Cluster Computing (2019) 22:S7069–S7077
https://doi.org/10.1007/s10586-018-2418-2

Malicious node identification using quantitative intrusion detection techniques in MANET

M. Arul Selvan[1] · S. Selvakumar[2]

Received: 19 February 2018 / Accepted: 6 March 2018 / Published online: 29 March 2018

Abstract
Due to rapid proliferation of WSN, the application of wireless devices or nodes and usage of mobile computing devices changed the shape of network security. One of the field which need the most security is Mobile Ad hoc Network (MANET). The term ad hoc itself ensures that there is no central entity in order to govern the nodes. The issue of security is a critical problem when implementing mobile ad hoc networks (MANETs) is widely acknowledged. The traditional method of firewall and encryption is not sufficient to protect the network. Therefore an intrusion detection system must be added to the mobile ad hoc network. One of the different kinds of misbehavior a node may exhibit is selfishness. A indiscipline or selfish or node wants to protect own resources when using the services of others and consuming their resources. Malicious nodes that disobey the standard, degrades the performance of well-behaved nodes significantly. One way of preventing selfishness in a MANET is a detection and exclusion mechanism. In this paper, we de-scribe different method for detecting indiscipline or malicious nodes in mobile ad hoc network.

Keywords MANET · Malicious nodes · Intrusion · Proliferation

1 Introduction

The Mobile Ad hoc Network [1] is the collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictable over time. It is also known as infrastructure less net-work. Mobile Ad hoc Networks can form stand-alone groups of wireless terminals, but some of these may be connected to some fixed network. Compared to wireless networks in infrastructure mode ad-hoc net-working doesn't require any access points. This makes them useful in a lot of different applications. MANET [2] is largely used in military applications and in rescue operations where the existing communication infrastructure has been destroyed or is unavailable, for example after earthquakes and other disasters. As Mobile Ad hoc Networks (MANETS) is quickly spreading for the property of its capability in forming temporary network without the aid of any established infra-structure or centralized administration, security challenges [3] has become a primary concern to provide secure communication. MA-NETs is able to configure themselves on-the-fly without intervention of a centralized administration. The terminals in ad hoc network [4] that can not only act as end-system but also as an intermediate system (routers). It is possible for any two nodes that are not in the communication range of each other, but it still can send and receive data from each other with the help of the intermediate nodes which can act as routers. This functionality gives another name to ad hoc network as "multi-hop wireless network".

There are different routing attacks [5] which appear in network layer during wireless transmission of messages. These attacks are caused by either some internal or external intruders. We have done literature survey and gathered information related to different types of attacks and its solutions. We have observed that secure routing protocol is

✉ M. Arul Selvan
arulselvanm78@gmail.com

S. Selvakumar
cselvakumarphd@yahoo.com

[1] Bharath Institute of Higher Education and Research, Chennai, India

[2] Department of Computer Science & Engineering, G.K.M. College of Engineering & Technology, Chennai, India

the essential requirement and there is no general algorithm that suits well against the most commonly known attacks. In our paper we have proposed an approach that deals with the network layer attacks [6].

The term “ad hoc” means, nodes that are self-organized which means that they do not have a central entity to govern them. So, that’s how the name mobile ad hoc network (MANET) was formed. Unlike networks which are using dedicated nodes to support some of the basic functions [7] like routing, packet forwarding and network management, in adhoc networks these are carried out by all nodes. Nodes that present in an adhoc network move in all different directions with any speed but still they are connected to the network because of the wireless links. These ad-hoc networks do not have any kind of fixed infrastructure and are also called by the names MANET and adhoc networks. Each node acts like both a host and as a router at the same time in order to do both transmission and reception in a network. As the nodes keep moving in the network, the topology of the network changes frequently and it is not predictable. Whenever a There are different routing attacks [8] which appear in network layer during wireless transmission of messages. These attacks are caused by either some internal or external intruders. We have observed that secure routing protocol is the essential requirement and there is no general algorithm that suits well against the most commonly known attacks. In our paper we propose an approach called the quantitative intrusion detection techniques for dealing with the network layer attacks. Then the rest of the section is organized as follows, Sect. 2 discusses about the literature survey according to the intrusion detection, Sect. 3 examines the problem definition along with proposed the quantitative intrusion detection techniques in Sect. 4, excellence of the system is evaluated in Sect. 5 and conclusion in Sect. 6.

