ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 8, August 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Performance Analysis on IDS based Secure Routing over Ad hoc Networks

Sweta[1]
M. Tech Scholar
Department of Computer Engineering
Om Institute of Technology & Management,
Hisar, Haryana – India

Surender Singh[2]
Assistant Professor & H.O.D. (CSE)
Department of Computer Science and Engineering
Om Institute of Technology & Management,
Hisar, Haryana – India

Abstract: ***Ad hoc routing protocols operate in open network environment and any malicious node can intercept the network traffic and can use it later on. It is quite hard to detect the signatures of the malicious nodes at early stages. Researchers have developed many solutions to detect various threats and prevent the network. Each solution can identify a particular attack type but if the intensity of attack is very low then it cannot be rectified. In this paper, we introduced a IDS based solution which can prevent the network from malicious nodes and supports three different sensitivity modes i.e. LOW, MEDIUM and HIGH. In case of compromised network, proposed scheme performs well under the various constraints i.e. Throughput, PDR, Routing Load and End to End Delay etc.***

Keywords: Intrusion Detection, Intrusion Prevention, Security Threats, MANET, Ad hoc Routing.

I. INTRODUCTION

Intrusion Detection System (IDS)

An ID defines some set of rules which are used to filter the traffic and collected data is further used to make decisions. IDS can be configured as per the network environment. For traditional networks following are some common IDS:

1. **Host based IDS:** HIDS can be deployed into a network to trace the traffic conditions and it can also generate as per the detected threats. Its scope is limited to a specific network only.
2. **Network based IDS (NIDS):** It is similar to HIDS but it offers more capabilities. It can be used for multiple devices and on the basis of traffic patterns it can detect the known threats but does not support the dynamic authentication and its accuracy is degraded due to congestion over network.
3. **Local Intrusion Detection System (LIDS):** It offers security at node level. It collects data and shares among all nodes. Large scale data collection and processing consumes excessive amount of resources.
4. **Zone Based Intrusion Detection System (ZIDS):** It gathers the location of each node on the basis of zones. It can filter the data for Interzone as well as for Intrazone and traffic analysis becomes easy. [16]

Now we will discuss the different type of intrusion detection and prevention methods developed to secure mobile Ad hoc Network.

Watchdog Method

Watchdog method is used to provide protection to MANETs and embedded with network layer. Watchdog mainly ensures to improve throughput of network performance with the presence of malicious nodes. It uses two schemes:

1. **Watchdog scheme and Path rater scheme:** Watchdog scheme protects the IDS mechanism for MANETs, capable of identifying malicious nodes misbehaviors in the network. This further detects malicious misbehaviors by dissolutely listening to its next hop's transmission. If Watchdog node overhears in a network that will make failure count of the mobility of nodes [8]. This increases its failure counter of packets while transmitting and receiving the nodes. Whenever a node is failure while transmitting and receiving at a certain threshold value, it reports to Watchdog and it verifies as a misbehaving node in network.

2. **Path rater scheme:** It will identify the misbehaving nodes in the form of failure count and reports to Watchdog scheme for future transmission [1] [2] [3]. This gives more advantages in reporting the Misbehaving nodes, hence Watchdog is popular in some cases.

Receiver Collision

There may be large scale collision between the intermediate nodes thus can degrade the network performance. High false rejection reports can be generated to protect the network from intrusion and by isolating the intruder nodes from the network[5].

Hybrid Cryptographic Key Exchange Algorithm

Hybrid Cryptographic key exchange algorithm uses asymmetric key such as it may use public key as well as private key in a communication network to exchange request and response .The Key distribution is an important feature of predictable algorithm and the entire protection is needy on the distribution of key using secured channel [9].HYBRID Cryptographic mechanism [4] utilizes the public and private key of asymmetric key cryptography to exchange the secret key to secure the information.

Algorithm	Description
Pathrater	Uses link reliability data, rating the path (reputation system) and Watchdog technique but it is applicable to Applicable only to source routing protocols. Cannot detect partial dropping and collaborative attacks
LiPaD	It deals with packet dropping and it can enable all nodes to monitor the packets being propagated in network. It can Detect only selective forwarding attacks and it cannot detect dropping attacks in Collaborative attacks.[4][5][6][7]
Anomaly Detection:	It can be referred as unauthorized data access, Channel Noise, false packet injection over network etc. anomaly detection scheme uses compression methods to identify its symptoms. It adopts the multiple data patterns and saves them in to profiles which are further used to analyze the coming traffic but it suffers from the variations in data rate/ false positives. [16]
Signature Detection:	It uses traffic patterns as signature which can be used to detect the malicious nodes in network. Its response time is minimum and having low false positive rate as compared to other IDS.
Enhanced Adaptive Acknowledgement (EAACK)	It uses ACK for each communication between nodes. If any node overhear the ACK packet that means originator of ACK can identified as malicious node. It has merits over Watchdog method as it can handle the issues related to receiver collisions and false misbehavior data etc.
S-ACK:	It is an enhancement of TWO ACK method which can identify the malicious nodes on the basis of ACK packets. When a node receives any packet from sender, it just increments the trust value for the same otherwise false value is increased.
Misbehavior Report Authentication:	MRA is the enhanced version of S-ACK which reacts over the false reports. It can verify the packets on the basis of local knowledge and analyze the false report. [16]

II. LITERATURE REVIEW

Trupti K. Marve et al. [10] explored the IDS solution for multiple layers which can identify the Denial of Service attack over various layers. It detects the attack using different levels. First level identified the presence of malicious nodes and second level uses this information to protect the routing layer attacks. Results show its performance in terms of reduction of false positive rates.

