International Journal of Grid Distribution Computing
Vol.7, No.6 (2014), pp.241-256
http://dx.doi.org/10.14257/ijgdc.2014.7.6.20

Intrusion Detection System for Mobile Ad hoc Networks Based on the Behavior of Nodes

S. Mamatha[1] and A. Damodaram[2]

[1]*Bhoj Reddy Engineering College for Women,Hyderabad,India*
[2]*JNTU College of Engineering,Hyderabad,India*
msathineni@yahoo.co.in, damodarama@rediffmail.com

Abstract

*A Mobile Ad ho**c** Network (MANET) can be defined as a network of mobile nodes that communicate over the wireless radio communication channel. It is also defined as a network without any underlying infrastructure and offers unrestricted mobility. Due to their open nature and lack of infrastructure, security for MANETs has become an intricate problem. To transmit data over such a network, generally any routing protocol that enables dynamic, self-starting multi hop routing between mobile nodes is used. However these routing protocols are vulnerable to various kinds of attacks. The conventional security mechanisms of protecting a network are not sufficient for these networks. Hence a second level of defense to detect and respond to the security problem called an Intrusion Detection System (IDS) is required. An IDS based on anomaly based intrusion detection that works by checking the behavior of the nodes was proposed to overcome some of the attacks like blackhole, grayhole and flooding attacks. Generally the malicious nodes demonstrate a different behavioral pattern of all the other normal nodes. So the specified approach where a Data Transmission Quality (DTQ) function is used to determine the behavior of the nodes as malicious or legitimate is used. The DTQ function is defined in such a way that it will be close to a constant or keep changing smoothly for genuine nodes and will keep on diminishing for malicious nodes. The proposed method was implemented using AODV as the routing protocol for transmitting data. The evaluation results show that the performance of the AODV protocol under attacks has improved significantly by using the proposed approach.*

Keywords: *MANET, Intrusion Detection System, blackhole, grayhole, flooding attacks, DTQ function*

1. Introduction

In the current era, the wireless and mobile communication networks have quickly developed and are widely used. A mobile ad hoc network (MANET) is a multi hop wireless network formed by the collection of mobile devices that cooperatively communicate with one another without any predefined infrastructure. The typical application areas where these MANETs are used include battle fields, emergency search, rescue sites and data acquisition in remote areas. The ad hoc network is hence useful in situations where the geographical and terrestrial conditions demand totally distributed network system. The lack of fixed infrastructure and dedicated nodes which provide network management operations like routers in the fixed network poses many new challenges. The first challenge being maintaining the connectivity in the network. This problem of routing data is solved by using protocols like AODV, DSR, *etc.* The second challenge is providing security to the network. The characteristics such as dynamic topology, limited resources, decentralized and

ISSN: 2005-4262 IJGDC

heterogeneous control and unfriendly environment , enforce the ad hoc network vulnerable to various attacks like spoofing, black hole attack, flooding, modification of packets, denial-of service, *etc.* [1, 2]. In order to secure the ad hoc network from these attacks the prevention based approach is not enough as it cannot protect against the attacks from internal nodes [3]. So it is necessary to provide a second level of defense called intrusion detection system. The intrusion detection system involves the runtime gathering of data from system operation and subsequent analysis of the data.

In this paper a modular solution is proposed that deal with internal attacks and attempts to solve the complete problem. In the proposed IDS, a distributed and cooperative architecture is used where IDS agents run on every node try to identify and isolate misbehaving nodes. The main function of the solution depends on the IDS agents. Each IDS agent consists of a Data Collection module, Intrusion Detection module, Voting module and Intrusion Response module. The function of IDS agent is to send data as a bunch and wait for acknowledgments. Based on which the DTQ of a node is calculated and this is the main criteria in the detection of the behavior of nodes. Each node evaluates the behavior of its neighbor and compares it with the calculated threshold. Based on the comparison result anode detects any other nodes as either misbehaving or legitimate. Once a node is detected as misbehaving , it will proceed for the segregation of nodes agreeably by other.

The entire working is structured around the four modules of the IDS agent which will be exemplified in detail later. As the segregation of malicious node is done globally by taking the consensus of all the other nodes of the network the problem of misbehaving node rejoining at any other place of the network is overcome in the solution.

The rest of the paper is organized as follows: Section 2 specifies the related work done. Section 3 presents an overview of the AODV protocol along with some attacks, in Section 4 the intrusion detection system is described, Section 5 describes proposed approach in detail. Section 6 summarizes the evaluation of the solution implemented in ns-2. Section 7 presents the conclusion and future work.

2. Related Work

Intrusion detection has become the most important issue in MANETS as it addresses, secure routing and also has interested many researchers. Various techniques for IDS have been proposed in literature. Some of the prominent techniques are presented briefly in this section.

Zhang and Lee have proposed an intrusion detection technique for wireless ad hoc network that used cooperative statistical anomaly detection technique [4]. In this method each node has an IDS agent running independently and detecting intrusion from local traces. Each node maintained only one hop information. If local evidence is uncertain; the neighboring IDS agents cooperate to perform the global intrusion detection. In this system they neglected the aspects of how their local data collection should find out about incidents such as dropped packets and obscured links. Serigo and Marti proposed an attractive intrusion detection system called watchdog for identifying the misbehaving nodes [5]. They implemented it on DSR (Dynamic Source Routing) protocol and rely on monitoring the neighbors in the promiscuous mode. The solution proposed was to forward packets to those nodes which share a prior trust relationship. The problem was that it was not applying any punishment against the detected nodes. Bhargava *et al.* [2001] proposed a solution to the attacks that are caused from node internal to the ethos network where the underlying routing protocol was AODV [6]. The IDS composed of Intrusion Detection Model (IDM) and the Intrusion response Module (IRM). The proposed model claims to capture the attacks like denial of service, impersonation,

routing information disclosure and distributed false requests. The problem with this method was that it has adopted a predefined threshold in identifying the malicious nodes, which is not supportive for the dynamic environment of MANETs. Venkatraman extended the Zhang and Lee model and proposed a method by modifying the protocol to maintain two hop information at each node for each route [7]. The detection method used threshold levels to identify packet dropping and route hijacking attacks. The overhead of this method was that it requires a modified protocol along with an intrusion detection agent at each node.

