International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 31983-31998
© Research India Publications
http://www.ripublication.com

Multicast Route Stability based Intrusion Detection System for MANET

[1]S.Gopinath and [2]Dr.N.Nagarajan

[1]Research Scholar, Anna University, Chennai
[2] Principal, Department of ECE,
Coimbatore Institute of Engineering and Technology, Coimbatore
[1]gopi.vasudev@gmail.com and [2]swekalnag@gmail.com

Abstract:

In recent years Mobile Ad hoc Network (MANET) has become a very familiar network for providing communication without need of access point. It is a smart technology widely used in both domestic and commercial applications. Due to flexibility nature, several security attacks are introduced. Intrusion detection system is a major technique in ad hoc networks for monitoring node activities and identifies misbehaving activities. In this research, we develop Multicast Route Stability based Intrusion Detection System (MRSIDS) for identifying misbehaving nodes in the network. The proposed system comprises three phases. In initial phase, the reliable backbone multicast routing is used to identify the reliable links as well as nodes. In middle phase, the stability of link is derived to improve the network connectivity and to achieve overhead reduction. In end phase, the intrusion detection system is deployed to identify the malicious behaviors depends on trust threshold vector value. Network Simulator (NS 2.34) tool is used for simulating the proposed system. Compared to our previous work and the existing schemes, the proposed system achieves better performances in terms of false positive rate, detection efficiency, link stability rate, detection time and communication overhead.

Keywords- MANET, Multicast routing, link stability, Intrusion detection system, detection time, detection efficiency, Communication overhead and false positive rate.

1. INTRODUCTION

A. Intrusion Detection System in MANET

Due to flexibility nature of MANET environment, cooperativeness of mobile nodes introduces new security risks. To identify the risks, there is need of Intrusion Detection System (IDS). Multicast routing protocols deliver the data from source to many destinations organized in a multicast group community. A major issue and challenge in a network is to ensure the heftiness to path failures and resilience to the malicious attackers. Multicasting can efficiently support IDS to detect intruders inside the network. To ensure the robustness and resilience to these failures and attackers, there is a need of optimized multicast routing protocol in MANET.

Intrusion Prevention System and Intrusion Detection System technologies were studied and examined how to properly use classification methods in intrusion detection for MANETs [1, 2]. The information data sets include various conditions like various attack types, various levels of network mobility and malicious activity and finally different data collection intervals for the intrusion detection system. The major requirement of tracking, identifying network attacks was identified to detect misbehavior through logs of IDS systems and prevent an action through IPS systems.

B. Design Issues of Intrusion Detection System in MANET

The characteristics of MANET make conventional IDS useless and incompetent for the new environment. Consequently, researchers have been working on developing new IDS for MANETs. The following design issues of IDS have been taken into an account.

Lack of Entry Points

MANETs does not have any routes and gateways etc. Since wireless ad hoc networks are cooperative and distributed network, IDS also need to be distributed and cooperative. Distribution of IDS agents is difficult where the resources are very limited. Gathering and distributing attack signatures are not suited to the ad hoc environment.

Mobility

Since the mobile nodes move randomly inside and outside the network, it leads to network topology changes. Mobility effect causes network partition which makes IDS unreliable.

Wireless Links

Link breakages are common in the ad hoc environment. IDS agents need to communicate with other agents to find the awareness of wireless links. Heavy IDS traffic causes congestion and more communication delay. Sometimes, IDS agents may become disconnected due to link unavailability.

Limited Resources

Due to limited resources like bandwidth, battery power and node capacity, it may prevent the IDS processing a significant number of alerts.

Lack of Secure Communication

Cryptography and authentication are difficult tasks in wireless environments which makes IDS ineffective by sending false alerts. IDS communication can also be suppressed by blocking and jamming communications on the network.

Distributive and Cooperative nature

MANET routing protocols are highly directly distributive and cooperative. It can make protocols the goal of attacks. For an example, node can pose as intermediate node in decision mechanism which affects the significant parts of the network.