A.**Lupia et al. [11]** focused on energy aware IDS module to detect the intruders over multiple networks. It estimates the time required to monitor the network traffic at fix packet transmission rate. If any node drops the packet irrespective to transmission rate over a certain time interval, its time bound trust value is reduced and after a Threshold, particular node is identified as malicious node. Simulation results show that it consumes very less energy for traffic monitoring and energy consumption does not affect the detection accuracy.

Qi Guo et al. [12] developed an attack type environment to verify the protocol behavior under compromised conditions. It defines attack type and attack target for intrusion detection under the constraints of IDS rules i.e. PURPOSE, CONDITION and CAUSE etc. Simulation results show the effectiveness of the proposed scheme

depends upon the selected rules for intrusion detection.

I.Marchang et al. [13] considered the energy consumption due to excessive monitoring of data traffic and introduced a solution based on activation time without compromising the network resources. Proposed scheme reduces the active time for IDS and intermediate nodes monitor their neighbors at regular interval and if any node does not fulfill the compulsory security level, it is recognized as malicious node. Simulation results show its performance in terms of resource conservation and it can be extended to support the heterogeneous networks.

S.V.Shirbhate et al. [14] used a method based on k-means Clustering algorithm. It uses three different phases i.e. Training, Testing and Update. During Training phase, data is normalized at odd level. k-means Clustering defines the normal profile for nodes. Testing phase defines a regular time interval and within this time frame, data is collected at node level and compared with normal profiles to identify the malicious nodes. After each interval, normal profile is updated. If Test phase detects any intruder node, then it is isolated from entire network. Simulation results show its performance in terms of detection accuracy and false positive rate.

Amar Amouri et al. [15] developed a IDS framework which defines promiscuous zones (PZ) using clustering algorithm and cluster head is used to collect the data from other nodes. Zone subdivides the area into small areas and node can join and leave the zones any time. Data collect at node level is used to detect the intrusion and final decision tree are used to take initiate the action against intruders. Simulation result shows its performance in terms of attack detection ratio and optimal energy consumption.

S. Banerjee et al. [16] investigated the various types of intrusion detection system. For traditional networks, Host based IDS can be used to detect the intrusion, for interval network. Network based IDS monitors the real time traffic and filter out the packets as per the defined rules. Zone based IDS can be used to protect the Interzone as well as the IntraZone traffic. In case of ad hoc networks, WatchDog is used to analyze the behavior of all nodes in a given network and node can also use Acknowledge method to overcome from the limitations of watchdog method, Anomaly Detection method analyze the Noise level and false packet recognition. It can also use the existing database. Intrusion can also be detected on the basis of application signatures

P. S. Moon et al. [17] explored the various hybrid methods which can be used for intrusion detection and prevention. Some recent developed solutions are Modern Encryption Standard, cellular automata based security algorithm, Enhanced Adaptive Acknowledgment, Cellular Automata based key management scheme and Secured Data Communication scheme etc. All these

methods also consider the power consumption, successful data transmission, capability to detect the multiple attacks at same time, double encryption/decryption standards etc.

T. A. Ghaleb et al. [18] investigated the impact of intruder density over the performance of intrusion detection system. Experimental results show that if density f malicious nodes vary, then performance of AACK may be degraded. Current research work can be extended to analyze the impact of scalability over the performance of IDS.

Ming Zhang et al. [19] developed a anomaly detection model based on One-class SVM for intruders. Distributed training data is used to analyze the current traffic conditions and OC- SVM maintains the higher detection rate for low intensity attacks. Simulation results show that it performs well as compared to existing Probabilistic Neural Network but its detection accuracy may suffer due to unavailability of large scale data and proposed scheme can be extended to overcome from this limitation.

III. PROPOSED SCHEME

Intrusion Detection Scheme

0: Set node(s): n;

1: Topology Deployment

2: Set Sensitivity Level sL: (LOW/ MEDIUM/ HIGH)

3: Initiate Communication

4.1: Analyze_Traffic->Layer. Application

4.2: Analyze_Traffic->Layer.Routing

4.3 If Drop(PKT)==true for each layer

4.4: Switch () { Case: sL->LOW

{ Set Filtering_Threshold_H=High;

Set Alarm->True while Packet_Loss> Filtering_Threshold_H }

Case: sL->MEDIUM

{Set Filtering_Threshold_M=Medium; Set Alarm->True while Packet_Loss>Filtering_Threshold_M }

Case: sL->HIGH{ Set Filtering_Threshold_L=Low; Set Alarm->True while Packet_Loss>=Filtering_Threshold_L}

Default: repeat Steps:4}}

Rules:

LOW	MEDIUM	HIGH
Ignore Packet loss at each layer because it may be due to contention, congestion or buffer overflow. In case of huge packet loss, start filtering at node level	Start monitoring the traffic for each layer, if packet loss occurs at least two layers simultaneously.	Start monitoring the traffic for each layer, if packet loss occurs if packet drop occurs at routing layer followed by application layer.