To detect attacks on AODV a solution based on pecification-based intrusion detection was proposed [8]. This approach uses a finite state machine for specifying correct AODV routing behavior and a distributed network monitor for detecting runtime violation specifications. The Real-Time Intrusion detection for Ad hoc Networks (RIDAN) is a novel architecture that is based on knowledge –based intrusion detection technique to detect active attacks performed against the routing fabric of the mobile ad hoc network [9].This method uses a finite state machine which enables the detection of real time attacks. But it is not shown in this system how an attack that requires more than one- hop information gets detected.

Hao Yang et al proposed a self organized network layer security in mobile ad hoc networks, called SCAN that protects the routing and data forwarding operations through localized collaboration and information cross validation [10]. In this method each node posses a valid token in order to cooperate with other nodes and participate in the network. A novel credit strategy for the tokens has been adopted to decrease network overhead as time evolves. The only drawback of this method was that there is a small probability of legitimate nodes being incorrectly accused. A mechanism which is competent of identifying and blaming those nodes that exhibit packet forwarding misbehavior by using the principle of flow conservation was proposed [11]. Though it is giving good detection rate the drawback is that they have adopted a predefined threshold which cannot support autonomic environment.

A method to identify, account and average abnormal data in a network using clusters was proposed [12]. Here, each node runs a local IDS agent and measures the abnormality by checking the variation of computed data from that of the normal data. The measured value is then reported to the cluster head, which is the incharge of taking all the decisions. The problem with this approach is that the cluster becomes non functional if the cluster head itself is compromised by the attacker. A non centralized solution for detecting the malicious nodes was proposed [13]. The proposed method very well detected the malicious nodes in a sensor network, but do not outfit to mobile nodes or MANETS. Kumar has proposed a distributed and dynamic intrusion detection system for MANETS based on the behavior of the nodes [14]. In this method there are no central entities and it is the function of each and every node to detect the malicious nodes and take respective action. A new intrusion detection architecture based on agents and clusters which is suitable for multi-hop networks were proposed [15]. In this method an IDS agent is attached to each mobile node. The IDS agents on each mobile node run independently to monitor the local activities and detect any abnormal behaviors. The problem with this method is that even though the detection of abnormality is done in the local IDS, the final process of confirming the abnormality is to be done at the cluster head. So if the cluster head itself is compromised the detection becomes obsolete.

In [16] an Enhanced Intrusion Detection System for the detection of malicious nodes using the Data Transmission Quality(DTQ) of nodes is proposed. Here the DTQ is used for the detection and isolation of all those nodes which simply drop the packets. It is also shown how the malicious nodes are detected efficiently by reducing the false positive rate. In the current paper, we use the same procedure of [16] and try to overcome the attacks like black hole attack, gray hole attack and flooding attack in an ad hoc network which is using AODV protocol as the routing protocol.

3. AODV and Attacks in AODV

3.1 Overview of AODV

AODV is an on-demand routing protocol. The route discovery process in this protocol is initiated only when a node needs to communicate with other nodes. First, the source node broadcasts a route-request (RREQ) packet to its neighbors. On receiving RREQ a node will unicast route reply packet (RREP) if it has a fresher route source node or it itself is the destination of RREQ. If the route does not exist then RREQ will be broadcasted to other nodes until it reaches the destination. Once the RREP is received by the source node, it starts the data transmission. The router table of the source, destination and all other intermediate nodes are updated by sending the route request, route reply and route error control messages during the route discovery process. AODV on the other hand also uses a sequence number and hop count to select newer or better routes. Figure 1 shows the process of route discovery in AODV. Node S wants to send data to node D. Node S first broadcasts the RREQ message to its neighbor nodes A and C. The intermediate nodes forward the RREQ packet to other nodes until it reaches node D. After receiving the RREQ the destination D will unicast a RREP packet back along the reverse path to the source. When the source S receives the RREP, it can start sending data to node D.

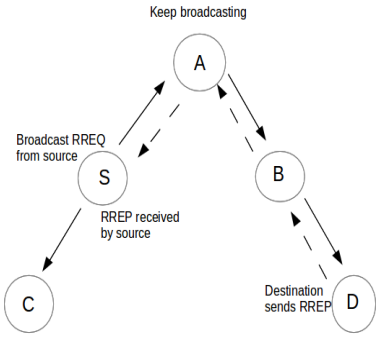

Figure 1. working of AODV

3.2 Attacks in AODV

In this section the attacks that can be easily implemented by an internal node against AODV and that are handled by the proposed IDS are discussed.

Blackhole Attack

In this attack the attacker by using the routing protocol advertise itself to have the shortest path to the node whose packet it wants to intercept. An attacker listens the request for routes in a broadcast based protocol. When the attacker receives a request for route to the destination it creates a reply consisting of an extremely short route. If this malicious reply reaches the source before the reply from actual node a fake route get created. Once the malicious node was able to insert itself in between the communicating nodes it can do anything with the packets passing between them.

