I.J. Computer Network and Information Security, **2014, 10, 32-39**
Published Online September 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.10.04

Enhanced Intrusion Detection System for Malicious Node Detection in Mobile Ad hoc Networks using Data Transmission Quality of Nodes

S. Mamatha
Bhoj Reddy Engineering College for Women, Hyderabad, India
Email: msathineni@yahoo.co.in

A. Damodaram
JNTU College of Engineering, Hyderabad, India
Email: damodarama@rediffmail.com

Abstract—Mobile Ad hoc NETworks (MANETs) are the new generation of networks that offer unrestricted mobility without any underlying infrastructure. It relies on the cooperation of all the participating nodes. Due to their open nature and lack of infrastructure, security for MANETS has become an intricate problem than the security in other networks. The conventional security mechanisms of protecting a wired 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 is required. Generally the malicious nodes demonstrate a different behavioral pattern of all the other normal nodes. So an Intrusion Detection System based on anomaly based intrusion detection that works by checking the behavior of the nodes was proposed. Here, in this paper to determine the behavior of the nodes as malicious or legitimate a Data Transmission Quality (DTQ) function 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 final decision of confirming nodes as malicious is determined by a group consensus method. The evaluation results show that the proposed method increases the detection rate as well as decreases the false positive rate.

Index Terms—MANET, Threshold, Intrusion Detection System, Behavioral Pattern, DTQ function.

I. Introduction

A mobile ad hoc network (MANET) is a collection of mobile devices that cooperatively communicate with one another without any pre-established infrastructure such as centralized access point. Multi-hop routing is used whenever the nodes are not in each other's radio range. To perform the multi hop routing, the nodes in the ad hoc network act as routers and pass the messages to those nodes that are not in the radio range. The ad hoc network is useful in situation where geographical or terrestrial conditions demand totally distributed network system without any fixed infrastructure. The characteristics of MANETS such as restricted battery power, node mobility and unreliable transmission medium make them enormously susceptible to a variety of attacks [1] [2]. Hence there is a need for harder security in MANETs than the traditional wired networks.

The dynamic and cooperative nature of MANETS presents a great challenge in securing these networks. The wired networks in general posses a prominent level of security at gateways and routers. The topology of an ad hoc network on the other hand keeps changing and does not have a well-defined boundary, so the network based access control mechanisms like firewalls are not directly applicable. It is exceptionally easy for a malicious node to break the entire network. The security services such as authentication and access controls can provide protection against some types of external attacks, but cannot protect against the internal attacks [3]. So the preventive mechanisms alone cannot prevent all possible attacks. Therefore, it is expected to provide other security mechanisms that can deal with the malicious nodes. Hence, to create a highly secure ad hoc network. It is required to implement an Intrusion Detection System (IDS) in the network to create the second wall of defense. The idea of intrusion detection system is to detect the intrusions as early as possible so that the MANET can be saved before any harm is done.

Kumar (2009) has proposed an Intrusion detection System for MANETs based on anomaly based intrusion detection that works by checking the behavior of the nodes [4]. The main problem of this method was that the detection was based on using a predefined threshold value which is not appropriate for a dynamic network like MANET. The other problem was that the decision of misbehavior was not done appropriately. So here in this paper an enhanced method is proposed wherein the

threshold value is calculated adaptively such that it suffices the needs of the dynamic network. The confirmation of a malicious node is also done efficiently.

In this paper a modular solution is proposed that deal with internal attacks and attempt to solve the complete problem. In the proposed IDS, a distributed and cooperative architecture is used where IDS agents run on every node and 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, an Intrusion detection module, Voting module and Intrusion Response Module. The function of IDS agent is described in brief as follows.

A. For Ensuring

Data packets are sent as a bunch and wait for acknowledgments. Based on this the DTQ of node is calculated which is the main criteria in the detection of the behavior of the nodes.

B. For condemnation

The threshold value is calculated and is used for checking the behavior of nodes. Each node evaluates the behavior of its neighbor and compares it with the calculated threshold. Once a node detects any other node as misbehaving, it will proceed to its segregation agreeably with others.

C. For condemnation and segregation

A social-based approach is offered to endorse detection and segregation of misbehaving nodes. The main aim of this approach is to decrease the false positives caused by channel conditions and node mobility. That is, each node monitors and evaluates the behavior of its successor and as soon as it detects a node as misbehaving, it launches a procedure to endorse the detection and collaboratively segregate the node from the network.

