds and by RTT is 84.22 seconds. Hence, in terms of wormhole detection delay, FSSAM is better than RTT.

For each communication, even for living in the network each node needs some amount of energy. The energy is consumed after certain functions like, transmit, receive and listen, wakeup, idle and idle-listen. All the nodes are initialized by a fixed amount of energy (for example initial_energy = 100). When the node starts doing a function, the energy of the node is reduced due to function carried. To calculate the energy consumption, here the remaining energy is calculated. The obtained results in terms of remaining energy are shown in Fig. 6

The other QoS parameter which defines the effectiveness of the proposed system is end-to-end delay. The time consumed to complete a single cycle of data transfer from source to destination is the delay. The delay calculated using RTT method and FSSAM method is given in Fig. 7. From Fig. 7, it is understood that the delay taken by FSSAM method is very less than the RTT method where it shows that FSSAM is more efficient. The presence of wormhole attack transmits the data in their private route which is illegal. This means that the data packet does not transmit through the original path to the real destination and it is considered as packet loss. The obtained packet loss using FSSAM is very less than the existing RTT method and it shows that FSSAM is more efficient than the RTT method. From Fig. 8, it is identified that the number of attacker nodes detected by RTT is 14, whereas FSSAM is 6. The reason for less wormhole detection is FSSAM which provides prevention in the network and it avoids wormhole attack. Also, more packet loss determines the in-efficiency of the approach and it is decided that those kinds of approaches are not suitable for better routing in MANET.

Finally, the PDR is calculated in the simulation for FSSAM approach and the obtained result is shown in Fig. 9 The number of packets effectively received in end node is called as PDR. From the obtained result it is clear that the amount of PDR achieved by FSSAM is higher than the RTT. For example, when 500 nodes are deployed in the network, the PDR obtained by RTT method is 77% whereas FSSAM is 97%. The high PDR determines the more quality of service of the method in general. From the comparative results, it is concluded that FSSAM is a suitable method for data transmission with very good detection procedure.

6 Conclusion

The most important purpose of this work is to model and implement a Five Stage Security Analysis Model (FSSAM). The proposed model is designed for identifying the wormhole attacks in MANET. Network simulation-2 software is used to simulate the proposed system and performance is analyzed. From the results, it is analyzed that the proposed FSSAM approach is enhanced more than the RTT method in terms of various QoS parameter.

References

[1] C. Siva Ram Murthy and B.S. Manoj, *Mobile Ad Hoc Networks-Architectures and Protocols*, Pearson Education, New Delhi (2004).

[2] M. Meghdadi, S. Ozdemir and I.A.Güler, A survey of wormhole-based attacks and their countermeasures in wireless sensor networks. *IETE Technical Review*, **28**(2), 89–102 (2011).

[3] R.S Khainwar, M.A. Jain and M.J.P. Tyagi, Elimination of Wormhole Attacker node in MANET using performance evaluation multipath algorithm, *Journal of Network and Complex Systems*, IISTE, **3**(7), 22–29 (2013).

[4] K.S. Win, Analysis of detecting wormhole attack in wireless networks. In World Academy of Science, Engineering and Technology, *International Journal of Electronics and Communication Engineering*, **2**(12), 2704–2710 (2008).

[5] M. Imran, F.A. Khan, H. Abbas and M. Iftikhar, *Detection and prevention of black hole attacks in mobile ad hoc Networks*, in: International Conference on Ad-Hoc Networks and Wireless. Springer, Berlin, Heidelberg, 111–122 (2014).

[6] P. Nagrath and B. Gupta, *Wormhole attacks in wireless adhoc networks and their counter measurements: A survey*, in: IEEE 3rd International Conference on Electronics Computer Technology, **6**, 245–250 (2011).

[7] Y.C. Hu, A. Perrig and D.B. Johnson, Wormhole attacks in wireless networks, *IEEE Journal on Selected Areas in Communications*, **24**(2), 370–380 (2006).

[8] V. Mahajan, M. Natu and A. Sethi, *Analysis of wormhole intrusion attacks in MANETS*, in: MILCOM'2008 IEEE Military Communications Conference, 1–7 (2008).

[9] J. Zhen and S. Srinivas, *Preventing replay attacks for secure routing in ad hoc networks*, in: International Conference on Ad-Hoc Networks and Wireless, Springer, Berlin, Heidelberg, 140–150 (2003).

[10] M.R. Alam and K.S. Chan, *RTT-TC: A topological comparison based method to detect wormhole attacks in MANET*, in: 2010 IEEE 12th International Conference on Communication Technology, 991–994 (2010).

[11] S. Keer and A. Suryavanshi, *To prevent wormhole attacks using wireless protocol in MANET*, in: IEEE International Conference on Computer and Communication Technology (ICCCT), 159–163 (2010).

[12] A.S. Alshamrani, *PTT: packet travel time algorithm in mobile ad hoc networks*, in: IEEE Workshops of International Conference on Advanced Information Networking and Applications, 561–568 (2011).

[13] I. Mokube, *Honeypots: concepts, approaches and challenges*, in: Proc. of the 45th Annual Southeast Regional Conference, 23–24 (2007).

[14] G. Wu, X. Chen, L. Yao, Y. Lee and K. Yim, An efficient wormhole attack detection method in wireless sensor networks, *Comput. Sci. Inf. Syst.*, **11**(3), 1127–1141 (2014).

[15] P. Amish and V.B. Vaghela, Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol, *Procedia Computer Science*, **79**, 700–707 (2016).

S. Muthukumar received the B.E. degree in Computer Science and Engineering from Madurai Kamaraj University in 2000. He received the M.E. degree in Computer Science and Engineering from Annamalai University in 2005. At present he is working as Associate Professor in the department of Computer Science and Engineering, SreeSowdambika College of Engineering, Aruppukottai, Tamil Nadu, India. He has 14 years of teaching experience to UG and PG classes. He is the Life member of Indian Society for Technical Education and Computer Society of India.

K. Ruba Soundar received the A.M.I.E. degree in Computer Science and Engineering from The Institution of Engineers (India) in 2000. He received the M.E. and Ph.D., degrees in Computer Science and Engineering from Anna University, Chennai in the year 2004 and 2010 respectively. Currently he is a Professor in Computer Science and Engineering Department of P.S.R. Engineering College, Sivakasi, Tamil Nadu, India. He has authored / coauthored over 100 research articles in various Journals and Conferences in the areas of Cloud Computing, Image Processing, Wireless and Wired Networking.