Grayhole Attack

In this attack, data packets are dropped but the nodes malicious activity is limited to certain condition or trigger. The two common types of behavior are dropping of data packets

destined towards a certain victim node e, coming from certain nodes and behaving normally for other nodes. Dropping of data packets based on some predetermined trigger time while behaving normally during the other instances.

Flooding Attack

This attack is launched by flooding the network with fake RREQ or data packets leading to the congestion of the network and reduces the probability of data transmission of the genuine nodes.

4. Intrusion Detection System

4.1. Overview of IDS

Intrusion detection can be defined as the process by which malicious activities that may compromise system security are identified. An intrusion detection system is hence defined as a defense system which helps in identifying, assessing and repeating unauthorized or unapproved network activities. An IDS basically does not detect intrusions but detects the activity in traffic that may or may not be an intrusion by continuously monitoring the network for unusual activity. Because of the inavailability of concentration points and fixed infrastructure the IDS in MANET must run continually minimize overhead and the algorithm it uses may be distributed in nature.

4.2. Distributed and Cooperative IDS

A distributed wireless intrusion detection and response system proposed by Y. Zhang and W. Lee [5] is shown in Figure 2. The individual IDS agent runs independently and monitors local acrtivities. It detects intrusions from local traces and initiate response. if the anomaly is detected in local data or if the evidence is inconclusive, neighboring IDS agents can cooperatively participate in global intrusion detection action.

The methods for collecting data, detection and response are independent of each other and the other IDS agents in the network.The system discussed in [5] was anomaly based and provided experimental results exploring the performance of anomaly based detection using different ad hoc routing protocols. It is worth noting that the architecture is not limited to using anomaly or signature baased intrusion detection or hybrid of both.

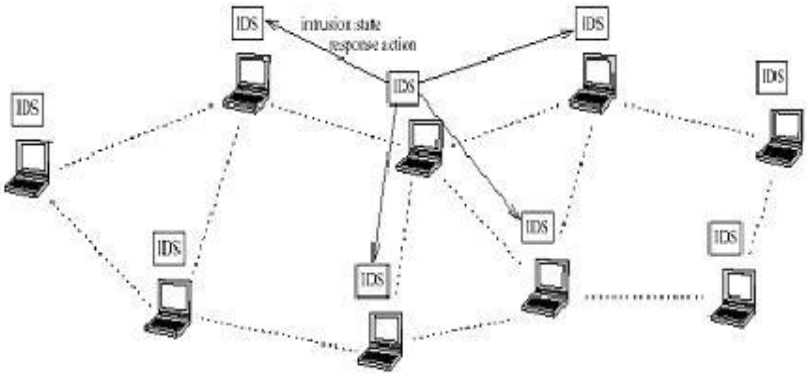

Figure 2. Distributed and cooperative IDS

5. Proposed Approach

The proposed system is based on the distributive and cooperative architecture of Zhang and Lee where an IDS agent is used by every node to detect and isolate the misbehaving nodes [5]. The structure of the IDS agent is as shown in Figure 3. Each IDS agent includes four modules. The first one is the data collection module responsible for collection of data and calculation of DTQ of each node. The second module is the intrusion detection module. It uses the information made available by the previous module and the threshold value in detecting the bad behavior of monitoring nodes. The voting module is the third module, which is responsible for detection approval, in which a node condemning another as misbehaving is required to get approval from the other nodes of the network before proceeding to isolation. The fourth module is the intrusion response module responsible for segregating the misbehaving nodes based on the outcome of the voting module.

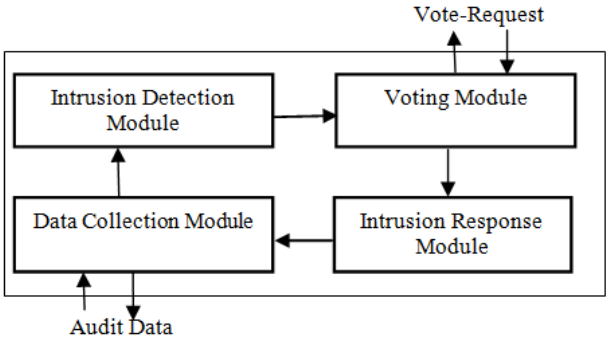

Figure 3. Structure of an IDS agent

The detailed working of each module of the IDS agent is as follows:

5.1. Data Collection Module

The main function of this module is to supervise the behavior of nodes for collecting the data. For every neighboring node that a node tries to transmit data, we measure the node quality [16]. We use a DTQ function proposed by Alam to measure a nodes quality [14]. Using the DTQ function helps the sender get information on the misbehaving and well-behaving nodes based on the acknowledgments received by the sender after forwarding the packets to other nodes. The function also helps in measuring the transmission quality of intermediate nodes. Each node maintains a DTQ table that stores the DTQ value of all the neighboring nodes in the network.