All these approaches are structured around the four modules of the IDS agent which we will exemplify in detail later. The proposed solution allows detecting and segregating misbehaving nodes that drop data packets in many cases. The detection process is inexorably slower as it prevents false detections in case of packet collisions and node mobility which cause inadvertent packet loss. The segregation is global, where once the node is approved as malicious by all the nodes of the network it is isolated from the network. As the misbehaving node is isolated based on social–based approach, the problem of misbehaving node rejoining at any other place of the network is overcome in the solution. However the process of reintegration of isolated nodes, if required, is not considered in the proposed method.

The rest of the paper is organized as follows: Section II specifies the related work done. Section III specifies the assumptions, in section IV the proposed approach is described in detail. Section V summarizes the simulation results and discusses the performance measurement and evaluation of our scheme. Section VI presents the conclusion and future work.

II. 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.

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. Zhang and Lee have proposed an intrusion detection technique for wireless ad hoc network that used cooperative statistical anomaly detection technique [6]. 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. 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. 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 [8]. 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.

To detect attacks on AODV a solution based on specification-based intrusion detection was proposed [9]. This approach uses a finite state machine for specifying correct AODV routing behavior and a distributed network monitor for detecting runtime violations of 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 [10]. This method uses a timed 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 [11]. 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 [12]. 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 [13]. 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 [14]. 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 [4]. 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 was 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 at 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 this paper, a new enhanced IDS for MANETs is proposed based on the one proposed by Kumar [4]. To check the behavior of nodes he has used a DTQ function and predefined threshold. But as the MANETS are dynamic and irregular the use of predefined threshold in the detection of malicious nodes does not give correct results.We have enhanced the performance of this system by calculating the threshold adaptively such that it meets the requirements of the dynamic nature of MANETs and hence reduces false positives and also increase the detection rate.

III. Assumptions

Our solution operates with the following assumptions on ad hoc network:

- Bidirectional communication links are present between each pair of nodes, facilitating communication in two directions.
- Nodes are mobile and links are not always steady, i.e. packet collisions and losses are possible.
- Nodes are in the direct transmission range of another node.
- Nodes in the network are adapted with wireless interfaces to support promiscuous mode.
- We assume that normal and abnormal behaviors have distinct symptoms, also the local IDS agents are secure.
- A misbehaving node is represented by a given drop in the transmission quality of the node which is checked from the DTQ value calculated.

IV. Proposed Approach

The proposed system is based on the distributive and cooperative architecture of Zhang and Lee where every node has an IDS agent running on it to detect and isolate the misbehaving nodes [6]. The structure of the IDS agent is as shown in Fig. 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 which is responsible for detecting the bad behavior of monitoring nodes by using the information made available by the previous module and the threshold value calculated adaptively. 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 which is used for segregating the misbehaving nodes based on the outcome of the voting module. Segregating a misbehaving node means: i) do not route packets through it, to avoid losing them and ii) do not forward packets for it, to castigate it. Now we introduce our solution by presenting these modules and interactions between them.

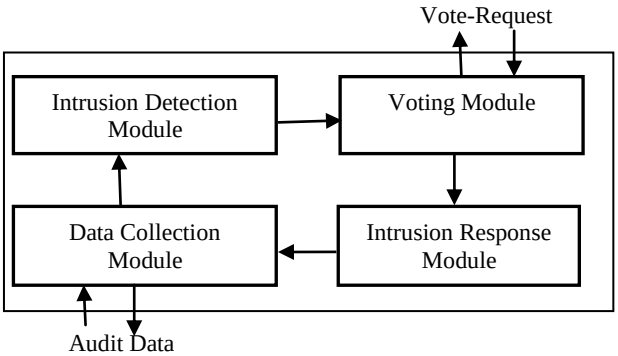

Fig. 1 Structure of an IDS agent

The working of our IDS agent to handle all internal attacks is as shown in the flowchart Fig. 2.

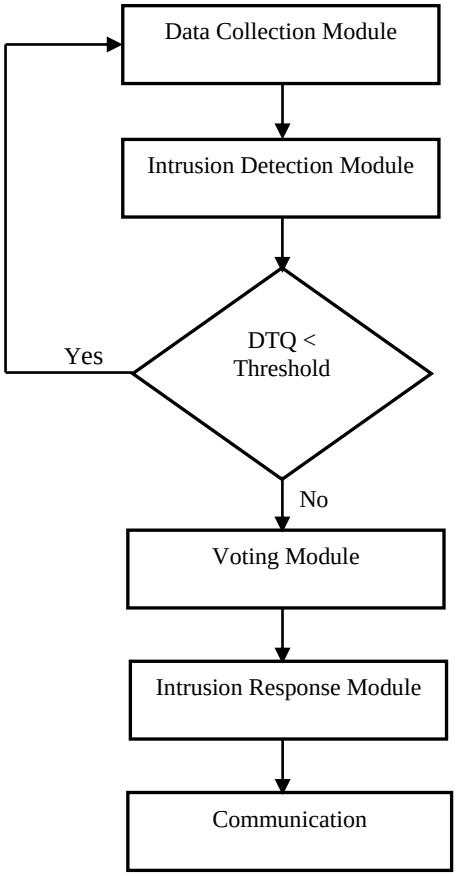

Fig. 2 Flowchart representation of working of an IDS agent

Now we see in detail the working of each module of the IDS agent.

