RWD based IDS for MANET

Kavita Varule
PG student, Computer Engineering Dept.
Alamuri Ratnamala Institute of Engineering and Technology,
Shahapur, Thane, India

Sachin Bojewar
Assistant professor, Computer Engineering Dept.
Vidyalankar Institute of Technology,
Wadala (east),
Mumbai, India

ABSTRACT

Mobile Ad-Hoc network (MANET) is a temporary infrastructure less network. This network is formed by combining some set of wireless mobile hosts [1] [5]. The host is called as a node which dynamically establishes their own network. Intrusion detection in MANETs, however, is challenging for a number of reasons. These networks change their topologies dynamically due to node mobility; lack concentration points where traffic can be analyzed for intrusions; utilize self-configuring multi-party infrastructure protocols that are susceptible to malicious manipulation; and rely on wireless communications channels that provide limited bandwidth .To overcome these constraints, researchers have proposed a number of intrusion detection approaches specifically for MANETs. Intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources. In this IDS architecture multilayer specification based detection engine is used along with Random Walker Detector (RWD) [1] [16]. It randomly traverses a network and find outs that on which node which attack is occurred. If there is attacks it performs re-routing.

Keywords

Attacks, Intrusion Detection System (IDS), and Mobile Ad-Hoc network (MANET), Random Walker Detector (RWD).

1. INTRODUCTION

A network can be characterized as wired or wireless. Wireless can be distinguished from wired as no physical connectivity between nodes is needed. A mobile ad-hoc network (MANET) is an autonomous system of mobile nodes, a kind of a wireless network where the mobile nodes dynamically form a network to exchange information without utilizing any pre-existing fixed network infrastructure[9][16][8]. For a MANET to be constructed, all needed is a node willing to send data to a node willing to accept data. Each mobile node of an Ad-hoc network operates as a host as well as a router, forwarding packets for other mobile nodes in the network that may not be within the transmission range of the source mobile node[11][8]. Each node participates in an ad-hoc routing protocol that allows it to discover multi-hop paths through the network to any other node. Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network [17] [12] [10]. So it is important do find such attackers in Mobile Ad-Hoc Network (MANET). In this proposed architecture detection engine performs detections using a set of specifications. These specification describe normal nodes operations at different layers. Using the specification based detection engine it detect the few attacks at transport, network and data link layer. The proposed detection engine also performs the re-routing. This detection engine uses the Finite state Machine (FSM)[1] where each state of the FSM corresponds to either the legitimate or malicious behavior of the monitored node. It monitors the correct operation of critical protocols at the transport, network and data link layer. Intrusion detection system is a security technology which attempts to identify individuals who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges.

2. PROPOSED IDS ARCHITECTURE

In the proposed system effectiveness of detection engine at each node is increased. It consists of several robust RWDs that randomly traverse a network, while monitoring each visiting node for malicious behavior. A Random Walker (RW) is a stochastic process, which represents a path of random successive steps. At each visiting node RWD deploys a multi-layer specification based intrusion detection engine, which monitors the protocols and operations at the transport, data link and network layer. Because of the features of MANET there are many possibilities of attack in network. Existing system tries to prevent the system from attacker and also find the attack in the network [1] [16]. Here I developed such intrusion detection system which will detect the attacks on each node or network. Also while transmitting a packet from source to destination if any intermediate node is malicious node, system will tries to skip that node and will forward the packet using another path.

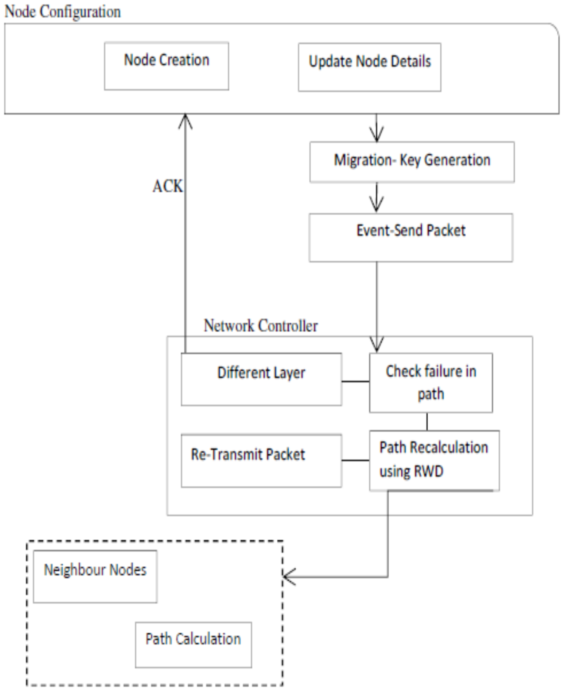


Figure 1. Proposed system

Fig. shows the proposed system. The system is divided in to following modules.