Each node in the network tries to transmit data to all its neighbors and these neighbors try to collect DTQ of the transmitting node and store the value in their respective DTQ tables. To decrease the communication overhead, which is caused due to acknowledgments and the statistical packets the concept of bunch is introduced. Every bunch is composed of a set of specified packets. The advantage of bunching is that instead of sending acknowledgment packets for each and every data packet sent, it is just enough to send one acknowledgment for each bunch. The bunches are categorized into 2 types, an enduring bunch having statistical information on the quality of forwarding of last N packets. The other is an interim bunch that includes the statistic data on recently sent M packets. M and N are so defined that N is divisible by M, Also we select N and M such that (N mod M =0). Hence it is observed that the statistics collected for M statistical bunches of (N+M) messages represent the recent

behavior of the node, whereas the historical data is given by the statistics collect for N sent messages. According to Alam et.al after collecting the data the DTQ is calculated as [14] :

$$DTQ = k \frac{D}{E} P \quad (1)$$

Where k>0 is a constant. D is the total data packets that have been transmitted successfully. E is the total energy cost of transmitting a data bunch. P is the expected probability of successful data transmission when nodes work normally under the influence of environment. STB is the stability of a node which measures how fast the transmission quality changes in a period of time.

The stability factor STB is defined as:

$$STB = \left[\frac{\sum_{i=1}^{M} \frac{d_i}{u_i}}{\sum_{j=1}^{N} \frac{d_j}{u_j}} \right]^{\alpha} \quad (2)$$

Where d_i and u_i represent the bytes successfully transmitted and the bytes attempted to be transmitted respectively. When sending the past ith data bunch, α >1; N is a positive integer giving the data sending statistics of a node, M is a positive integer such that N%M =0.

Further the STB can be represented as

$$STB = \left(\frac{\text{Total number of packets successfully transmitted in } \frac{N}{M} \text{ times}}{\text{Total number of packets attempted to be transmitted in } \frac{N}{M} \text{ times}} \right) \quad (3)$$

5.2. Intrusion Detection Module

The main function of this module is to take the information from a data collection module and detect the malicious nodes in the network. The module identifies the malicious nodes by calculating an appropriate threshold. Here the threshold value plays a key role in scrutinizing the nodes. Each node computes the threshold value and compares all the DTQ values in its DTQ table. If it finds one or some of the DTQ in the table are less than the threshold then it realizes that there may be one or more malicious node in the network. Once it detects the suspicious nodes the intrusion detection module should not condemn the detected node immediately as malicious. This is because the DTQ value may be less than threshold due to other reasons also. So the intrusion detection module sends the information to the voting module for global response to make sure from other nodes of the network that the detected nodes are really malicious.

The threshold value is calculated by using the following algorithm.

Step 1: The node calculates the average of all the DTQ's in its DTQ table.

$$avg\_dtq = \frac{\sum_{i=1}^{n} dtq_i}{n} \quad (4)$$

Where n represents the number of neighbors, dtq_i represents the DTQ value of node i.

Step 2: The threshold is calculated with the avg_dtq of all the neighbors and its own avg_dtq value.

$$sum = \sum_{i=1}^{n} avg\_dtq_i \quad (5)$$

Sum of all avg_dtq of the neighboring nodes.

$$sum_{neighbor} = \sum_{i=1}^{n} \sum_{j=1}^{k} avg\_dtq_{neighbor_j} \quad (6)$$

Where k represents the neighboring nodes of n

Finally the threshold is given as

$$Thr = \frac{avg\_sum}{n+1} \quad (7)$$

Step 3: The node compares its DTQ table values with the threshold (thr). When it finds any of the DTQ values in the table less than the threshold, it realizes that there may be one or more malicious node in the network.

5.3. Voting module

Once the voting module receives a vote request from the intrusion detection module, it immediately broadcasts the message to all the nodes in the network and ask them to vote for the request. Based on the DTQ value present for the requested node in their tables and the threshold value of the node, the node either vote for or vetoes to the request. Based on the number of positive votes or negative votes received, the node is either identified as legitimate node or malicious node.

In the process of voting, the node which initiates the voting process keeps track of the votes that it receives. In order to implement this we are considering all the nodes other than the initiating node, *i.e.*, N-1 nodes where N is the number of nodes in the network. As soon as the vote-initiator node sends the vote request, it will start a timer to receive the vote responses from the participating nodes because there may be packet losses or some nodes may not respond and we cannot wait for long periods. Here all the vote responses received after timeout are ignored. After receiving the vote responses we first check if at least 60 % of the nodes in the network have sent the response. If not it will re initiate the voting process for 3 more times.

After receiving the votes from at least 60% of the nodes the information is passed on to the Intrusion Response module.

5.4. Intrusion response Module

According to the results of voting the node X can be well-behaving node so acquit it or it may be a malicious node so penalize it. A node is decided as malicious or legitimate based upon the number of positive or negative votes received in response to the vote request in the following manner.

If 90% of the received votes are positive votes (in favor of X) then the node is identified as a good node and acquitted by updating the DTQ value of the corresponding node in the DTQ table. If the number of positive votes is < 90% but greater than 60% then send the information to the voting module to repeat voting process 2 more times. If the number of positive votes is <60 % and greater than 30%, then send information to the voting module to repeat the voting

process for 1 more time. If the number of positive votes is <30%, then it is identified that the node is malicious so dismiss it from the network by blacklisting it.

The information of blacklist node is broadcasted on the network as a result all nodes will remove the entry of the blacklisted node from their routing table and hence no communication is done from such nodes in the network.

The complete working of the four modules of IDS agent are shown as flowchart representation in Figure 4 and Figure 5.