A. Data Collection Module

The main function of this module is to supervise the behaviors 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]:

$$DTQ = k\ X\ \frac{D\ X\ STB}{E\ X\ P} \tag{1}$$

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:

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

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

$$STB = \left(\frac{\text{Total ACKed messages for the last } \frac{N}{M} \text{ messages}}{\text{Total ACKed messages for the last N messages}} \right)^{\alpha} \tag{3}$$

Working of data collection module is given as follows:

- Let node X transmit to node Y
- Node X waits for the acknowledgment
- Update the number of data packets transmitted (D)
- Calculate the recent throughput (R) for fraction M of N packets.
- Calculate the total throughput (H) based on acknowledgments of N packets.
- Calculate the $STB = \left(\frac{R}{H}\right)^{\propto}$ where $\propto$ is a step power function
- Calculate $DTQ = k \times \frac{D \times STB}{E \times P}$
- Store the value of DTQ in the DTQ table.

B. 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.

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

Sum of all avg_dtq of the neighboring nodes.

$$sum\_dtq = \sum_{i=1}^{n} \left[avg\_dtq_i + \sum_{j=1}^{k} avg\_dtq_j \right] \quad (6)$$

Where k represents the neighboring nodes of n
Finally the threshold is given as

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

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.

The working of the intrusion detection module is given as follows:

- Calculate the threshold.
- Compare DTQ with threshold.
- If DTQ< threshold then send a voting request to voting module for confirming the node as malicious or not.

C. 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 reinitiate 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.

The working of the voting module is given as follows:

- Let node Y broadcast the voting request for node X in the network
- All the nodes check their DTQ table for the DTQ value of node X
- Nodes reply to the voting request based on the value in their DTQ tables.
- Wait till vote request timeout.
- Check whether at least 60% nodes sent the response.
- If at least 60% nodes sent response then pass the information to IRM module.
- Otherwise repeat the process of voting for 3 more times.

D. 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 working of the IRM module is given as follows:

- Check the number of positive and negative votes.
- If 90% of the received votes are positive votes then the node is identified as a good node and acquits it.
- If the number of positive votes is between 90% and 60% then send the information to voting module for repeating the process 2 more times.
- If the number of positive votes is between 60% and 30% then send information to voting module for repeating the process for 1 more time.
- If the number of positive votes is <30% then node is identified as malicious so dismiss it from the network by blacklisting it.

V. Simulation Analysis

Here we have used the NS2 simulator for our implementation [17]. The simulation is done on a 1000X1000 flat space with 100 wireless nodes scattered. We have used the random waypoint mobility model, where the nodes move from a random starting point to random destination with a speed uniformly distributed between 0-20 m/Sec. The MAC layer protocol used is 802.11 and the transport protocol used is UDP (User Datagram Protocol). The traffic sources used are CBR (Constant Bit Rate) with a data packet of 512 bytes long and the rate of packet generation is 4 packets/sec. The number of connections used is 40 and the simulation is done for a period of 900 sec.

In the first step we have compared the detection rate and false positive rate of the proposed method with that of Kumar [4] method. In Fig. 3, it is observed that the detection rate has increased in the proposed system when compared to the existing system. It is also observed that as the number of malicious nodes increases to 50 the detection rate of the proposed method was 89%, whereas the existing method, it is only 85% and when the malicious nodes are 60 the detection rate of the proposed method was 85% and existing method was 76%. In Fig. 4 it is observed that the false positive rate of the proposed method has decreased considerably when compared to the existing method. Thus the simulation results show that the method proposed gives good results compared to the existing method.