Application Level Traffic Monitoring

For each transmitted packet w.r.t Rules **Analyze**: 1. Sent Packets 2. Received Packets 3. Lost Packets 4. Packet Sequence Number **If**(sL) {**set Loga**(1)}	**Set Loga()** If (**Set Loga**==1){ 1. e:=Get PKT->Expected_SEQ-No 2. r:=GET PKT->RCVD_SEQ-No 3. l:=GET PKT->LAST_SEQ-No 4. if (e!=r && r+x!=e || l+x!r) 5. DeleteRoute(Node->Index) }
Routing Level Traffic Monitoring For each forwarded packet: w.r.t. Rules **Analyze**: Received Packets Packets Loss when forwarded to next Hop Route resolved failure Route Discovery failure **If**(sL) { **Set Logr** (1)}	**Set Logr**(1) If (**SetLogr**==1){ 1. Rt:= Get RoutingTableEntry 2. If (Rt->forward=1 && Drop()=1 3. Set Drop()=0 for each PKT in Rt 4. Set Forward()=1 for each PKT in Rt 5. }

IV. Simulation Analysis and Results

Simulation Configuration

Simulation Parameters	Values
Multicast Routing Protocol(s)	AODV
Wireless Terrain	1200x1200
Node Density	30
IDS Level(s)	LOW, MEDIUM, HIGH
MAC Protocol	MAC 802.11
Traffic Type	CBR
Packet Size	512
Sampling Interval	0.1 seconds
Simulation Time	10 seconds
Network Simulator	NS-2.35
Simulation Scenario(s)	Open Network Environment (OPN) IDS- Sensitivity-LOW IDS- Sensitivity-MEDIUM IDS- Sensitivity-HIGH