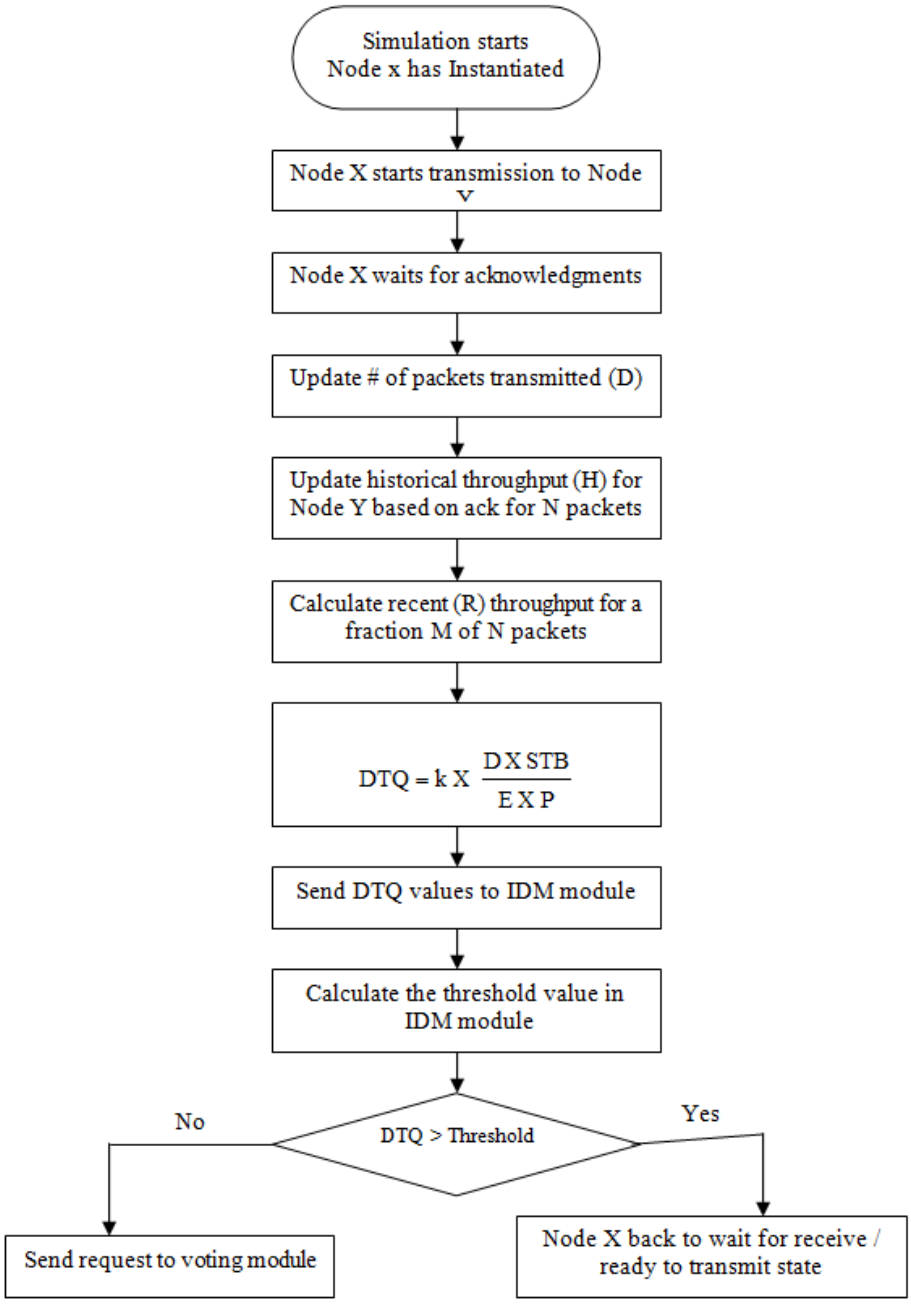

Figure 4. Working of Data Collection and Intrusion Detection Modules

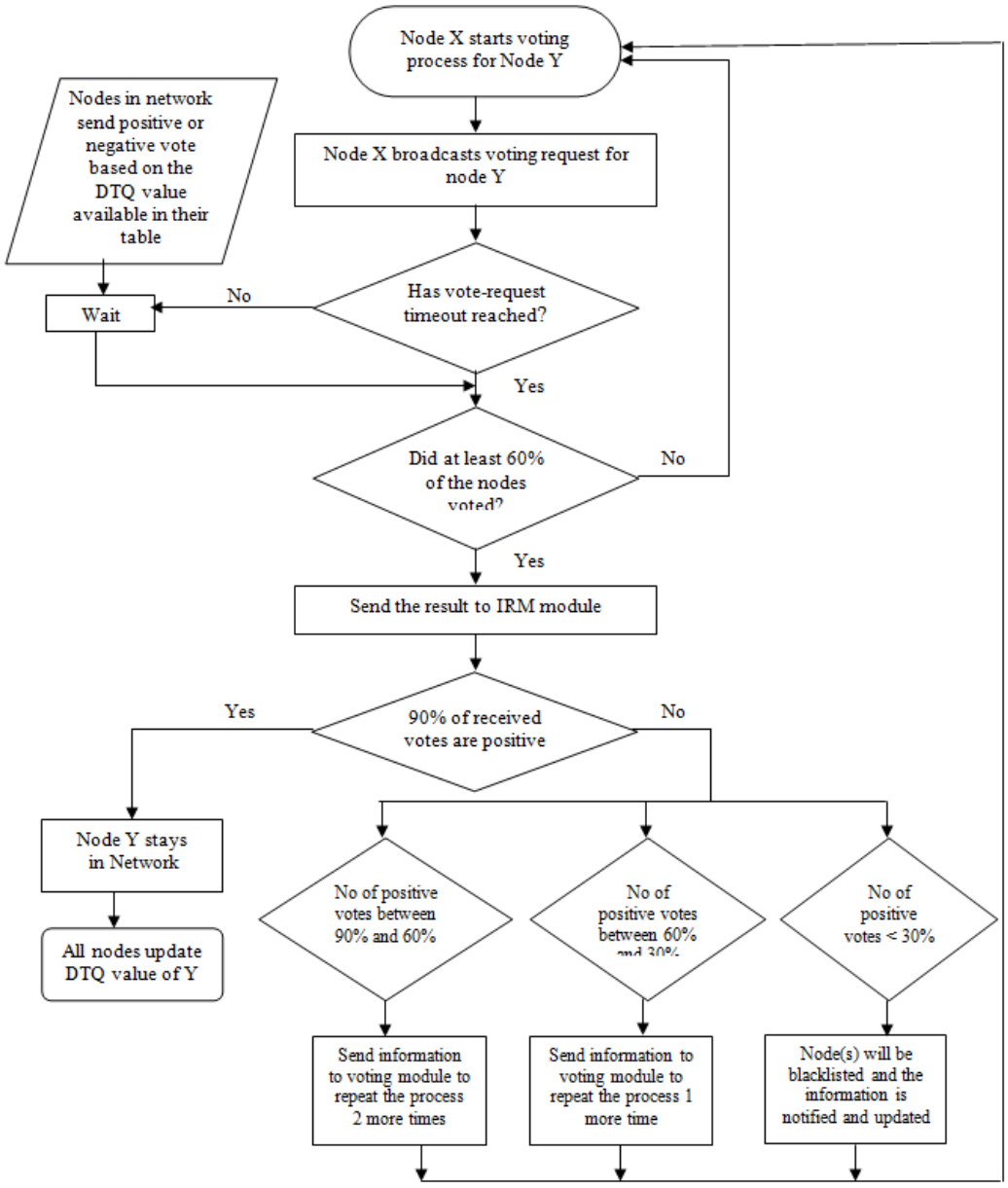

Figure 5. Working of Voting Module and Intrusion Response Module

6. Simulation Analysis

6.1 Simulation Setup

We have used the NS-2 simulator for our implementation. Mobility scenarios are generated by using the random waypoint model with 50 nodes moving in an area of 1000 x 1000m flat space. Each node independently repeats this behavior and the average degree of mobility is varied by making each node remain stationary for a period called pausetime every time before it moves to the next position. The IEEE 802.11 as the MAC layer and CBR as the traffic source is used. Simulation parameters are summarized in Table 1.

Table 1. Simulation parameters

Parameters	value
Nodes	50
Mac layer	IEEE 802.11
Traffic model	CBR
Packet size	512
Area	1000x1000
Packet Rate	4
No. of malicious nodes	3
Simulation time	200 sec

The following metrics are used to evaluate the performance of the proposed scheme.

Packet Delivery Ratio : It is defined as the ratio of the total number of data packets received from all the nodes to the number of packets sent from the sources.