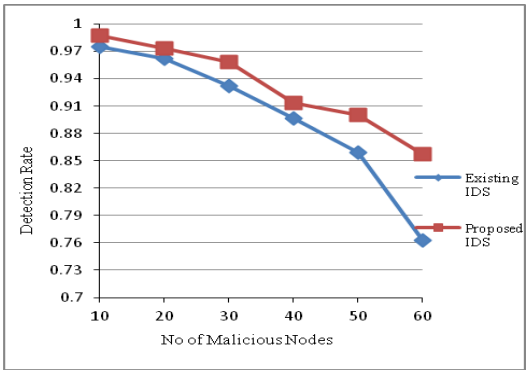

Fig. 3 Detection rate vs Malicious Nodes

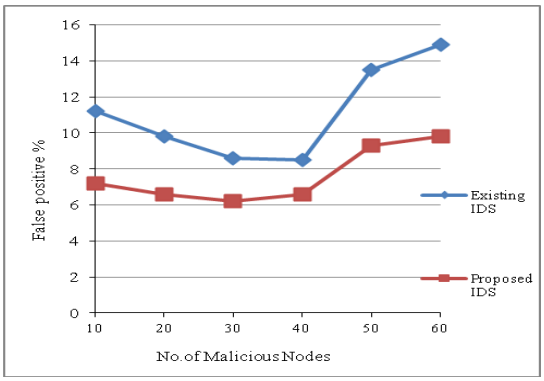

Fig. 4 False Positives vs No of Malicious nodes

In the second step we have performed the simulations for the given metrics with malicious nodes created in the network and AODV protocol integrated with our IDS.

The performance of the metrics was checked by simulating 50 nodes with a maximum of 40 connections and by varying speeds from 0-20m/Sec for a simulation time of 900 Sec.

We have considered the following performance metrics for the evaluation of the proposed method.

1. **Packet Delivery Ratio:** It is the ratio of number of CBR packets received to that transmitted.
2. **Throughput:** The number of packets correctly received over the simulation time.
3. **Total Network Overhead:** It is the sum of the overhead produced by the various other packets in the network.