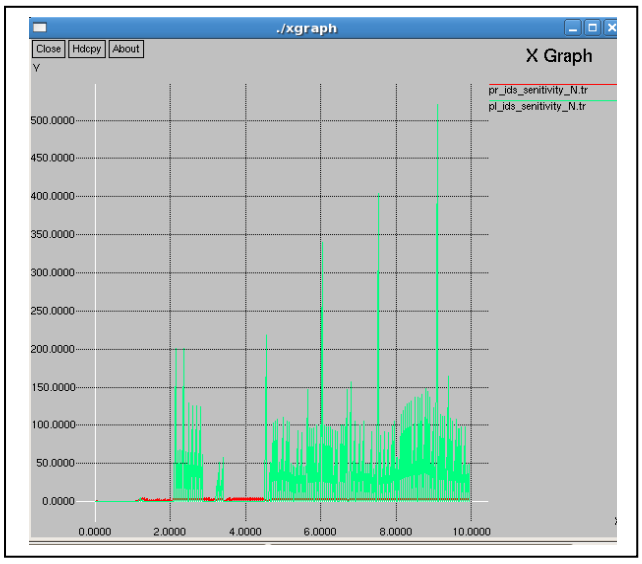

Figure 1: Packet Lost/Receive over Open N/W

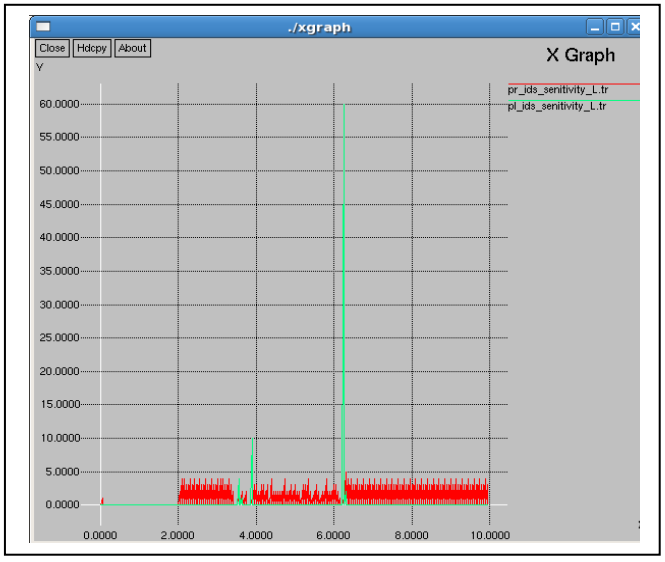

Figure 2: Packet Lost /Recvd-IDS-Sensitivity-L-Level

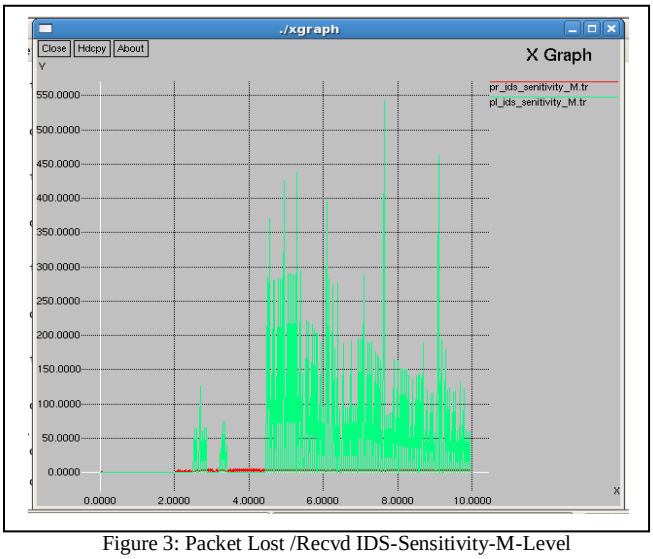

Figure 3: Packet Lost /Recvd IDS-Sensitivity-M-Level

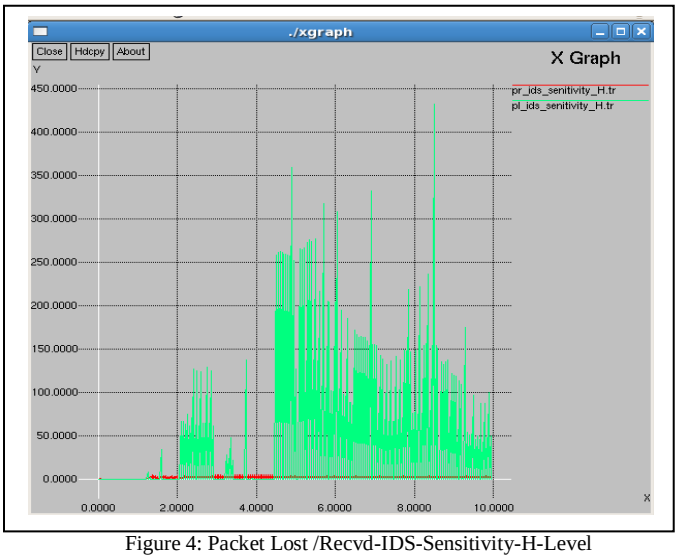

Figure 4: Packet Lost /Recvd-IDS-Sensitivity-H-Level

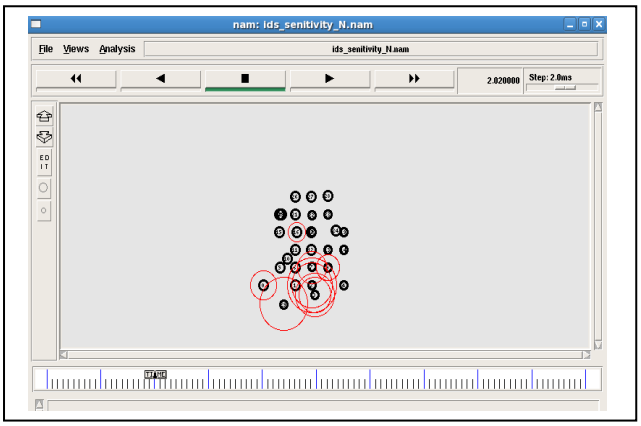

Figure 5: Simulation-Open Network Environment

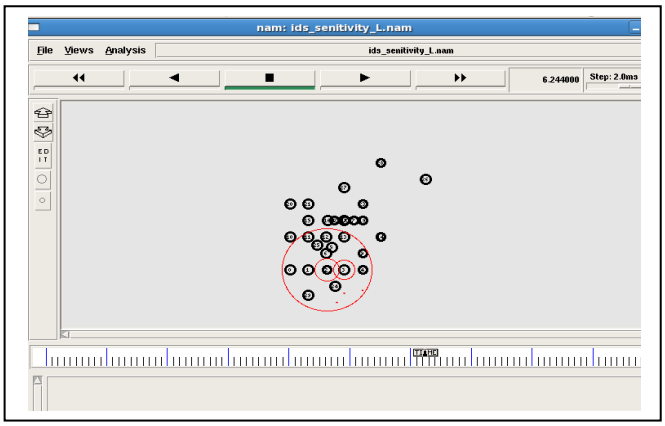

Figure 6: Simulation- IDS-Sensitivity-LOW-Level

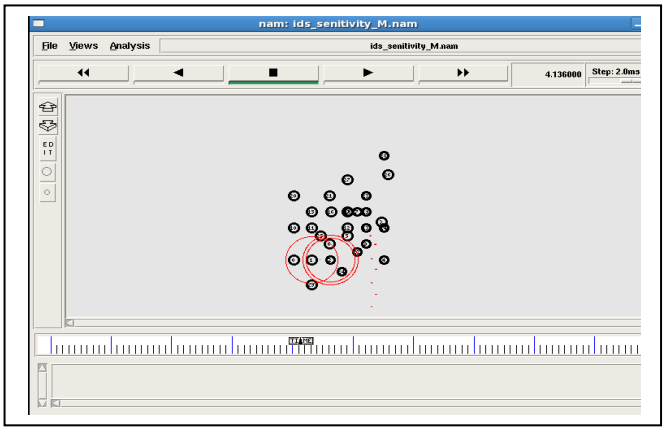

Figure 7: Simulation- IDS-Sensitivity-M-Level-0

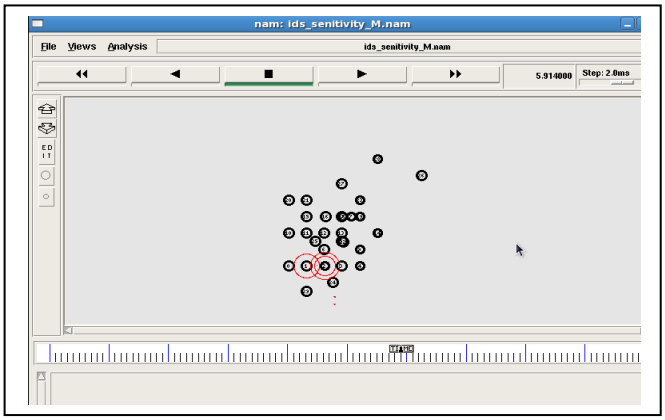

Figure 8: Simulation- IDS-Sensitivity-M-Level-1

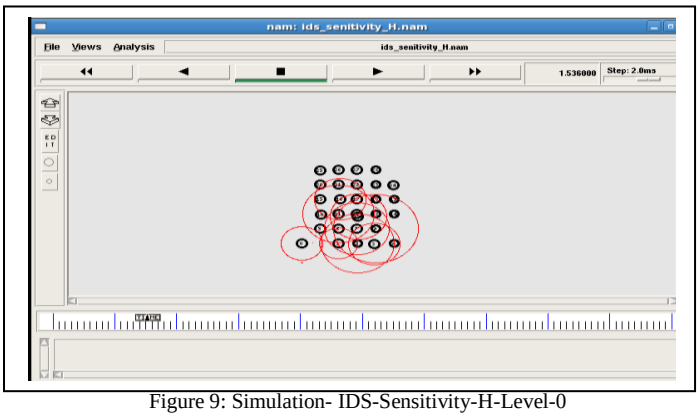

Figure 9: Simulation- IDS-Sensitivity-H-Level-0

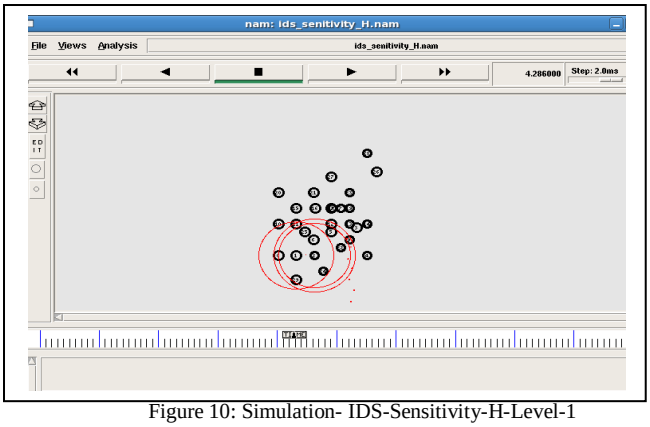

Figure 10: Simulation- IDS-Sensitivity-H-Level-1


```
22 - recvReply: received a REPLY
3 - recvReply: received a REPLY
handle_link_failure(6.163890): 22        (2       11       2)
handle_link_failure(6.163890): 22        sending RERR...
sending Error from 22 at 6.16
handle_link_failure(6.174275): 19        (2       9        11)
handle_link_failure(6.174275): 19        (0       9        11)
handle_link_failure(6.174275): 19        sending RERR...
sending Error from 19 at 6.17
handle_link_failure(6.198719): 3         (2       11       22)