2. RELATED WORK

Enhanced Adaptive Acknowledgement [3] was introduced for defending against malicious attacks and to achieve network reliability. It does not affect network performance. In this work, the author does not focus on stability based link to forward the packets. Neighbor recommendation is necessary to obtain the number of misbehaving nodes in the network. A new intrusion-detection system named Reinforce Adaptive ACKnowledgment (RAACK) [4] was developed and specially designed for detecting malicious nodes despite the existence of false misbehavior report. It was focused on false positive report and network division. But there was no stable routing is deployed for intrusion detection. In [5], the author proposed accurate and lightweight intrusion detection framework for vehicular networks to handle mobility and topology characteristics. In this framework, an effective secured clustering algorithm was developed based on node's mobility during cluster formation and clusters with high stability. A new intrusion detection system based on K-nearest neighbor classification algorithm was introduced [6] in wireless sensor network. The system isolated the misbehaving nodes from genuine nodes by observing their abnormal behaviors, and parameter selection. Here data mining technology was used for detecting flooding attack. In [7], a new approach to intrusion detection using Artificial Neural Networks (FNN) and fuzzy clustering was proposed to enhance the detection precision for low-frequent attacks and detection stability. Three steps were adopted. In first stage, a fuzzy clustering technique was used to produce the different training subsets. Various ANNs are trained in the second stage. In the third stage, errors are eliminated. The combination of distributed and cooperative scheme [8] was adopted to detect malicious nodes with the help of the mobile agent. Buffer level, Time To Live (TTL) and key are assigned by mobile agents. Packets are transmitted from source to destination node via neighbor nodes. Mobile agents are used to monitor neighbor nodes by means of routing table. If any one of the nodes not achieved predefined time and not cleared the buffer level, it was reported as misbehavior node based on key and negative acknowledgement intimation. In [9], the signature-based multi-layer IDS using mobile agents was discussed. This intrusion detection system used the mobile agents to transfer rule based signatures from large database to small database and to update with newly detected signatures. A modular intrusion detection system was introduced [10] that dealt with internal attacks and attempts to solve the complete problem. To identify and isolate misbehaving nodes, a distributed and cooperative architecture was developed with IDS agents. Each IDS agent includes packet receiving system, misbehaving detection system, voting system and Intrusion Response module. The major work of agent is to send data as a whole and wait for acknowledgments. The behavior of its neighbor node was evaluated by each node and compared it with the calculated threshold. Based on the result, the malicious nodes are detected. A Cognitive Radio Networks based on IEEE wireless regional area network (WRAN) and some of the security threats was described [11]. Effective Intrusion Detection System was developed to detect intrusion whether they are being attacked. This system used non-parametric cumulative to discover the abnormal behavior due to attacks. An anomaly detection approach and it profiles was adopted with the cognitive radio networks parameters through a learning phase. The concept of threshold mechanism [12] was concluded applying on packet drop metrics to calculate maliciousness using fuzzy logic. The solution for the black hole (BH) and gray hole was discussed. Farzaneh et.al [13] proposed adaptive anomaly detection system to update, online adaptation, tangible improvement in accuracy compared with non-adaptive methods and almost online adaptation. It consists of a number of fuzzy rules that each one has a prediction confidence ratio. Test records are classified by using this model. The test classification results and parameters were used for updating the detection model. In this approach [14], a cluster head was assumed to not to be malicious or selfish node. It can detect external intrusion in its cluster with enough resource and honest behavior. Trust relationship was built between nodes and trust value was estimated for each node to prevent internal intrusion. Cluster head election was by using trust value and the threshold value was found for notifying the malicious node to launch its IDS once the probability of attack exceeds that value. Bayesian game was applied in this IDS. In [15], the author proposed RIDM-Robust Intrusion Detection Mechanism for increases the performance of EAACK through Energy based Geographic Routing Protocol. The Routing Overhead caused by acknowledgement packets was reduced in EAACK through Batch Processing. In [16], the Digital Signature Algorithm approach was used to avoid network overhead by using limited bits for key generation. It is quite efficient to defense the security attacks along with low power consumption. In [17], the system used the noble solution and identified the attack using the fuzzy logic technique. It also contains Intrusion Prevention System which gets input from fuzzy technique and provides the secure packet transmission over the network. It also monitored for the traffic of black hole and gray hole attacks. A log signature-based Intrusion Detector [18] was dedicated to ad hoc routing protocols. In this case traffic is not focused with the majority of other IDSs. The permanent strain of energy, bandwidth and computational power with traffic sniffing and analyzing was determined. The system used the audit logs to detect the evidence of intrusion attempts. In [19], an Intrusion Detection System was used to detect intrusion in a MANET with the help of threshold values, fuzzy logic and intuitionistic fuzzy. It was dealt with different aspects such as the relative significance of symptoms, the varied symptom patterns of different attack stages. Here, the symptoms attack connection comprises one source of ambiguity and insecurity in the detecting process. In our previous work [20], optimized multicast routing scheme has been introduced to attain more network stability. In this work, the estimation of link stability, path stability and node stability is determined to provide more network stability. The trustable network was formed based on stability model. In paper [21], energy based multicast routing protocol is proposed to increase packet forwarding with more residual energy. Our aim is to arrive at a multicast protocol which strikes a balance between defending against malicious nodes and link stability.

3. IMPLEMENTATION OF PROPOSED INTRUSION DETECTION SYSTEM

The multicast route stability based intrusion detection system consists of three phases i.e. reliable multicast route construction, Link stability determination and Intrusion detection system.

3.1 Reliable Multicast Routing

The creation of optimized multicast backbone is shown in Fig.1. Reliable multicast route establishment is initiated based on two assumptions,

(i) establishing a trustable loop that should be located at 4/6 th of an average radius from the centroid so as to be reached by all the nodes with least hop distance whether they are either towards the centroid or towards the boundary nodes on the convex hull.

(ii) The network is formed by connecting links formed by trustable factors of reliability factor, packet arrival rate, packet sending rate, packet forwarding rate and link stability.