2 Related Works

Razak et al. [9] demonstrated friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks through friendship relation. The main objective of this work is to reduce the false alarms. Here a collaborative friend detection mechanism will be triggered to support the IDS decision along with a local anomaly detection mechanism. This mechanism is able to solve the problem caused by the colluding blackmail attackers.

Otrok et al. [10] designed a unified framework that is able to prolong the lifetime of IDS in a cluster by balancing the resource consumptions among all the nodes. This is achieved by truthfully electing the most cost-efficient node that handles the detection process. Incentives are given in the form of reputations to motivate nodes in revealing truthfully their costs of analysis. Reputations are computed using the well known Vickrey, Clarke and Groves (VCG) mechanism where truth-telling is the dominant strategy. The distributed mechanism is able to elect the most cost-efficient node and to punish misbehaving nodes by withholding cluster’s services. A cooperative decision game theoretical model is established to efficiently catch the misbehaving leader-IDS with less false-positive rate. Additionally, a zerosum non-cooperative game is used to help the leader-IDS to maximize the probability of detection. This game is played between the leader-IDS and intruder with incomplete information about the intruder’s identity. The solution of the game advised the leader-IDS to his/her optimal sampling strategy. The simulation results show that the framework is able to elect the most cost-efficient node, reduce the catch false-positive rate by the checkers and maximize the probability of detection by the leader-IDS.

Komninos and Douligeris [11] proposed a layered intrusion detection framework (LIDF) to detect compromised and malicious nodes in an ad-hoc network. LIDF consists of three modules namely, collection, detection and alert. These modules operate locally in every node of a network. The collection and storage of audit data is performed with the use of a binary tree. The detection is achieved with Lagrange interpolating polynomials and the alert is accomplished with linear threshold schemes. The detection method handles route logic compromise, traffic patterns distortion and denial of service attacks. The detection approach is implemented with dynamic source routing protocol, the ad-hoc on-demand distance-vector routing protocol and the destination sequenced distance vector routing protocol. The performance is evaluated using the metrics detection rate and false alarm rate.

Al-Roubaiey et al. [12] developed adaptive acknowledgment intrusion detection for MANET with node detection enhancement. This is an acknowledgement based scheme which can be considered as a combination of scheme called TACK and an end -to-end acknowledgement scheme called ACKnowledge (ACK). In this system source node sends out packet 1 to its destination. All the intermediate nodes simply forward this packet. When the destination node receives packet 1, it is required to send back an ACK acknowledgment packet to the source node along with the reverse route within a predefined time period. If the source node once receives this ACK packet, then packet transmission from source to destination node is successful. Otherwise, the source node will switch to TACK scheme by sending out a TACK packet. AACK greatly reduces the network overhead.

Mohammed et al. [13] described a mechanism design based model for secure leader election in the presence of selfish nodes. To balance the resource consumption of the nodes in the network, nodes with the most remaining resources should be elected as the leaders. This model has introduced a two leader election algorithm, namely cluster dependent leader election (CDLE) and cluster independent leader election (CILE). The former does not require any pre-clustering whereas CDLE requires nodes to be clustered before running the election mechanism. The ideas proposed by them are mainly focused on the leader election process instead of detecting the malicious behavior.

Nadeem and Howarth [14] have adopted generalized intrusion detection and prevention (GIDP) mechanism for protecting various unknown attacks. Detection and prevention of a specific kind of attack such as sleep deprivation, black hole, grey hole, and rushing or sybil attacks on MANET has been focused. GIDP mechanism uses the combination of anomaly-based and knowledge based intrusion detection to secure MANET from a wide variety of attacks. The impact on the MANET performance of the various attacks and the type of intrusion response has been investigated.

Duhan et al. [15] handling many security threats such as security, functionality, network lifetime issues due to the resource utilization in wireless sensor networks. This security issues has been overcome by applying the intrusion detection techniques which handles the security threats according to the game theory approach, probability distribution, specification based approach, computational and data mining methods for overcoming the intrusion issue while accessing the data in wireless sensor environment.