handle_link_failure(6.198719): 3         sending RERR...
sending Error from 3 at 6.20
( 9) -  3 sending Route Request, dst: 2
(10) -  3 sending Route Request, dst: 2, tout 0.405848 ms
2 - recvRequest: destination sending reply
sending Reply from 2 at 6.20
recvRequest: discarding request
```

Figure11: Routing Log-Compromised Network

```
==========================================================
NODE: 0t 0.0265t 2t 2t 1t 2t 4t -0.1426t137087641
PACKET DROP started by 1===
==========================================================
NODE: 3t 2.0073t 2t 2t 1t 2t 6t -0.1426t137087641
NODE: 3t 2.0073t 0t 1t 2t 1t 4t -0.1426t137087641
PACKET DROP started by 1===
==========================================================
NODE: 1t 2.5111t 3t 3t 1t 3t 4t -0.1426t137087641
NODE: 1t 2.5111t 2t 2t 1t 2t 8t -0.1426t137087641
NODE: 1t 2.5111t 0t 0t 1t 0t 4t -0.1426t137087641
Packet DROP for NODE1 has been blocked===
==========================================================
NODE: 0t 3.0569t 1t 1t 1t 1t 4t -0.1426t137087641
NODE: 0t 3.0569t 3t 6t 2t 6t 4t -0.1426t137087641
NODE: 0t 3.0569t 2t 10t 3t 10t 6t -0.1426t137087641
==========================================================
NODE: 0t 3.0607t 1t 1t 1t 1t 4t -0.1426t137087641
NODE: 0t 3.0607t 3t 6t 2t 6t 4t -0.1426t137087641
NODE: 0t 3.0607t 2t 6t 2t 6t 10t -0.1426t137087641
Packet DROP for NODE1 has been blocked===
```