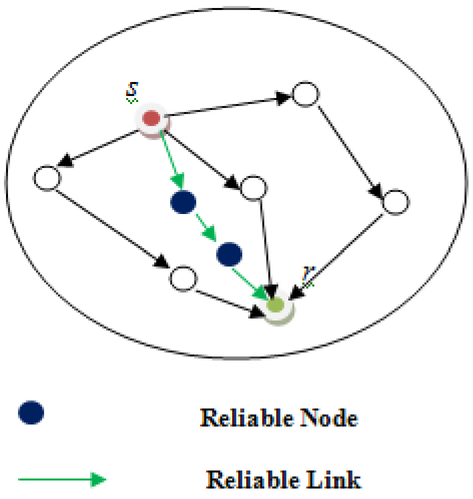

Fig.1. Reliable Multicast Route Establishment

3.2 Stability Calculation

The link connectivity is mainly getting affected by the radio channel characteristics when both nodes are fixed or move at a fairly low speed. The probability of incorrect reception of a packet is generally indicated by the error probability, which is independent of whether the previous packet has been received successfully. Let t_f denote the present time, the link stability probability is evaluated when the link remains connected for time τ,

$$p_{remain}(\tau) = P\{\eta_{10} > \tau\} = e^{-\mu(t_f)\tau} \quad (1)$$

The probability that the link recovers within time τ after a link failure,

$$p_{re\,cov\,er}(\tau) = P\{\eta_{01} \le \tau\} = 1 - e^{-\mu(t_f)\tau} \quad (2)$$

p_{remain} (τ) is generally more significant than $p_{recover}$ (τ), since the probability of the link remains connected for a given time τ can be used to estimate how long the link is connected. Generally in ad-hoc networks, especially when hidden terminals are present, collisions are likely to occur which may result in a temporal packets loss. Consider all mobile nodes have the same magnitude of velocity with only their directions being different. Link Expiration Time is determined on each link on the path, it becomes clear that the Path Expiration Time (PET) would correspond to the minimum LET on a path. i.e.

PET(PQR) = min{LETPQ, LETQR} and *PET(PQRS) = min{LETPQ, LETQR, LETRS}.*

Based on link stability, the overhead reduction can be achieved as following steps:

1. Step 1: The source node broadcasts a route request (RREQ) to all nodes within range. The receiving node first checks whether the current request packet contains correct sequence number and is not duplicated.
2. Step 2: If it is, it will then check whether it can provide the requested data, or whether it has knowledge of a path that can provide this requested data. If it does, it will produce a *route reply* (RREP), else it will add its own address and sequence number to the request packet and rebroadcast the packet.
3. Step3: A new route discovery is always initiated prior to the link being expired. This happens at a time *t* before the estimated link expiration time.
4. Step 4: Set a maximum lifetime (i.e. threshold value 100ms) for packets that minimizes broadcasting. The lifetime of packet ensures that rebroadcasting of packets ceases after certain number of rebroadcasts by hop count.
5. Step 5: The possibility of having broadcast storms and the limited resources is reduced during route discovery based on link stability.
6. Step 6: By reducing control traffic, more data traffic can be transmitted over the network.

3.3 Intrusion Detection System

The subject determines the trust values of objects according to both straight and circuitous trust values. Assume the node *k* is subject, which not only makes straight assessment of object l, but also makes circuitous estimation of object l through nodes

k_1, k_2 and k_3. It is assumed that node k makes trust estimation for node l and adopted acknowledgement mechanism. In this case, trust threshold value is maintained to find the malicious node. If any node falls below the trust threshold value, it is considered as misbehaving node. The trust threshold value combines the value of packet arrival rate, packet sending rate, packet forwarding rate, reliability factor and node proposal. The determination of the above packets is given below.

Step 1:

The packet arrival rate can be calculated as ratio of common ACK packets sent to total data packets. According to the change of the rate, it is known whether node k has response counterfeit behavior. If the change maintains in the interval $(-\zeta_1, \zeta_2)$ in various periods, node k works usually. The packet arrival rate ($PAR_{kl}(\tau)$ represents the number of received packets,

$$PAR_{k,l}(\tau) = \frac{PA_{k,l}(\tau) - PA_{k,l}(\tau - 1)}{PA_{k,l}(\tau) + PA_{k,l}(\tau - 1)} \tag{3}$$

Step 2:

Let consider that *k* sends packets to *l* who is beyond the communication region of node *k*. If node *k* is not able to monitor the successfully sent packets rate of *l* directly in this situation, node a can monitor the number of the same packets sent by node *k*. It's known that every packet sent by nodes contains a time stamp and can be distinguished efficiently even if the packets have the same content. It is obtained the sending number of a certain packet according to different time stamps. ($PS_{k,l}(\tau)$ is the requiring number of sent packets, $PR_{k,l}(\tau)$ is the repeating number of sent packets. The equation as follows,

$$PSR_{k,l}(\tau) = \frac{PS_{k,l}(\tau)}{PS_{k,l}(\tau) + PR_{k,l}(\tau)} \tag{4}$$

Step 3:

If node *k* is beyond the communication range of node *l* and it cannot monitor the received packets number of node *k* directly. It is required to collect the feedback information of node *k* to obtain the number of received packets. In order to differentiate the forwarding packets and the stayed packets, an UPDATE packet which contains a special bit is constructed. If any node *k* receives a forwarding packet, it transmits an UPDATE packet. After that, node *l* can collect these UPDATE packets of node *k* to obtain the number of forwarding packets. According to the packet forwarding change rate of $PFR_{k,l}(\tau)$, the active and passive attack can be easily avoided. It is given as,

$$PFR_{k,l}(\tau) = \frac{PF_{k,l}(\tau) - PF_{k,l}(\tau - 1)}{PF_{k,l}(\tau) + PF_{k,l}(\tau - 1)} \tag{5}$$

Step 4:
The reliability factor is introduced to prevent misbehaving nodes from modifying primary data packets. Node *k* acquires a packet transmitted by *l* randomly and makes the comparison with its packet. If the node of this packet is in the same area of node *k* and the diversity rate maintains in the interval $(-\zeta_1, \zeta_2)$, the number of accordant packets increases. If the source node does not belong to the area of node *k*, the reliability factor between node *k* and node *l* would not be adopted. $AP_{k,\, l}(\tau)$ is the number of accordant packets, $IP_{k,\, l}(\tau)$ is the incompatible packets. The Reliability factor ($RF_{k,\, l}(\tau)$) is as follows,

$$RF_{k,l}(\tau) = \frac{AP_{k,l}(\tau)}{IP_{k,l}(\tau) + AP_{k,l}(\tau)} \qquad (6)$$

Step 5:
The node proposal is given by R_l^k which is node *k*'s evaluation to node *l* by collecting proposals,

$$R_l^k = \frac{\sum_{v\in\gamma} V|k \rightarrow l| * V|l \rightarrow m|}{V|k \rightarrow l|} \qquad (7)$$

γ is a group of recommenders.
$V|k \rightarrow l|$ is trust vector of node *k* to *l*.
$V|l \rightarrow m|$ is trust vector of node *l* to *m*.

Step 6:
Probability of packet delivery is given as,

$$P_l^k = (1-p_{k,\, l}) * (1-p_{l,\, k}) \qquad (8)$$

$p_{k,\, l}$ is packet loss probability from node *k* to node *l*, while, $p_{l,\, k}$ is packet loss probability from node *l* to node *k*.

Step 7:
For a node n_k, if $Tv_k < Tv_{thr}$, where Tv_{thr} is the trust threshold vector value, then that node is assumed to be a misbehaving node.

3.4. Packet format of MRSIDS

Source ID	Destination ID	Hop Count	Link Stability	Intruder status	CRC
2	2	1	4	4	2

Fig.2.MRSIDS Packet format

In fig.2, the proposed packet format of MRSIDS is shown. Here the source and destination node ID carries 2 bytes. The third field hop count determines the number of nodes connected to the particular node in the cluster. It occupies 1 byte. The link stability of 4 bytes size indicates whether link life time is good and it can handle network environmental defects. Status of intruder is verified during the route maintenance phase. It occupies 4 bytes. The last filed CRC i.e. Cyclic Redundancy Check used for error correction during packet transmission.

4. PERFORMANCE EVALUATION

The performance of the proposed approach is evaluated in this section. The simulation model is discussed in Section 4.1 and the simulated results are presented and described in Section 4.2.

4.1 Simulation Model and Parameters

We have simulated our results using NS2.34 simulator. It is an object oriented discrete event simulator to identify the performance of proposed scheme. The Backend language of NS2.34 is C++ and front end is Tool command language (Tcl). NS2 is user friendly and easy to fabricate our own protocol. Tcl is a string-based command language. The language has only a few fundamental constructs and relatively little syntax, which makes it easy to learn.

The syntax is meant to be simple. Tcl is designed to be a glue that assembles software building blocks into applications. Here we made the assumption that adopted for simulation is all nodes are moving dynamically including the direction and speed of nodes. Mobility scenario is generated by using random way point model with 300 nodes in an area of 1200 m × 1200 m. Our simulation settings and parameters are summarized in table 1.

A. Performance Metrics

We evaluate mainly the performance according to the following metrics.

- **Communication Overhead:** The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets. It suppresses the communication between the source and destination nodes.
- **End-to-end delay:** It depends on the routing discovery latency, additional delays at each hop and number of hops.
- **Detection Ratio:** It is the ratio of detection of link, path and node failure as well as malicious node to the total number of nodes during transmission phase.
- **Detection time:** It is the required time for IDS to detect all malicious nodes for each security framework increases.
- **False positive rate:** It is the ratio of number of nodes falsely compromised by the attackers to the number of genuine nodes.
- **Link Stability Rate :** It is defined as the ratio of number of stable links to the number of links established.

Table1. Simulation and Settings parameters of SIDS

No. of Nodes	300
Area Size	1200 X 1200
Mac	802.11
Radio Range	200m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	80 bytes
Mobility Model	Random Way Point
Initial energy	75
Transmitted power	0.879 watts
Received Power	0.08 watts
Protocol	ODMRP

4.2 Results

We compared our proposed system MRSIDS with SIDS [9], EAACK [3], AAIDS [13] and our previous schemes OMRS [20], RERMR [21] and FLRMRP. In Fig.3, we vary the simulation time from 20 to 100 secs. While increasing the time, the communication overhead of proposed IDS is low than the existing IDS systems and previous schemes. This is achieved by employing the trustable factor in the transmission process.