Basabaa et al. [16] proposed an Adaptive three acknowledgements scheme. This method is an acknowledgement based technique on Dynamic source routing Protocol. It aims to solve the weaknesses of Watchdog scheme. It consists of three main models, namely End-To-End Acknowledgement (Aack) model, Two Acknowledgement (Tack) model and Three Acknowledgment (Thack) model. In the A3ACK, the default model is AACK model. The Thack model aims to solve the problems of receiver collision and limited transmission power and collaborative attacks. The performance of the system is evaluated using the metrics packet delivery ratio and routing overhead.

Pattanayak and Rath [17] proposed a mobile agent based intrusion detection and prevention architecture for a clustered MANET. This specific approach makes the mobile ad hoc network more robust to the external intrusions directed at the nodes in an ad hoc network. The advantages of this model are listed as follows. The architecture is simplified enough to implement. The model is applicable to a variety of applications such as simplified communication since no multi-hop communication is allowable. The Intrusion detection procedure is simple enough as the detection module monitors only the cluster head. The drawbacks of this approach are the mobile agent may happen to be overloaded with multiple functionalities that may lead to errors. The process may not optimally run the real time applications with limited time bounds since the communication is time consuming for the reason that all packets are routed through the cluster head. Deployment cost may appear to be very high and may not conform to the needs of a customer.

3 Problem statement

Intrusion can be defined as, any kind of unwanted or unexpected activity [18] happened in the network which is affecting the integrity, confidentiality or using a network resource without its prior permission. A system which is used to find out these abnormal behaviors in this network is called as “Intrusion Detection System (IDS)” and the way that it does the actions can be termed as “Intrusion Detection”. There are many approaches for Intrusion Detection [19] in MANET. Mainly there are two important classifications of IDS and are namely behavior based and authentication based. Both the classifications give a brief thought about them by their names and in detail the former one is completely based on the behavior of a node and its nodal activities whereas the later one is based on authenticating the identity of a node and the usage of encryption keys (public key and private key pairs) falls into this category. The former approach is behavioral based algorithms where intrusion is defined based upon its nodal activities instead of its identifier. According to us, this is a better approach because of the following reasons such as Behavior of a node is very tough to replicate and No need of storage of identities. But the main challenge is to find a distributed, quantitative and dynamic intrusive detection solution for MANET which involves mobile nodes in a non-cluster based environment. In addition to this, our other challenge is to develop simulations for MANET which includes as follows namely, Implementation of the IDS, Implementation of a suitable routing protocol and mobility model and Physical layer which meets the IEEE 802.11 standards.

4 Proposed system

The proposed solution to our research challenge is discussed in detail in this paper. This solution is based on the quantitative intrusion detection techniques which have been proved in, but the solution is applied to a MANET [20] which contains mobile nodes. The main challenges to develop simulations for MANET are broadly classified into four parts. They are Intrusion Detection, Availability of mobility models, Availability of routing protocol implementation and Physical layer with Ieee standards for 802.11 which are explained as follows.

4.1 Intrusion detection

In this section discusses about the detailed explanation of intrusion detection process. Especially to deal with the insider attacks of a network, IDS techniques have been developed for detecting compromised nodes and also removing malicious nodes from the network in order to receive high survivability of the network and also to make the data secure. Pattern recognition approach is also a kind of approach which is used for intrusion detection. We are following the behavioral based detection for our IDS. In support with this the detection of malicious nodes can be done in two steps. First we need to identify which nodes are displaying the malicious/abnormal/unexpected behavior in the network and once we get the suspicion about the nodes which are in the network and then our process justifies its suspicion i.e., finalizing whether the suspicious node is the malicious node or not.

4.2 Identifying the malicious nodes

The term "malicious" signifies that something is wrong which has been termed as malicious whatever it could be. In this situation, it applies to a node(s) which are displaying this behavior and the process of identifying those node(s) is called as "Identifying the malicious node(s)". This whole process can be broadly classified into two major steps and they are recognizing a suspicious node and Confirming that the node is malicious. These mentioned steps are explained in the following sub section.