Node Creation

In this module we can add ‘n’ no of nodes and connect that nodes in a network. It keeps the track of node details i.e. all nodes in network as well as routing information. In routing table it stores all paths and respective messages in encrypted form.

Key Generation

After adding a node, node details in routing table are also get updated. Once node configuration for all nodes is done a secret key is generated for secure communication between nodes in network. The migration module of the node that initiates migration, generates a symmetric key using AES algorithm. Once the key is generated key exchange is performed. Every node will send its key to all the nodes in network as well as to docking service module.

Event

In event module actual communication is performed. A message or packet is transmitted from source to destination.

Network Controller

When source node will send the packet to destination, all the nodes in respective path are monitored for malicious behavior. A random walker detector monitors a specific node when it visit it for the malicious behavior. If any node in current path is malicious or attacked by attacker then retransmission can be done using new path. A new path is calculated using RWD. Instead of using any routing algorithm for MANET we used RWD for path calculation. It randomly select any intermediate node to form the new path. And using that path further communication is performed. After the successful transmission of packet an acknowledgment is send to the sender node from destination.

Re-routing

Because of features of MANET like Infrastructure less, Wireless Links, Multi-hop, Power limitation, Nodes movement autonomy, Memory and computation power limitation etc. There are many

Possibilities of attack in network. Existing system tries to prevent the system from attacker and also find the attack in the network. We developed such intrusion detection system which will detect the attacks on each node or network. Also while transmitting a packet from source to destination if any intermediate node is malicious node, system will tries to skip that node and will forward the packet using another path, called as re-routing.

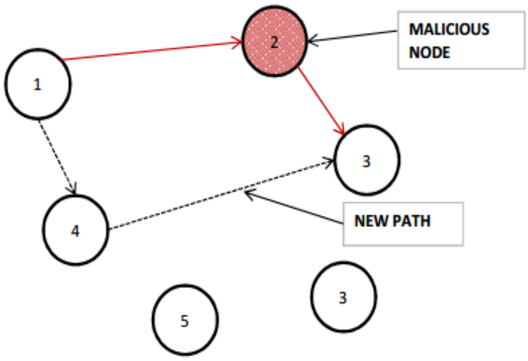
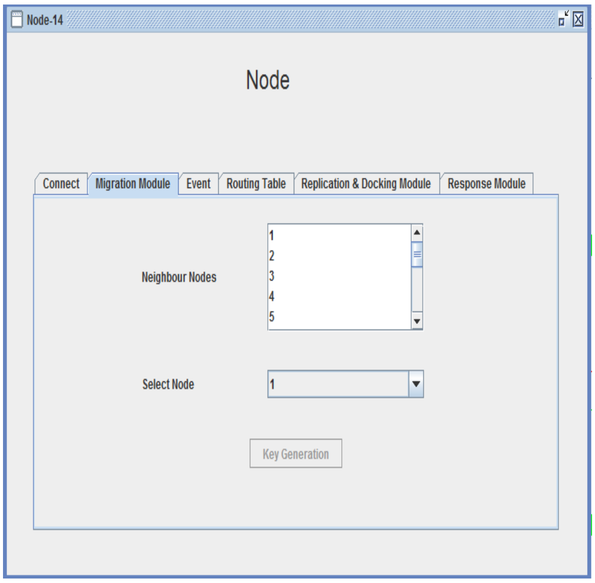


Figure 2. Re-routing

For example, in given fig.12 suppose transmission is from node 1 to node 3 via 2, and if intermediate node i.e. node 2 is malicious node then IDS will detect that node as malicious. In our case on node no. 2 there may be DoS attack, Session Hijacking, Black hole attack or SYN flood attack. After detecting the malicious node IDS will skip that node and will find new path using another node from network. In given example new path is 1-4-3. So transmission is completed using new path.