Routing Overhead : The number of routing packets transmitted per data packet delivered at the destination.

6.2 Simulation Results

All the three attacks are simulated for the above metrics.The evaluation results are as shown below.

Flooding attack: Figure 6 Shows a decrease in the packet delivery ratio under the flooding attack. However , when the IDS is enabled the delivery ratio increases and is almost 48 % more than with attack.

The second evaluation metric for this attack is the normalized routing load shown in Figure 7. In AODV under attack, the routing overhead is much larger than the normal AODV because the malicious node broadcasts many packets. Our approach shows the decrease in the overhead when the IDS is incorporated.

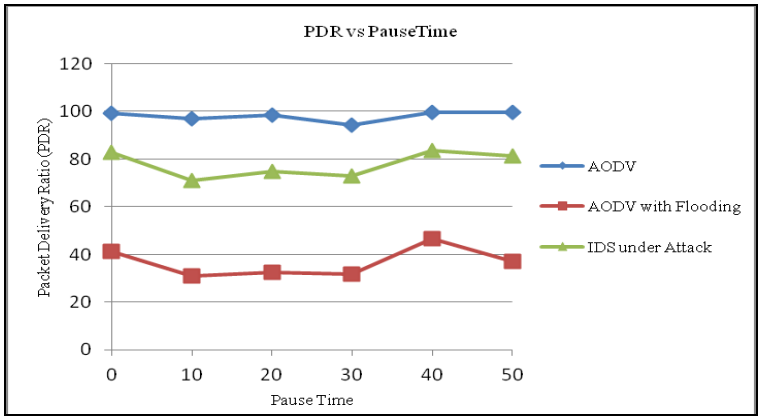

Figure 6. Packet Delivery Ratio vs PauseTime

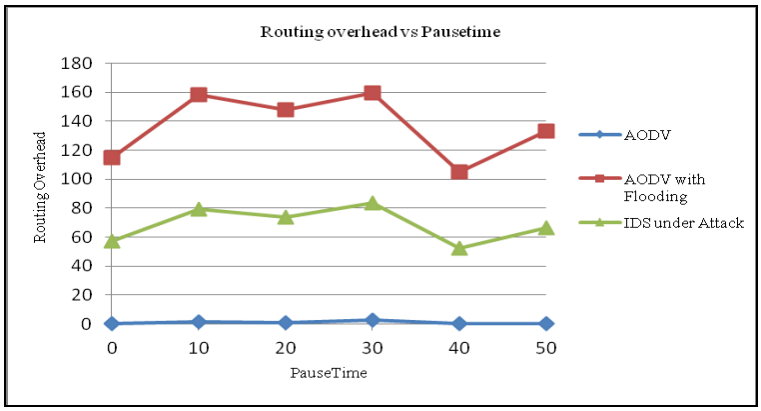

Figure 7. Routing Overhead vs PauseTime

Black hole attack: In order to evaluate the effect of IDS in black hole atatck we used the packet delivery ratio with the variable max connections and pause time. Figure 8 and Figure 9 shows that the packet delivery ratio has decreased considerably when AODV is under attack and it has increased by 50 % when the IDS is incorporated.