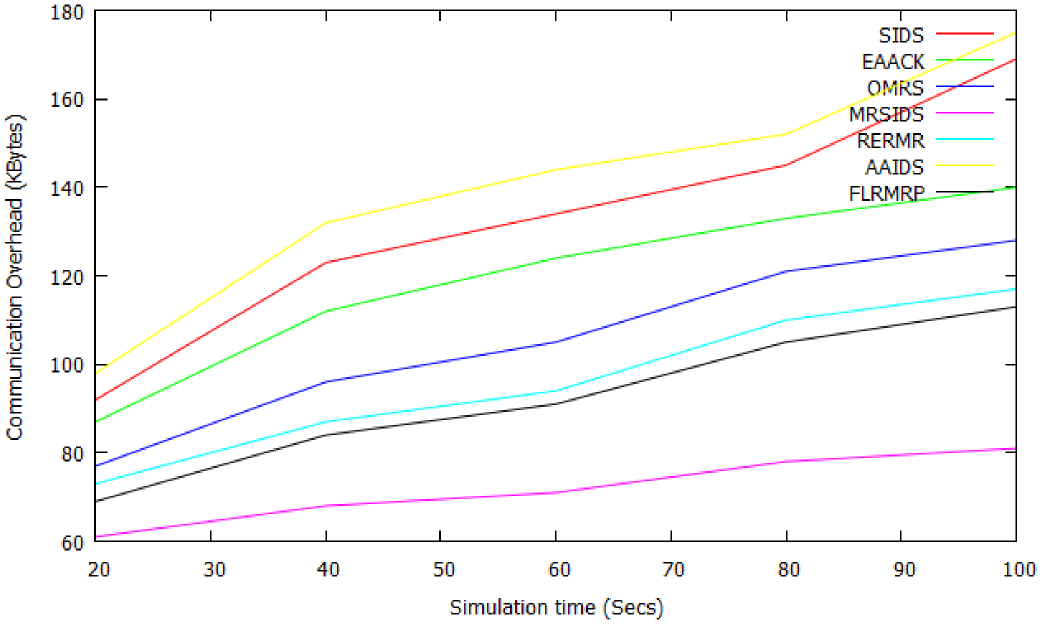

Fig 3. Mobility Vs Communication Overhead

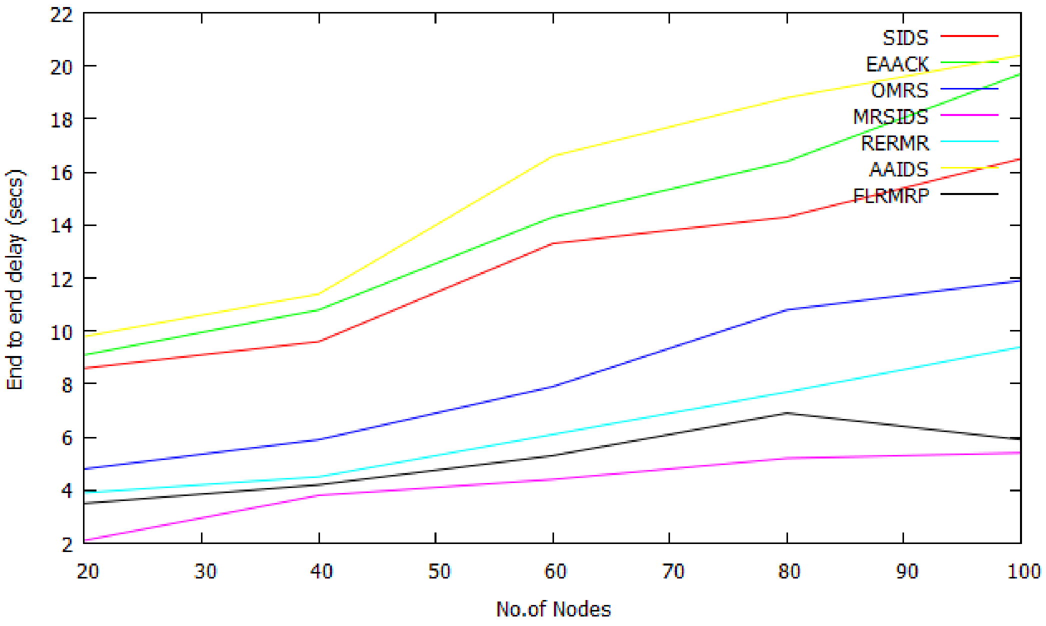

Fig 4. No. of Nodes Vs End to end delay

In Fig. 4, number of nodes is varied as 10, 20….100. When we increase the node, the mobility is also getting increasing. The proposed system achieves less end to end delay per packet than the existing IDS and our previous schemes because of link stability scheme.