3. RESULTS

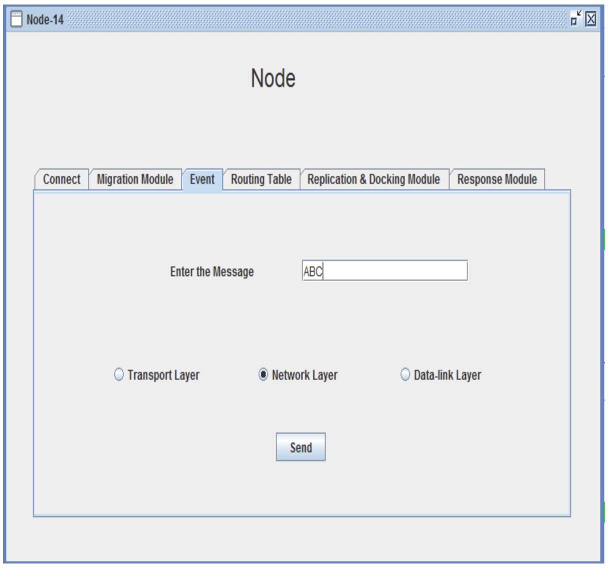
Case 1 - Network layer (DoS attack detected)



Neighbour Nodes: 1 2 3 4 5

Select Node: 1

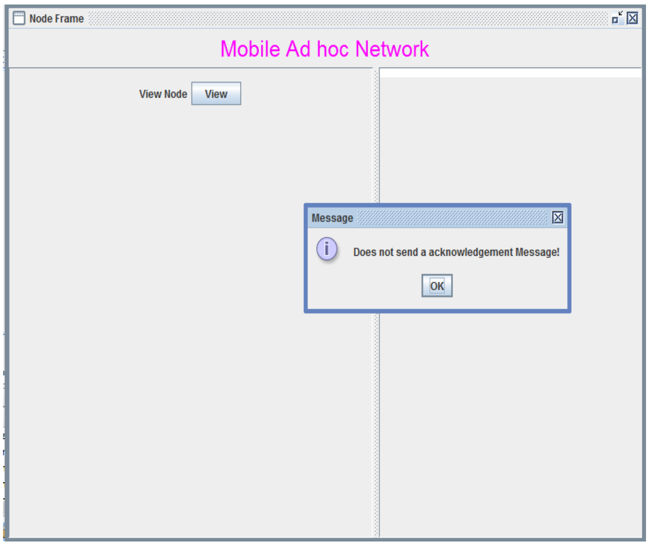
Figure 3 - Key generation between sender & destination



Enter the Message: ABC

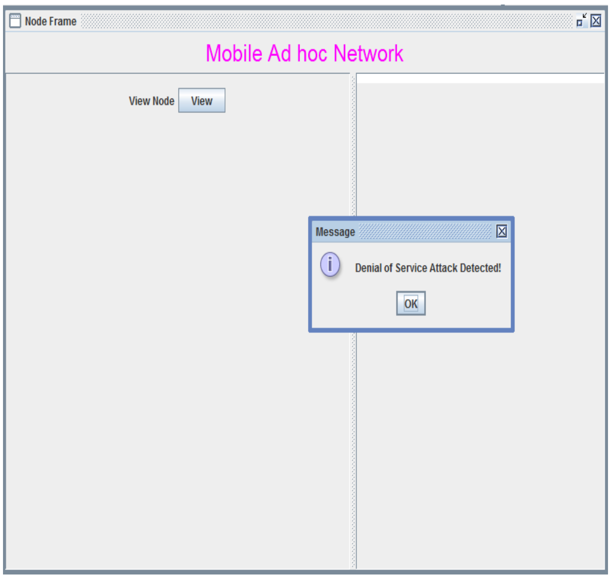
○ Transport Layer ● Network Layer ○ Data-link Layer

Figure 4 - Sending a message



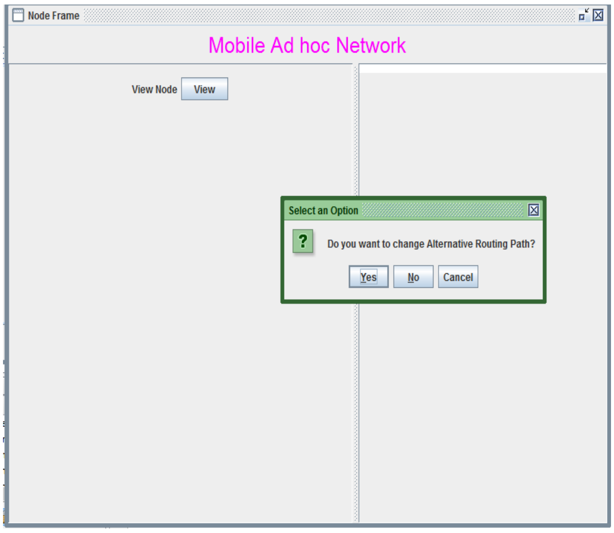
Does not send a acknowledgement Message!