4.3 Recognizing a suspicious node

The scope of this current research allows us to define the nodes to be termed as "malicious" when any node in the network is observed to have a different behavior than the regular behavior. Li and Alam et al., in have proposed a method that the nodes are expected to acknowledge the messages that they had received and also every node measures the acknowledgements that it has received and they have calculated that and the value is a measure of the near-term behavior. After a certain period of time this calculated value is called as the "Stability" of the nodal behavior and is referred to as "STB" from now on. With this the transmission quality of data is also calculated and it called as "Data Transmission Quality" (DTQ). In current research, the transmission of packets is considered as either a packet has been transmitted completely or the packet has not be transmitted at all which is like on and off of a switch i.e., either 1 or 0. But there will be nothing like partially transmitted packet. Each node calculates this "DTQ" value and also maintains it for its neighboring nodes (= nodes which are only in the transmission range for a node). If there is a fall of the DTQ value which is less than the threshold then the particular node can be a malicious node in the network. And even the threshold value will be updated periodically in the network.

4.4 Confirming that a node is malicious

This is the second step in the process of identifying a malicious node in the network. After the successful completion of the process in the above step, the confirmation that a node is malicious has to be done in this step. The process of confirming that a node is malicious is done by voting process. The node which observed suspicious activity [21] on any other node will start the voting process in that network about that node. Depending upon the votes that it receives from the neighboring nodes in the network, the suspicious node will be either will continue its stay in the network or it will be out of the network (which means blacklisted) and finally be removed from the network as it will be confirmed that the suspicious node is the malicious node in the network.

4.5 Proposed algorithm

There are various routing attacks that appear in network layer when wireless transmission of messages. These attacks are caused by either some internal or external malicious intruders. The routing attacks are black hole, worm hole, rushing attack etc. be-come robust in network layer. During the malicious node imitates itself a valid route to the destination node and combines with the routing correctly but later on ignoring all the packets that pass through it rather than forwarding them. This attack is known as Black hole attack [22]. While when the nodes forward some selective packets to the destination node instead of all. Then the type of attack is called grey hole attack. To resolve these types of problems we ensure that each node in a network forwards packets to its destination properly. In the security to network layer in MANETS we propose here a new secure approach which uses a simple acknowledgement approach, principle of flow conservation and encryption. Here in this paper we use DSR protocol to detect malicious node and provide a secure method against the routing attacks.

In our approach we detect the malicious nodes while computing the route in the network and re-routing the packets around it, find the shortest path among them. The protocols are existing ad hoc routing protocols like DSDV, AODV and DSR designed [23] to handle attacks. The encryption is used while sending the packets from one node to another node. We use this approach to ensure the security to network layer in MANETs against attacks. The basic design of our proposed system provides security from more than 2 attacks. In our algorithm we used encryption, acknowledgement and principle of flow conservation approach to security against attacks. Before discussing algorithm some basic terms are given for algorithm development:

- *Start time*—The packet sending time by the source node.
- *End time*—The time taken for the acknowledgement to reach back the source.
- *Round trip time* (*RTT*)—The total time taken for transmission.
- To count the number of packets sent by counter *Cpkt* is used.
- To count the number of lost packets counter *Cmiss* is used.
- In reference to principle of flow conservation the tolerance is set to some threshold value i.e. in this algorithm it will be 20%.
- When an acknowledgement received by the sender exceeds the RTT time limit, then the data packet will be accounted as a lost packet. The RTT time is set to 20 ms.

We calculate the (Cmiss/Cpkt) ratio. If the calculated ratio is greater than the limit of tolerance threshold value 20%, then the link is said to be misbehaving [24] otherwise properly behaving. Parallelly using the ratio value, the corresponding attacks will be identified. In our algorithm encryption method is applied on message from sender side and the message is decrypted at receiver side. In data format only 48 bytes are sent at a time. So the message is longer than 48 bytes is divided into packets of 48 bytes each. Each time when a packet is sent the counter Cpkt gets incremented and the time will be the start time.