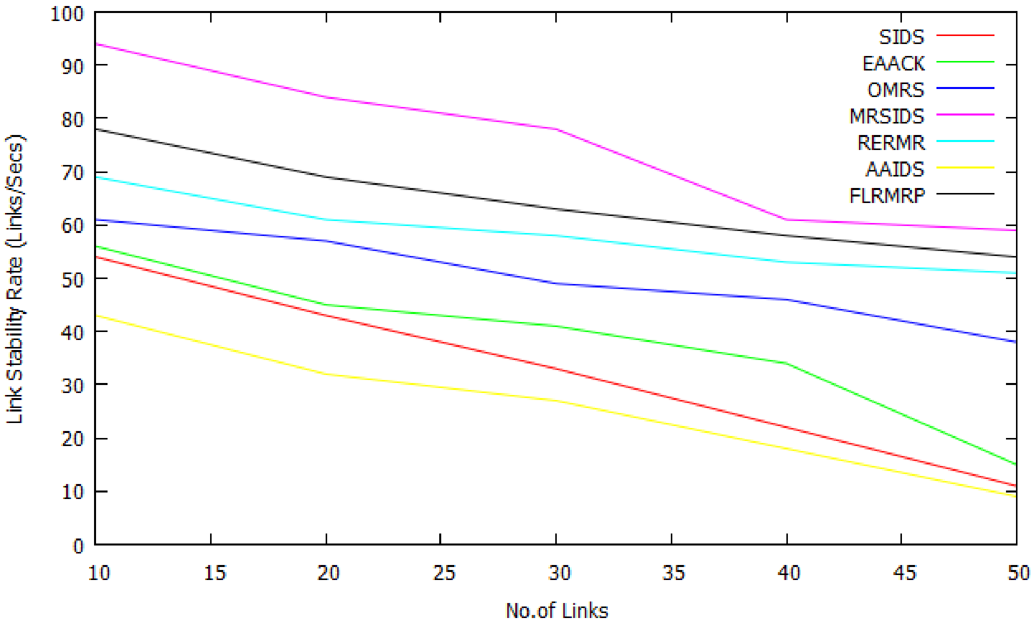

Fig 5. No. of Links Vs Link Stability Rate

In Fig.5, we vary the number of links like 10, 15, …50. The link stability rate of MRSIDS achieves higher than the existing IDS systems and our previous schemes.

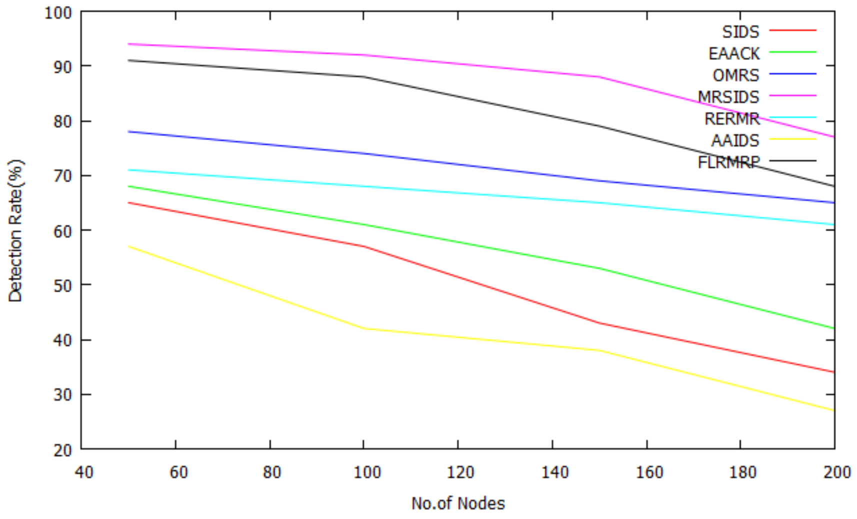

Fig 6. No. of Nodes Vs Detection Rate

Fig.6 shows the analysis of number of nodes Vs Detection Rate. From the results, our proposed system achieves high detection rate than the existing IDS and our previous schemes because of reliability and trust factors deployed in the multicast routing.

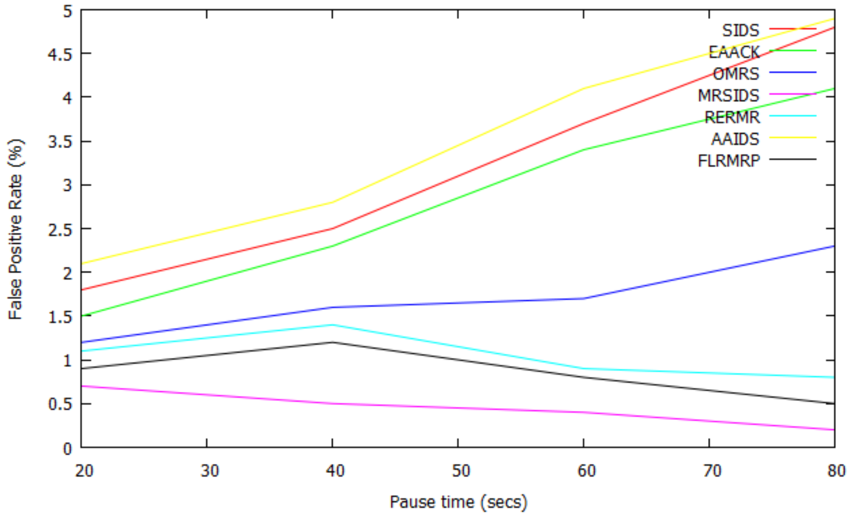

Fig 7. Pause time Vs False Positive Rate

In Fig. 7, pause time is varied as 20, 40….80 secs. When we increase the time, the packet transmission is also getting slow. The proposed system achieves less false positive rate per node than the existing IDS and our previous schemes because of less compromised nodes.