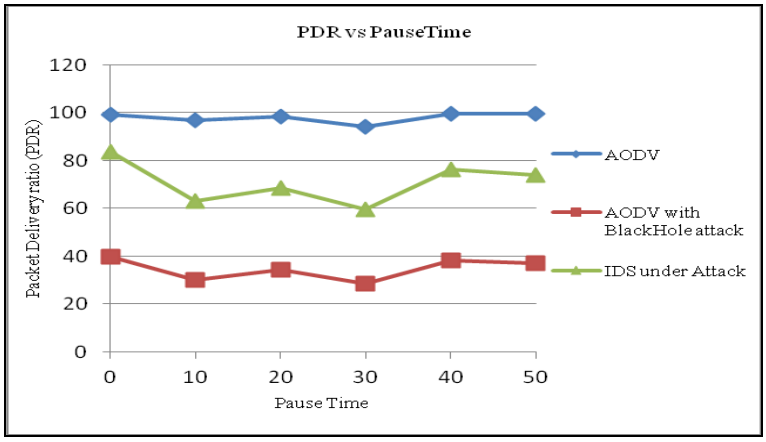

Figure 8. PacketDelivery ratio vs PauseTime

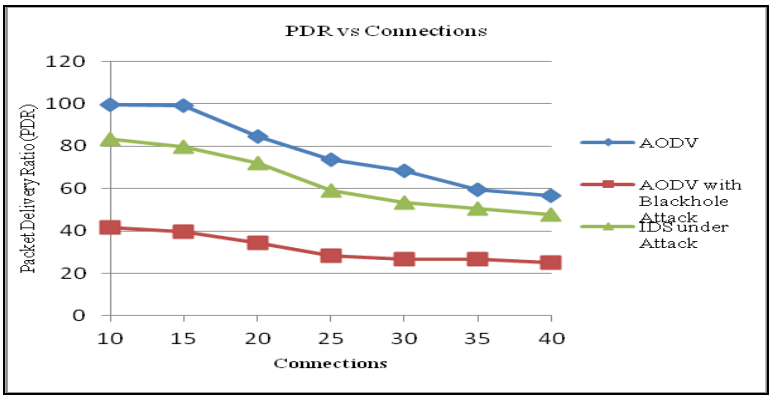

Figure 9. PacketDeliveryRatio vs No.of Connections

Grayhole attack: In order to evaluate the effect of IDS in grayhole attack, we used the packet delivery ratio with maximum number of connections and pause time. Figure 8 and Figure 9 shows that the packet delivery ratio has decreased considerably when AODV is under attack and it has increased by 55 % when the IDS is incorporated.

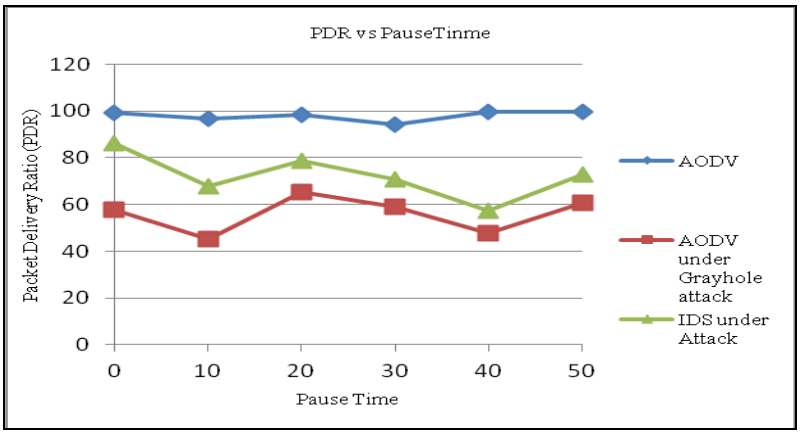

Figure 10. PacketDeliveryratio vs PauseTime

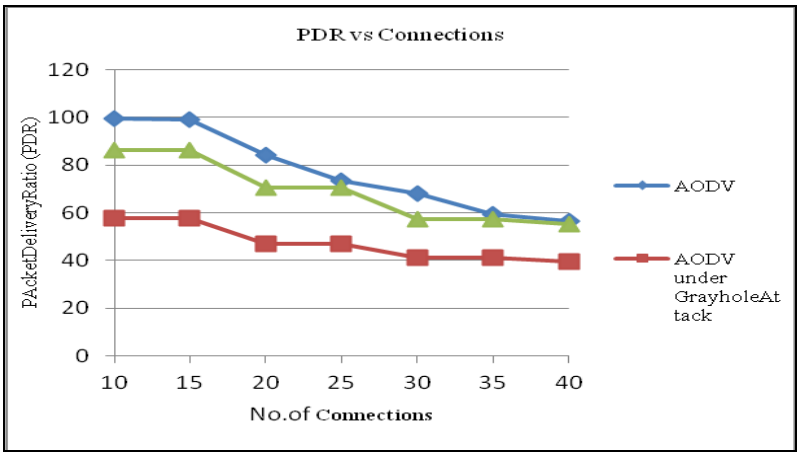

Figure 11. PacketDeliveryRatio vs No. of Connections

7. Conclusion

In this paper, we have proposed an IDS for MANETs based on the behavior of nodes to successfully identify three types of attacks like flooding attack, blackhole Attack and gray hole attack on ad hoc networks. The proposed IDS efficiently identify and eliminate the malicious nodes that causes the attacks. The solution is designed based on the data transmission quality of the nodes in the network. In the solution each node maintains a DTQ table for maintaining the DTQ values of its neighbors which help in identifying the malicious nodes. the nodes also maintain a blacklist table to maintain the information of blacklisted nodes so that no communication is done with these nodes.The simulation results show that using the proposed approach the packet delivery ratio in an adhoc network under attack has increased by 47 to 55% when compared to the packet delivery ratio under attack. To avoid falsely accusing the genuine needs of misbehavior an accusation in our approach is based on global consensus through voting. The results show that the proposed method is working