Figure 12: Routing Log-IDS Performance analysis

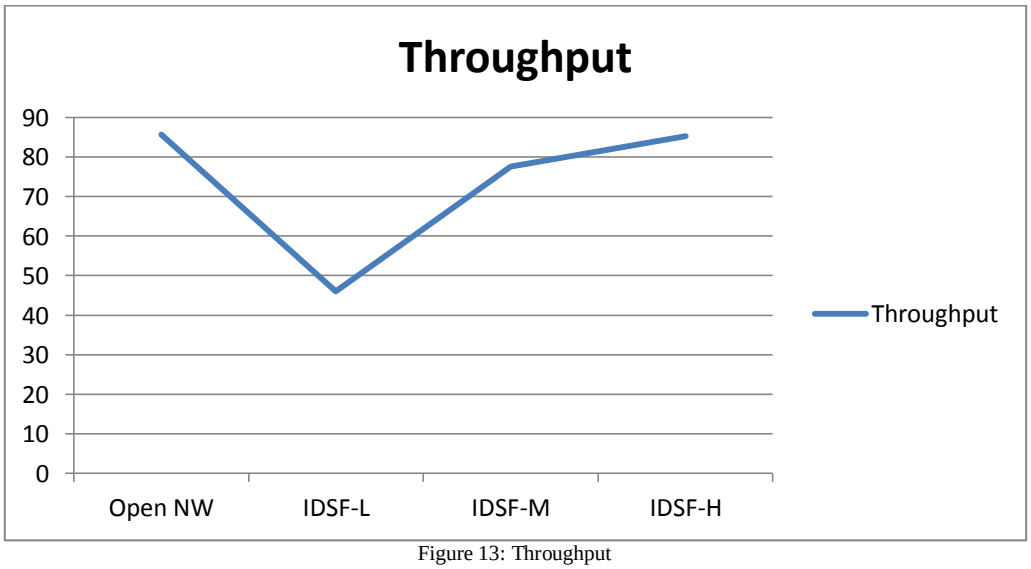

Figure 13: Throughput

Figure: above shows the Throughput of the AODV using different simulation scenarios. In case of open network environment (without any compromised situation), It is 85.7 bps, under compromised condition, when IDS sensitivity is LOW, it reduced upto its minimum level, 46 bps. If IDS sensitivity is set to medium level, it can be observed that Throughput is increasing (77.6 bps) and if IDS sensitivity is set to HIGH, than it is approx. 85.2 bps.

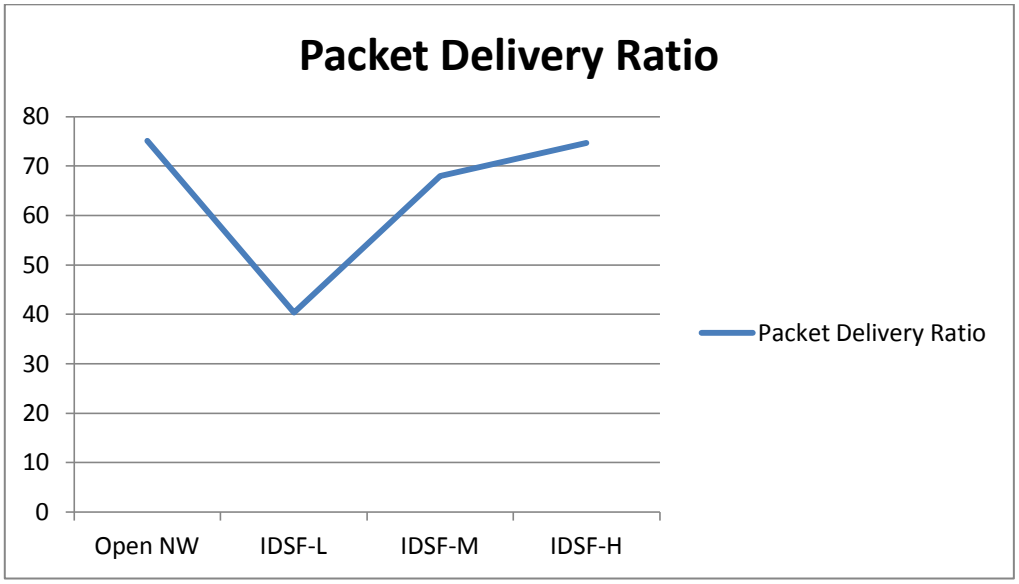

Figure 14: Packet Delivery Ratio

Figure: above shows the PDR of the AODV using different simulation scenarios. In case of open network environment (without any compromised situation), It is 75.10955302, under compromised condition, when IDS sensitivity is LOW, it reduced upto its minimum level, 40.31551271. If IDS sensitivity is set to medium level, it can be observed that PDR is increasing (68.01051709) and if IDS sensitivity is set to HIGH, than it is recovered upto 74.67134093.