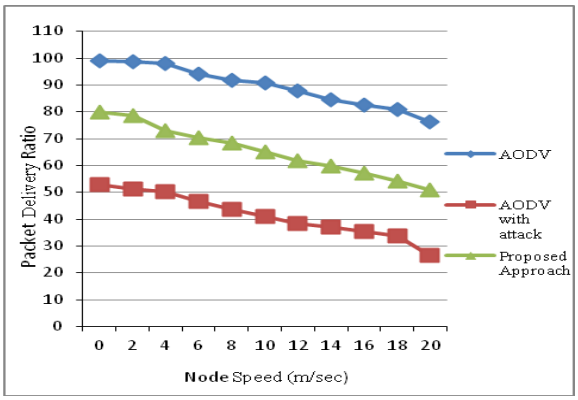

Fig. 5 Packet delivery ratio vs Node Speed

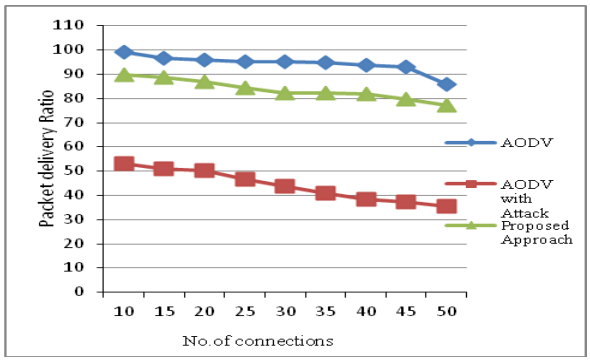

Fig. 6 Packet delivery ratio vs number of connections

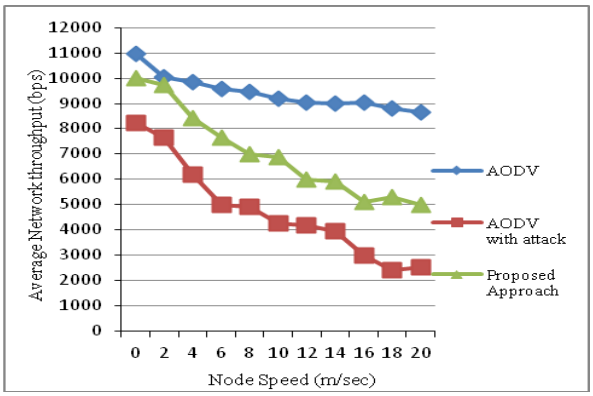

Fig. 7 Average network throughput vs node speed

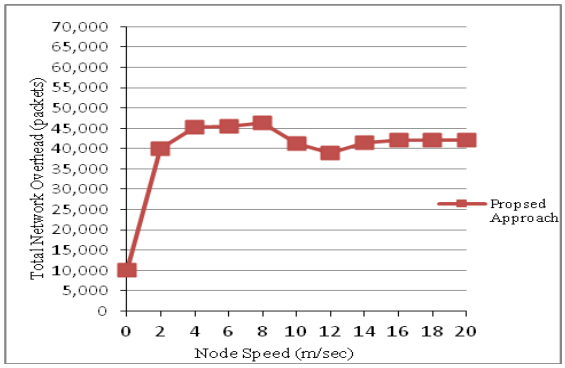

Fig. 8 Total Network overhead vs Node Speed

Evaluation of Results

Packet delivery ratio: The Fig. 5 shows that the packet delivery ratio of the network with respect to the node speed. It has been observed that the packet delivery ratio has decreased, when the malicious nodes are present. After implementing the proposed IDS the packet delivery ratio has considerably increased because the malicious nodes are identified and isolated from the network. The graph also shows that as the node speed increases the ratio decreases due to movement of nodes. In Fig. 6 the graph shows the packet delivery ratio of the network with respect to the number of connections at a node speed of 10 m/s. Here also we can observe that the packet delivery ratio increases with the proposed IDS when the malicious nodes are present.

Throughput: The Fig. 7 shows the improvement our approach has brought to the network with respect to the throughput. Our graph present results for network without misbehaving nodes, network with misbehaving nodes and network with our approach to deny access to misbehaving nodes. Results are displayed for network containing 50 nodes with 40 connections and varying node speed.

Total Network Overhead: The graph in Fig. 8 shows that the network overhead is least when nodes are stationary and increases with node speed. The overhead generated by our approach is higher in dynamic networks because a node has greater probability to become in contact with more nodes and hence more behavior checking tasks are scheduled.

VI. Conclusion

In this paper, we have proposed enhanced IDS for MANETs with respect to the one given by Kumar [4]. In our proposed method we have calculated the threshold adaptively such that it meets the dynamic nature of MANETs. The simulation results show that using our proposed method we could achieve a high detection rate even when the number of malicious nodes has increased when compared to the existing system. It is also observed that the false positive ratio of the proposed method has decreased considerably when compared to the existing method. We have shown that we can detect nodes that misbehave by dropping data packets. Detection is successful in spite of inherent packet losses in MANETs

caused by noisy links, mobility, etc. 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] Paul Brutch and Calvin Ko," Challenges in Intrusion detection for wireless Ad hoc network",Proceedings of the Workshop on Security and Assurance in Ad hoc Networks in Orlando, Jan 2003, pp. 368-373.

[4] Kumar K, "Intrusion Detection in Mobile Ad hoc Networks", Master's Thesis, The University of Toledo 2009.

[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] 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, August 2000, pp. 275-283.

[7] Lakshmi Venkatraman, "Securing Routing Protocol for Ad hoc Networks", Master's Thesis, University of Cincinnati, November 2000.

[8] S. Bharagava, 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".

[9] CY Tseng, P Balasubramanyam, C Ko, R Limprasittiporn, J Rowe, 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.

[10] I. Stamouli, Patroklos Argyroudis and Hitesh 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.

[11] 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, vol24, No 2, Feb 2006, pp. 261-273.

[12] Oscar F. Gonzalez, Godwin Ansa, Michael Howarth and George Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad hoc Networks", Journal of Internet Engineering vol. 2, No 1, June 2008, pp.181-192.

[13] Joo B. D. Cabrera, Raman K. Mehra and Carlos Gutirrez, "Ensemble Methods for Anomaly Detection and Distributed Intrusion Detection in Mobile Ad hoc Networks", Information Fusion Journal, Vol. 9, Issue 1, Jan 2008, pp. 96-119.

[14] Li.T, Song M and Alam M, "Compromised Sensor Nodes Detection: A Quantitative Approach", Proceedings of the IEEE International Conference on Distributed Computing Syatem.2008, pp. 352-357.

[15] M. Karami, Rafsanjani M, A. Fathi Navid, Y Yavari, "QAIDS: Quantitative and Agent based Intrusion Detection System", Computer and Information Science Journal, Vol 4, No 2, March 2011, pp. 64-74.

[16] S. Mamatha and A. Damodaram, "Quantitative Behavior Based Intrusion Detection System for MANETS", International Journal of Advances in Computer Networks and its Security, Vol 3,issue 2, June 2013, pp. 72-76.

[17] Kevin Fall and Kannan Vardhan, The ns Manual 2006, Available from http://www.mash.cs.berkley.edu/ns

Authors' Profiles

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.

How to cite this paper: S. Mamatha, A. Damodaram,"Enhanced Intrusion Detection System for Malicious Node Detection in Mobile Ad hoc Networks using Data Transmission Quality of Nodes", IJCNIS, vol.6, no.10, pp.32-39, 2014. DOI: 10.5815/ijcnis.2014.10.04