- At the receiver node the message is decrypted and an acknowledgement ACK packet is sent back to the sender through the intermediate nodes. Else when the decrypted mes-sage doesn't match then the acknowledgement packet sent back to the sender through the intermediate node consists of "CONFIDENTIALITY LOST".
- At Sender side, when acknowledgement reached, it computes the time taken for this acknowledgement to reach (end time). These steps are perform by the sender side-

Algorithm

```
1.IF(Total Transmission Time taken (end-start) > pre-specified interval( 20 ms)) Then
{
        2.Rejects the corresponding data packet, announce it as lost data packet and Increment
        the Cmiss counter.
}
 Else
{
        3.It checks for the contents of acknowledgement field.
        4.If (The ratio of (Cmiss/Cpkt)>=20% )Then
        {
                i) The intermediate node is malicious and a new field"CONFIDENTIALITY
                   LOST" is built in to the acknowledgement frame.
                ii) Sender switches to an alternate intermediate node for the future sessions.
                        Otherwise another new field "ACK" is built to the acknowledgement
                        frame.
                iii) This intermediate node is decided to be behaving as expected and the
                        transmission is continued with the same intermediate node. Such type
                      of intermediate nodes can be called genuine nodes.
                      }
                      }
```

The algorithm mainly identifies four attacks parallelly namely packet eavesdropping, message tampering, black hole attack and gray hole attack.

4.5.1 Packet eavesdropping

In Packet eavesdropping while delivery of packets some of the malicious nodes tend to drop packets intentionally to save their own resources and disturb the network operation. It can be determined by the value of the (Cmiss/Cpkt) ratio.

(i) If (Cmiss/Cpkt) $>$ 20%,
(ii) Then link contains a malicious node launching packet eavesdropping attack.

4.5.2 Message tampering

Sometimes network security integrity principle is not followed by the intermediate nodes. They pretend to tamper the data which has been sent either by deleting some bytes or by adding few bytes to it. This is an intentional malicious activity by the intermediate malicious nodes.

(i) If the acknowledgement frame sent by the receiver contains “CONFIDENTIALITY LOST” field in it. Then the node is called tam-pered the data sent.
(ii) If Ratio (Cmiss/Cpkt) $>$ 20%, Then link is called misbehaving and attack is message tampering.

4.5.3 Black hole attack

If the ratio (Cmiss/Cpkt) $\geq$ 1.0, Then all the sent packets are said to be lost or eavesdropped by the mali-cious node.

Gray hole attack: When the nodes forward some selective packets [25] to the destination node instead of all. Then this type of attack is called grey hole attack. In this attack malicious inter-mediate nodes selectively eavesdrop the packets i.e. 50% of the packets, instead of forwarding all. Thus If the ratio (Cmiss/Cpkt) $>$ 0.2 and (Cmiss/Cpkt) = 0.5, Then half of the packets that have been sent are eaves dropped by the malicious node. Based on the above process, the intrusion has been detected with effective manner according to the Cmiss and packet value. Then the excellence of the system is evaluated in terms of using experimental results which are explained as follows.

5 Experimental results

This section deals with the discussions about the results that were captured from the simulation runs. During the implementation process, the system uses the following simulation setup which shown in Table 1.

According to this, the few factors such as changes of mobility node, various speed settings which are discussed as follows.

5.1 Changes by mobility of the nodes

The detection of malicious nodes has been analyzed by varying the speed of the mobility of the nodes in the network.

5.2 Settings used for varying speed

Number of nodes = 10
Simulation run time = 500 s
Mobility update interval = 100 ms
Malicious nodes = 4

5.3 Varying speed

By varying the speed at which the node travels in the network. The variation of detection of malicious nodes in the network with our IDS is obtained as follows

The plot which is shown in above Fig. 1 shows the detection of malicious node versus simulation time (in seconds) with varying the speed of the mobile nodes in the network. From the figure it clearly shows that all the malicious nodes are successfully detected, If we observe the above graph then we can see that there are also false positives and False positives can be analyzed by the output files and especially by observing and analyzing the sent/received message counts that are obtained and they may occur due to one of the following reasons such as vote replies may be lost, false positives will decrease when the nodes have the comparable movement. When the node moves very fast then there might be connections that are lost and loss of packets and eventually there will be some false positives and during the process of transit, time-out in receiving the replies, losing connectivity when the nodes are mobile there might be loss of packets. The routing protocol also be the reason for a definite loss factor and is documented in the AODV routing protocol implementation.