effectively for AODV and in future it can be implemented in other routing protocols also and also detect various other attacks.

References

[1] L. Zhou and Z. Haas, "Securing Ad hoc Networks", IEEE Transaction on Networks, vol. 13, no. 6, **(1999)**, pp. 24-30.
[2] H. Deng, W. Li and D. Agarwal , "Routing Security in Wireless Ad hoc Networks", IEEE Comm. Magazine, vol. 40, no. 10, **(2002)**, pp. 70-75.
[3] P. Brutch and C. Ko, "Challenges in Intrusion detection for wireless Ad hoc network", Proceedings of the Workshop on Security and Assurance in Ad hoc Networks in Orlando, **(2003)** January, pp. 368-373..
[4] Y. Zhang, W. Lee and Y. Huang, "Intrusion Detection in Wireless Ad hoc Networks", Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, **(2000)** August, pp. 275-283.
[5] S. Marti, T. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks", In proceedings of MOBICOM, **(2000)**, pp. 255-265.
[6] S. Bharagava and D. P. Agarwal, "Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks", IEEE Semi-annual Proceedings of Vehicular Technology Conference (VCT'01), **(2001)**, pp. 2143-2147, doi:10.1109/VTC.2001.957123.
[7] L. Venkatraman, "Securing Routing Protocol for Ad hoc Networks", Master's Thesis, University of Cincinnati, **(2000)** November.
[8] C. Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe and K. Levitt, "A Specification-based Intrusion Detection System for AODV", In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03), Fairfax, VA, **(2003)**, pp. 125-134.
[9] I. Stamouli, P. Argyroudis and H. Tewari, "Real Time Intrusion detection for Ad hoc Networks", Proceedings of the sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WOWMOM'05), **(2005)**, pp. 374-380.
[10] H. Yang, J. Shu, X. Meng and S. Lu, "SCAN: Self-organized Network-layer Security in Mobile Ad hoc Networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, **(2006)** February, pp. 261-273.
[11] O. F. Gonzalez, G. Ansa, M. Howarth and G. Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad hoc Networks", Journal of Internet Engineering, vol. 2, no. 1, **(2008)** June, pp. 181-192.
[12] J. B. D. Cabrera, R. K. Mehra and C. Gutirrez, "Ensemble Methods for Anomaly Detection and Distributed Intrusion Detection in Mobile Ad hoc Networks", Information Fusion Journal, vol. 9, Issue 1, **(2008)** January, pp. 96-119.
[13] T. Li, M. Song and M. Alam, "Compromised Sensor Nodes Detection: A Quantitative Approach", Proceedings of the IEEE International Conference on Distributed Computing Syatem, **(2008)**, pp. 352-357.
[14] K. Kumar, "Intrusion Detection in Mobile Ad hoc Networks", Master's Thesis, The University of Toledo **(2009)**.
[15] M. Karami, M. Rafsanjani, A. F. Navid and Y. Yavari, "QAIDS: Quantitative and Agent based Intrusion Detection System", Computer and Information Science Journal, vol 4, no. 2, **(2011)** March, pp. 64-74.
[16] S. Mamatha and A. Damodaram, "Enhanced Intrusion Detection System for Malicious Node Detection in Mobile Ad hoc Networks using Dta Transmission Quality of Nodes" Accepted for publication in IJCNIS, vol. 6, no. 10 .
[17] K. Fall and K. Vardhan, The ns Manual 2006, available from http://www.mash.cs.berkley.edu/ns.

Authors

S. Mamatha obtained her B.E in CSE from O.U in 1998 and M. Tech in CSE from JNTUH in 2004. She is pursuing Ph.D in CSE from JNTUH, Hyderabad. She is working as Associate Professor in Bhoj Reddy Engineering College for Women and has 15yrs of teaching experience. Her areas of interest include security in wired and wireless Networks. Ms. Mamatha is a life member of ISTE, India.

Avula Damodaram obtained his B.Tech degree in CSE in 1989, M.Tech in CSE in 1995 and PhD in Computer science in 2000 all from JNTUH, Hyderabad. His areas of interest are Computer Networks Software engineering, Data Mining and image Processing. He has successfully guided 8 PhD and 2 MS scholars apart from myriad M.Tech projects. He is currently guiding 9 scholars for PhD and 1 scholar for MS.

He is on the editorial board of 2 International Journals and a number of course materials. He has organized as many as 30 workshops, short term courses and other refresher and orientation programs. He has published 35 research papers in National and International Journals and also presented 45 papers at National and International conferences. On the basis of his scholarly achievements and other multifarious services, he was honored with the award of DISTINGUISHED ACADAMICIAN by Pentagram Research Center, India, in January 2010. He was also awarded as the Best Professor for the year 2013 by the government of Andhra Pradesh, India.