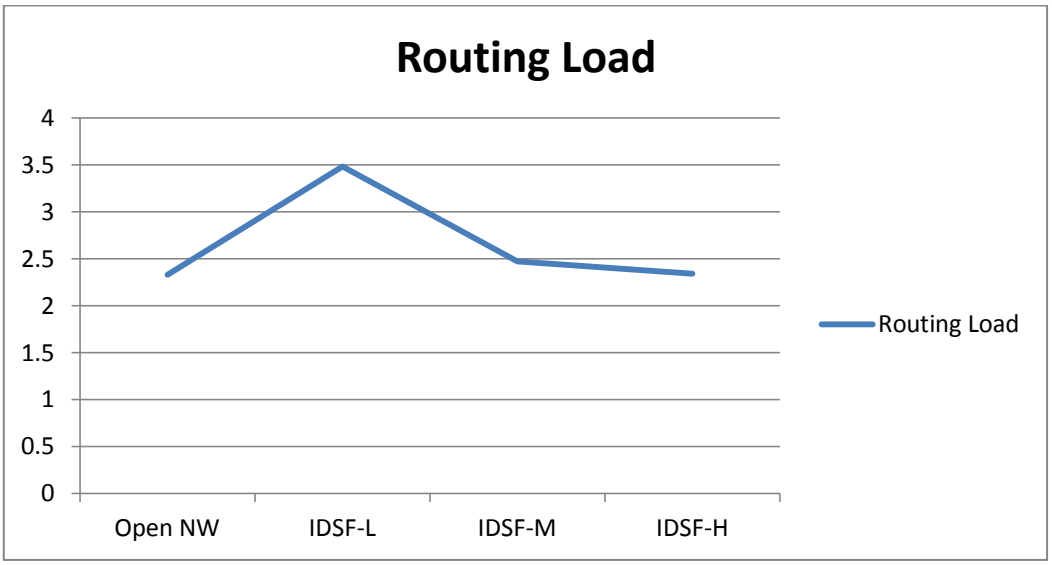

Figure 15: Routing Load

Figure: above shows the Routing Load of the AODV using different simulation scenarios. In case of open network environment (without any compromised situation), It is 2.331388565. Under compromised condition, when IDS sensitivity is LOW, it is increased upto its peak level, 3.480434783. If IDS sensitivity is set to medium level, it can be observed that it is decreasing (2.470360825) and if IDS sensitivity is set to HIGH, than it is 2.339201878.

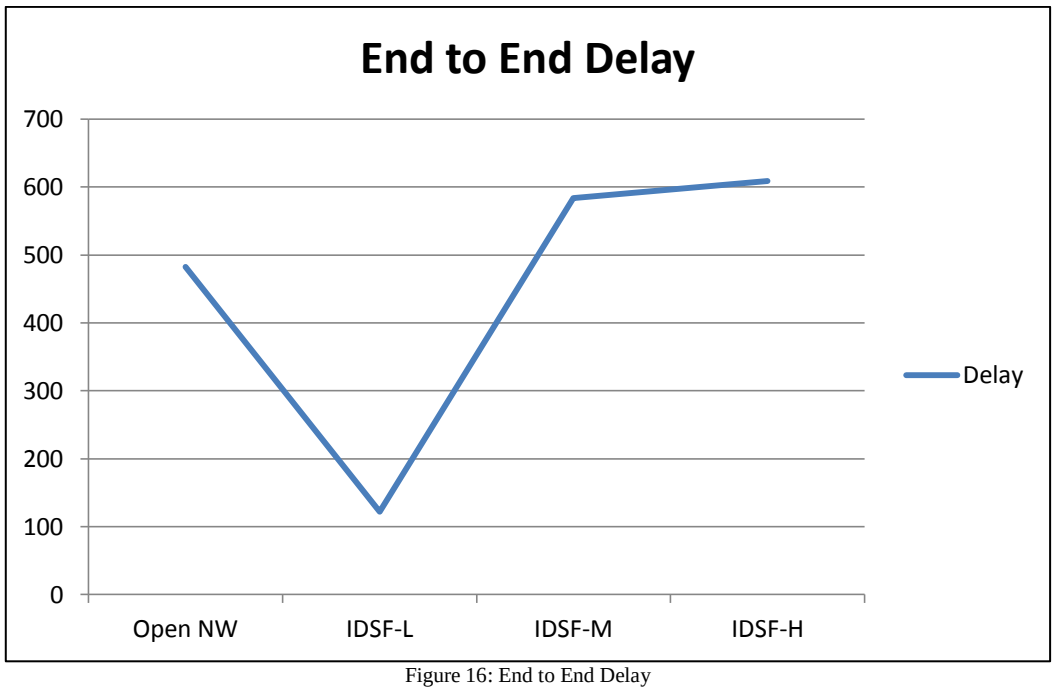

Figure 16: End to End Delay

Figure: above shows the End to End Delay of the AODV using different simulation scenarios. In case of open network environment (without any compromised situation), It is 482.632ms, under compromised condition, when IDS sensitivity is LOW, it reduced upto its minimum level, 122.157ms. If IDS sensitivity is set to medium level, it can be observed that End to End Delay is increasing upto 583.62ms and if IDS sensitivity is set to HIGH, than it is highest (608.591ms).