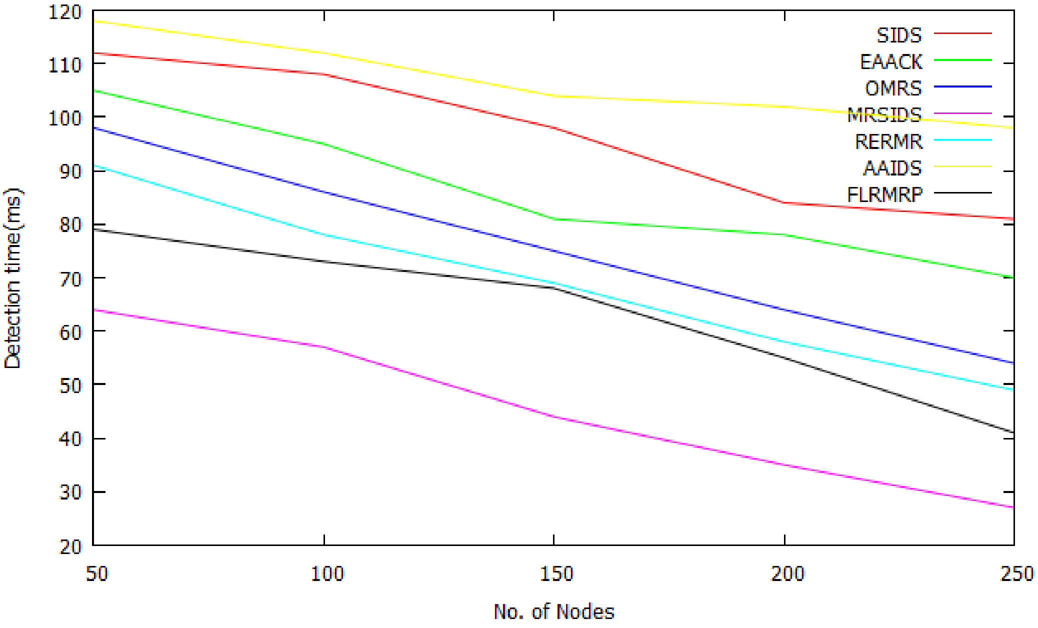

Fig. 8. No. of Nodes Vs Detection time

Fig.8 shows the analysis of number of nodes Vs Detection time. From the results, our proposed system achieves less detection time than the existing IDS and our previous schemes because of reliable multicast routing and trust threshold vector value.

5.CONCLUSION

In this research work, an multicast route stability based Intrusion detection system is proposed for handling link, node path failures and malicious attackers in ad hoc networks. The proposed scheme is based on threshold value to maintain the reliable multicast routing which enhances the stability and network connectivity. The detection rate is achieved higher by means of integrating link stability with intrusion detection system. Based on trust threshold vector value, node can be detected as genuine or malicious node. By simulation results, the MRSIDS is better than previous IDS systems in the presence of malicious nodes. Future studies can be extended to implement the authentication and security in the reliable multicast routing scheme to make high integrity. We plan to choose the symmetric cryptographic schemes to make network more secure.

References:

[1] Nilotpal Chakraborty, “Intrusion Detection System Aand Intrusion Prevention System: A Comparative Study”, International Journal of Computing and Business Research (IJCBR), Vol.4, Issue 3, 2013, pp.1-8.

[2] Aikaterini Mitrokotsa, Christos Dimitrakakis, “Intrusion detection in MANET using classification algorithms: The effects of cost and model selection”, Ad hoc Networks, Elseiver, 2012, pp.1-12.

[3] E.M.Shakshuki, Nan Kang, T.R.Sheltami, “ EAACK – A Secure Intrusion Detection System for MANETs”, IEEE Transactions on Industrial Electronics, Vol.60, Issue 3, 2013, pp.1089-1098.

[4] Ayesha Taranum, Manju N, Tejaswini R M, “RAACK-Reinforce Adaptive Acknowledgement A Secure Intrusion Detection System for MANETs”, International Journal of Computer Science and Information Technology Research, Vol.2, Issue 2, 2014, pp.283-296.

[5] Hichem Sedjelmaci and Sidi Mohammed Senouci, “An accurate and efficient collaborative intrusion detection framework to secure vehicular networks”, Journal of Computers and Electrical Engineering, Elsevier, 2015, Vol.43, pp.33-47.

[6] Wenchao Li, Ping Yi, Yue Wu, Li Pan, and Jianhua Li, “A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network”, Journal of Electrical and Computer Engineering, 2014, pp.1-9.

[7] Gang Wang, Jinxing Hao, Jian Ma and Lihua Huang, “A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering”, Expert Systems with Applications, Elsevier, 2010, pp.1-8.