5.4 Changes by malicious node count

The detection of malicious nodes has been analyzed by varying the number of the malicious nodes in the network.

5.5 Settings used for varying number of malicious nodes

Number of nodes = 20

Table 1 Simulation parameter

Simulation parameter	Parameter value
Simulator	NS2 (v.2.34)
No of nodes	300
Area size	900 × 900
MAC	802.11
Radio range	250 m
Simulation time	100 s
Traffic source	CBR
Packet size	128 bytes
Mobility model	Random way point
Protocol	AODV

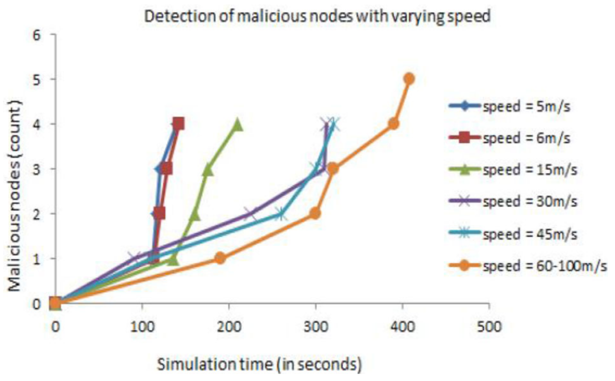

Fig. 1 Malicious node detection

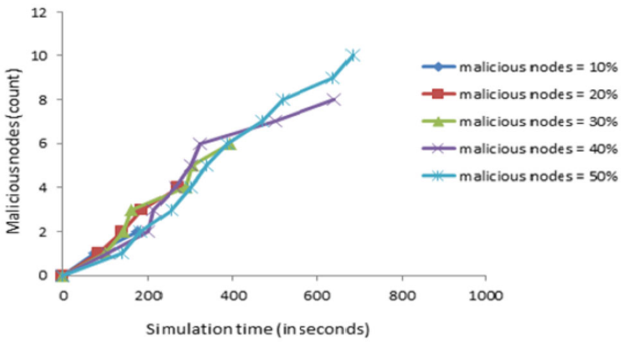

Fig. 2 Malicious node detection with time

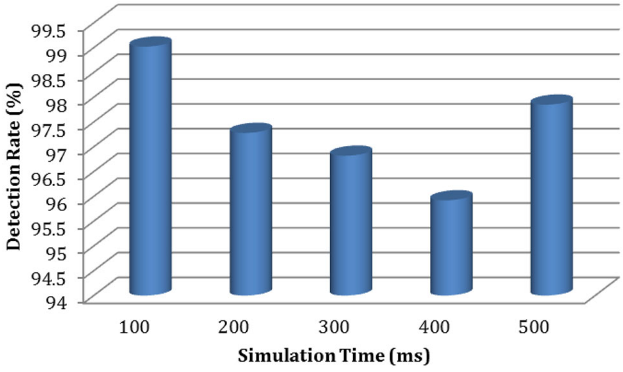

Fig. 3 Intrusion detection rate

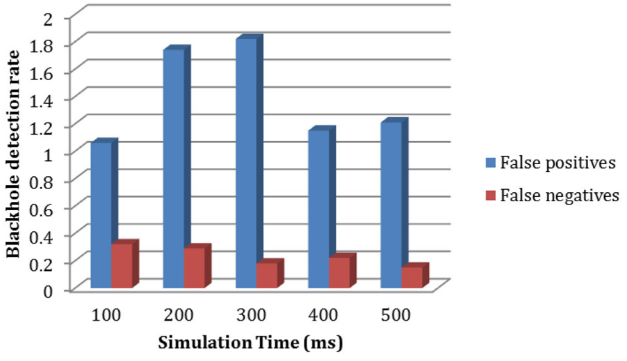

Fig. 4 Black hole detection rate

Simulation run time = 1000 s
Mobility update interval = 100 ms
Area size = 1000 × 1000 flat area
Transmission range = 250 m

By varying the number of the malicious nodes in the network, the variation of detection of malicious nodes in the network with our IDS is obtained as follows:

The graphs which are shown in the above Fig. 2 have started with plotting the values from 10% of malicious node count to 50% of malicious node. All the malicious nodes were successfully detected in these tested scenarios. No false positives were appened even though for some cases the simulation has ran for considerable amount of time (some times longer durations). This proves that the

Table 2 Black hole attack detection rate

Running time (sec)	Black hole attack		
	Detection rate (%)	False positives (%)	False negatives (%)
100	99.02 ± 0.14	1.06 ± 0.12	0.32 ± 0.05
200	97.28 ± 0.42	1.74 ± 0.09	0.29 ± 0.02
300	96.82 ± 0.48	1.82 ± 0.06	0.18 ± 0.03
400	95.92 ± 0.68	1.15 ± 0.05	0.22 ± 0.01
500	97.85 ± 0.52	1.21 ± 0.08	0.15 ± 0.06

IDS has good detection rate and more detailed values about the detection rate were given in the Table 2

The above Fig. 2, clearly depicted that the intelligent technique effectively detect the malicious nodes with various simulation time. According to this, the detection rate of black hole attacks is shown in Table 1. Detection of IDS in black hole attack is listed in the table below

The above Table 2 clearly indicates that proposed system detects the black hole attack with high detection rate 99.02% accuracy for 100 simulation time, 97.28% for 200 simulation time, 96.82% for 300 simulation time, 95.92% for 400 and 97.85% for 500 time. Then the achieved detection rate is shown in Fig. 3.

Along with the detection rate, the quantitative techniques consumes minimum ensures minimum false negative rate and attains correct false positive rate which is shown in Fig. 4.

Thus the proposed quantitative intrusion detection technique effectively predicts the black hole attacks successfully with different simulation time and simulation runs.

6 Conclusion

Our aim was to identify the malicious node(s) in a MANET where the nodes are mobile in the network; suspicion and the detection process of finding the malicious node in the mobile ad hoc network is based on the behavior of the node(s). We have chosen to use NS2 as the simulator for creating the environment of the Mobile ad hoc network. As the nodes are mobile, so obviously they do need a routing protocol for the implementation of mobility. So, in order to perform this function we have used the AODV i.e., Adhoc On-demand distance vector routing protocol. The MAC and physical layers for this follows the standards of IEEE 802.11. The attacks that we had used in this research in order to test the IDS are Packet eavesdropping, Message Tampering, black hole attacks and grey hole attack. All the malicious nodes were successfully detected. Each point in the plots is an average value of 10 runs. All the data that has been collected has been put in the previous chapter and also we have discussed about the results in detail. Our IDS can detect malicious nodes with almost 95% proficiency in the worst case scenario. And also the percentages of the false positives and false negatives are also reasonable and have never exceeded 5% for most simulation cases. This paper proposes a way to identify parallelly different types of attacks in MANETS. This proposed system is highly secure as it more concentrates on identifying number of significant packets dropped, misbehaving links and malicious nodes parallelly. This paper shows the implementation of identification and prevention of malicious nodes launching packet dropping and message tampering attacks, using a semantic security mechanism. And therefore the security scheme is highly impossible to break, thereby making it a highly secured approach.