V. Conclusion

Researchers have developed various solutions for intrusion detection and prevention but no solution can defend from all type of threats. This research work is related to analysis of the mobile ad hoc networks under the influence of intrusion. We developed a solution for intrusion detection and prevention and compared the network performance using different parameters i.e. Throughput, Packet Delivery Ratio, End to End Delay and Routing Load. For Simulation purpose, NS-2 was used. There are different simulation scenarios were used to analyze the behavior of proposed scheme over the compromised network. In case of open network environment (OPN), Throughput of the AODV is 85.7 bps, under compromised condition, if IDS filtering is at LOW level, it is reducing upto its minimum level, 46 bps. If we set the filter at medium level, Throughput is increased up to 77.6 bps. If filtering is set to its highest threshold value then Throughput can be recovered upto approx. 85.2 bps.In case of uncompromised situation, PDR is 75.10955302, under compromised condition, when IDS sensitivity is LOW, it reduced upto its minimum level, 40.31551271. If sensitivity is at medium level, PDR is increasing (68.01051709) and if it is set to its highest level, than PDR is recovered upto 74.67134093.For open network environment, Routing Load is 2.331388565. Under compromised condition, with LOW sensitivity level, it is increasing upto its highest level, 3.480434783. Using medium sensitivity level, it is decreasing (2.470360825) and if with HIGH level of sensitivity, it is reduced upto 2.339201878. In case of open network environment, End to End Delay is 482.632ms and if IDS filter is less sensitive then it reduced upto its minimum level, 122.157ms but at medium level, it can be observed that it is increasing upto 583.62ms. If filter sensitivity is set to HIGH, than it reaches at highest value as compared to other simulation scenarios (608.591ms). As per above discussion, it can be observed that proposed scheme performed well with the support of sensitivity levels. If sensitivity level is set to its lowest level, it could not filter out the malicious nodes thus results in excessive packet drop. If sensitivity level is changed to MEDIUM stage, it improves the network performance and using highest level of sensitivity, it can protect the network and can retain the network performance to its last good known performance stage. It recovers the network from malicious behavior of nodes at the cost of Delay.

References

1. IETF Ad-Hoc Networks Auto configurations (autoconf) Working Group, IETF website:"http://datatracker.ietf.org/wg/autoconf/charter/IEEE Std 802.11-2007."
2. IEEE standard for information technology- Telecommunication and information exchange between systems- Local and metropolitan area network- Specific requirement, Part 11 Wireless LAN medium access control and physical layer specifications, IEEE June 2007.
3. "IEEE communications surveys & tutorials", Adnan Nadeem, and Michael P. Howarth, IEEE 2013.
4. J. Kim, "Integrating artificial immune algorithms for intrusion detection",Ph.D Thesis, Department of Computer Science, University College London, 2003.
5. Tsai, C. F., & Lin, C. Y. "A triangle area based nearest neighbors approach to intrusion detection". Pattern Recognition, 43, 2010, 222–229.
6. Su, M. Y. "Real-time anomaly detection systems for Denial of-Service attacks by weighted k-nearest-neighbor classifiers", 38, 2011, 3492–3498.
7. www.wikipedia.org.
8. Taher Ahmed Ghaleb, "Would an Intrusion Detection System Perform Alike With the Change of the Number of Mobile Nodes? An Experimental Evaluation", IEEE-2015, pp.1-5.
9. MohitSaxena, "A Mutual Playmate Attack Prevention Algorithm Enhancing Trust Levels in MANET's systems", ABLAZE, IEEE- 2015, pp.500-504
10. Trupti K. Marve, Nilesh U.Sambhe, "A Review on Cross Layer Intrusion Detection System in Wireless Ad Hoc Network", IEEE-, pp.1-4.
11. A. Lupia, Floriano De Rango, "Trust Management using Probabilistic Energy-Aware Monitoring for Intrusion Detection in Mobile Ad-hoc Networks", IEEE-, pp.1-6.
12. Qi Guo, Xiaohong Li, Zhiyong Feng and Guangquan Xu, "MPOID: Multi-Protocol Oriented Intrusion Detection Method for Wireless Sensor Networks", ICESS-IEEE-, pp.1512-1517.
13. I.Marchang, Raja Datta, Sajal K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks", IEEE Transactions on Vehicular Technology, 2015, pp.1-13.
14. S.V.Shirbhate, Dr.S.S.Sherekar, Dr.V.M.Thakare, "Novel Framework of Dynamic Learning Based Intrusion Detection Approach in MANET", International Conference on Computing Communication Control and Automation, IEEE-2015, pp.209-213.
15. Amar Amouri, Luis G. Jaimes, Raju Manthena, Salvatore D. Morgera, Idalides J. Vergara-Laurens, "A Simple Scheme for Pseudo Clustering Algorithm for Cross Layer Intrusion Detection in MANET", IEEE-2015, pp.1-6.
16. S. Banerjee, Roshni Nandi,"A review on different Intrusion Detection Systems for MANET and its Vulnerabilities", IEEE-2015, pp.1-7.
17. P. S. Moon, Piyush K. Ingole, "An Overview on: Intrusion Detection System with Secure Hybrid Mechanism in Wireless Sensor Network", ICACEA, IEEE-2015, pp.272-277.
18. Ming Zhang, Boyi Xu, Jie Gong, "An Anomaly Detection Model based on One-class SVM to Detect Network Intrusions", International Conference on Mobile Ad-hoc and Sensor Networks, pp. 102-107.