[8] S.Parameswari and G.Michael, “Intrusion Detection System Using Mobile Agent In Manets”, Researchjournali’s Journal of Computer Science, Vol.1, No.2, 2014, pp.1-5.

[9] Mueen Uddin, Azizah Abdul Rehman, Naeem Uddin, Jamshed Memon, Raed Alsaqour, and Suhail Kazi, “Signature-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents”, International Journal of Network Security, Vol.15, No.1, Jan. 2013, pp.79-87.

[10] S. Mamatha and A. Damodaram, “ Intrusion Detection System for Mobile Ad hoc Networks Based on the Behavior of Nodes”, International Journal of Grid Distribution Computing, Vol.7, No.6, 2014, pp.241-256.

[11] Zubair Md. Fadlullah, Hiroki Nishiyama, Nei Kato, and Mostafa M. Fouda, “Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks, ” IEEE Network Magazine, vol. 27, no. 3, 2013, pp. 51-56,

[12] Sapna Choudhary and Alka Agrawal, “ Threshold Based Intrusion Detection System for MANET using Machine Learning Approach”, International Journal of Advance Electrical and Electronics Engineering (IJAEEE), Vol.3, Issue 1, 2014, pp.1-6.

[13] Farzaneh Geramiraz, Amir Saman Memaripour, and Maghsoud Abbaspour, “ Adaptive Anomaly-Based Intrusion Detection System Using Fuzzy

Controller", International Journal of Network Security, Vol.14, No.6, 2012, pp.352-361.

[14] Marjan Kuchaki Rafsanjani, laya Aliahmadipour and Mohammad Masoud Javidi, "A hybrid intrusion detection by game theory approaches in MANET", Indian Journal of Science and Technology, Vol. 5, No. 2, 2012, pp.2123-2131.

[15] Ms. Rasagna Chinthireddy & Dr. S Arvind, "Robust Intrusion Detection Mechanism for Mobile Adhoc Networks", International Journal of Computer Trends and Technology (IJCTT) – Vol.14 N0.3, 2014, pp.135-140.

[16] P. Uma Maheswari, N.Jeyananthini, K.Kalaivani and S.Vidya, "An Authoritative Intrusion Detection System for MANETs using DSAB", International Journal of Advanced Research in Computer Science Engineering and Information Technology, Vol.2, Issue 3, 2014, pp.255-262.

[17] Vishnu Balan E, Priyan M K, Gokulnath C and Prof.Usha Devi G, "Fuzzy Based Intrusion Detection Systems in MANET", International Symposium on Big Data and Cloud Computing, Elsevier, Vol.50, 2015, pp.109-114.

[18] Mouhannad Alattar, Françoise Sailhan, and Julien Bourgeois, "On Lightweight Intrusion Detection: Modeling and Detecting Intrusions Dedicated to OLSR Protocol", International Journal of Distributed Sensor Networks, 2013, pp.1-21.

[19] Anusha K, Jayaleshwari N, Arun Kumar S and Rajyalakshmi G V, "An Efficient And Secure Intrusion Detection Method In Mobile Ad hoc Network Using Intuitionistic Fuzzy", International Journal of Engineering and Technology, Vol.5, No.3, 2013, pp.2575-2584.

[20] Dr.A.Rajaram and S.Gopinath, " Optimized Multicast Routing Scheme for Mobile Ad hoc Networks, Journal of Theoretical and Applied Information Technology, Vol.59, No.1, 2014, pp.213-221.

[21] S.Gopinath and Dr.N.Nagarajan, "Energy based Reliable Multicast Routing Protocol for Packet Forwarding in MANET", Journal of Applied Research and Technology, Vol.13, Issue 3, 2015, Accepted for publication.

AUTHORS PROFILE

S.Gopinath received the **B.E.** degree in electronics and communication engineering from the Govt. College of Engineering, Salem, Anna University, Chennai, India, in 2007.He earned **M.E.** year in electronics and communication engineering (Communication Systems) in Anna University of technology, Coimbatore, India, during June 2011. He is currently pursuing the Part time Ph.D in the faculty of Information and Communication Engineering in Anna University, Chennai, India. He is currently working as an Assistant Professor, Department of ECE in Karpagam Institute of Technology, Coimbatore, India. His research interest includes wireless communication (**WiFi, WiMax**), Mobile Ad hoc networks, Sensor Networks, Neural Networks and fuzzy logic, Communication networks.

Dr.N.Nagarajan received his B.Tech. and M.E. degrees in Electronics Engineering from the Madras Institute of Technology, Chennai during the years 1982 and 1984 respectively. Later he obtained his Ph.D. degree from Anna University, Chennai in “Faculty of Information and Communication Engineering” during the year 2006. He has published more than 50 papers in International Journals and 25 papers in National and International Conferences. He is currently working as the Principal, Coimbatore Institute of Engineering and Technology, Coimbatore. He is member of board of study of faculty of information Technology at Anna University of technology, Coimbatore. His specialization includes optical, wireless Adhoc and sensor networks. He is guiding assorted research scholars in optical networks and wireless networks.