References

1. Khokhar, R.H., Ngadi, M.A., Mandala, S.: A review of current routing attacks in mobile ad hoc networks. Int. J. Comput. Sci. Secur. **2**(3), 18–29 (2008)
2. He, B., Joakim, H., Gu, Q.: Security in adhoc networks, An essay produced for the course secure computer systems HT2005 (1DT658) (2005)
3. IEEE Std. 802.11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications (1997)
4. Mamatha, G.S., Sharma, S.C.: A robust approach to detect and prevent network layer attacks in MANETS. Int. J. Comput. Sci. Secur. **4**(3), 275–284 (2009)
5. Sundararajan, T.V.P., Shanmugam, A.: Behavior based anomaly detection technique to mitigate the routing misbehavior in manet. Int. J. Comput. Sci. Secur. **3**(2), 62–75 (2009)
6. Tun, Z., Maw, A.H.: Wormhole attack detection in wireless sensor networks. World Acad. Sci. Eng. Technol. **22**, 545–550 (2008)
7. Dhanalakshmi, S., Rajaram, M.: A reliable and secure framework for detection and isolation of malicious nodes in MANET. Int. J. Comput. Sci. Netw. Secur. **8**(10), 184–190 (2008)
8. Gonzalez, O.F., Ansa, G., Howarth, M., Pavlou, G.: Detection of packet forwarding misbehavior in mobile ad-hoc networks. J. Internet Eng. **2**(1), 181–192 (2008)
9. Razak, S.A., Furnell, S.M., Clarke, N.L., Brooke, P.J.: Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks. Ad Hoc Netw. **6**(7), 1151–1167 (2008)
10. Otrok, H., Mohammed, N., Wang, L., Debbabi, M., Bhattacharya, P.: A game-theoretic intrusion detection model for mobile ad hoc networks. Comput. Commun. **31**, 708–721 (2008)
11. Komninos, N., Douligeris, C.: LIDF: Layered intrusion detection framework for ad-hoc networks. Ad Hoc Netw. **7**(1), 171–182 (2008)
12. Al-Roubaiey, A., Sheltami, T., Mahmoud, A., Shakshuki, E., Mouftah, H.: AACK: Adaptive acknowledgment intrusion detection for MANET with node detection. In: 24th IEEE International Conference on Enhancement, Advanced Information Networking and Applications (AINA) (2010)
13. Mohammed, M.N., Sulaiman, N.: Intrusion detection system based on SVM for WLAN. Procedia Technol. **1**, 313–317 (2012)
14. Nadeem, A., Howarth, M.P.: A survey of manet intrusion detection & prevention approaches for network layer attacks. IEEE Commun. Surv. Tutor. **15**(4), 2027–2045 (2013)
15. Duhan, S., Khandnor, P.: Intrusion detection system in wireless sensor networks: a comprehensive review. In: Electrical, Electronics, and Optimization Techniques in IEEE, pp. 2707–2713 (2016)
16. Basabaa, A., Sheltami, T., Shakshuki, E.: Implementation of A3ACKs intrusion detection system under various mobility speeds. Procedia Comput. Sci. **32**, 571–578 (2014)
17. Pattanayak, B.K., Rath, M.: A mobile agent based intrusion detection system architecture for mobile ad hoc networks. J. Comput. Sci. **10**(6), 970–975 (2014)
18. Choi, S., Kim, D., Lee, D., Jung, J.: International Conference on Sensor Networks, Ubiquitous, and Trust-worthy Computing, pp. 343–348 (2008)

19. Song, N., Qian, L., Li, X.: 19th IEEE International Parallel and Distributed Processing Symposium (2005)
20. Mutlu, S., Yilmaz, G.: A distributed cooperative trust based intrusion detection framework for MANETs. In: The Seventh International Conference on Networking and Services (2011)
21. Hubaux, J.-P., Buttyan, L., Capkun, S.: The quest for security in mobile ad hoc networks. In: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking computing, pp. 146–155. ACM, Long Beach, CA (2001)
22. Mitchell, R., Chen, R.: A survey of intrusion detection in wireless network applications. Comput. Commun. **42**, 1–23 (2014)
23. Liao, H.J., Lin, C.H.R., Lin, Y.C., Tung, K.Y.: Intrusion detection system: a comprehensive review. J. Netw. Comput. Appl. **36**(1), 16–24 (2013)
24. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E.: Anomaly-based network intrusion detection: techniques systems and challenges. Comput. Secur. **28**(1), 18–28 (2009)
25. Li, G., He, J., Fu, Y.: Group-based intrusion detection system in wireless sensor networks. Comput. Commun. **31**(18), 4324–4332 (2008)

M. Arul Selvan Research Scholar, Bharath Institute of Higher Education and Research, Chennai, India.

S. Selvakumar received Doctor of Philosophy in Computer Science and Engineering from the Anna University. He received the Master of Engineering in Computer Science and Engineering from the Madurai Kamaraj University. He received the Master of Business Administration from the same University. He is working as Professor in GKM College of Engineering and Technology, Chennai. His current research interests includes Data Analytics, Software Engineering, Mobile Computing. He has authored more than 70 referred papers in international journals and conferences in his research areas. He is a Senior Member in Computer Society of India, Member in IEEE, ACM, Institution of Engineers and ISTE.