Figure 5- Error (Attack Detected)



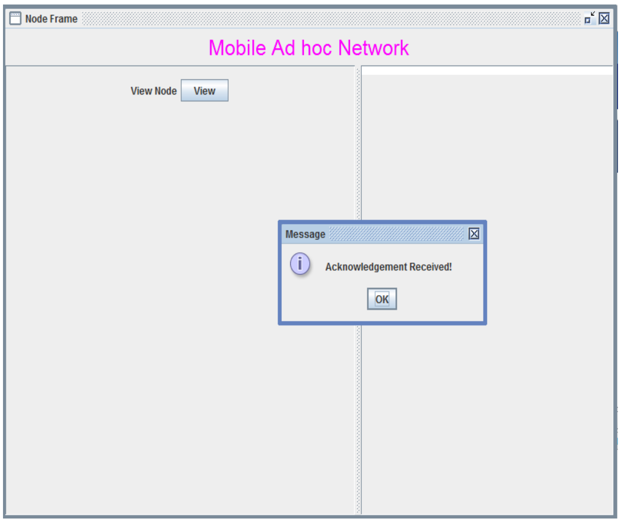
Denial of Service Attack Detected!

Figure 6- DoS attack Detected



Do you want to change Alternative Routing Path?

Figure 7- Alternate path



Acknowledgement Received!

Figure 8- Acknowledgement Received

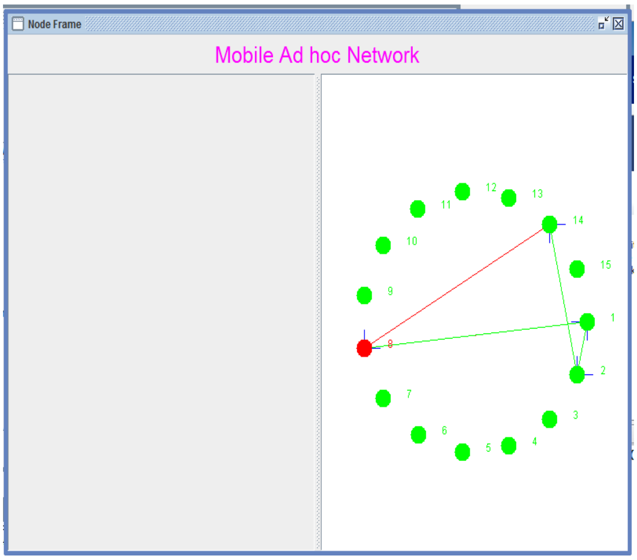
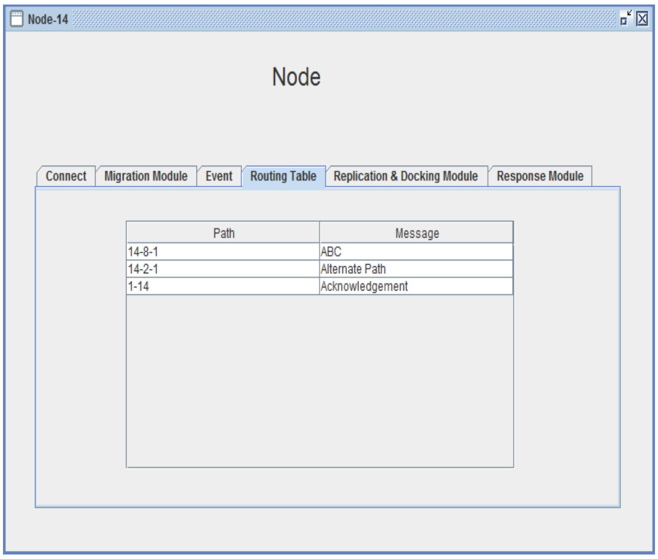
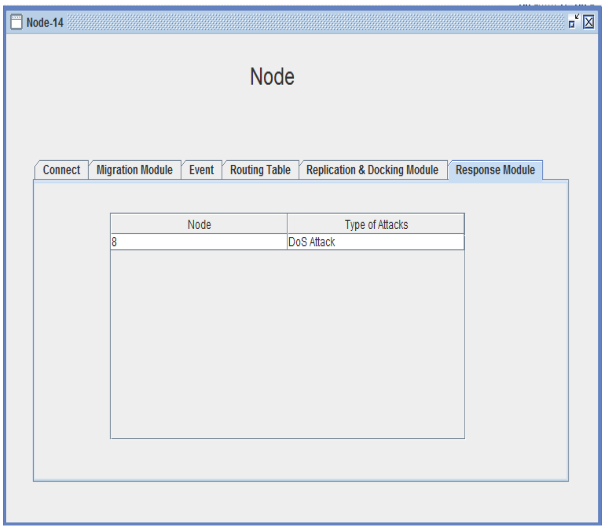


Figure 9- Output graph



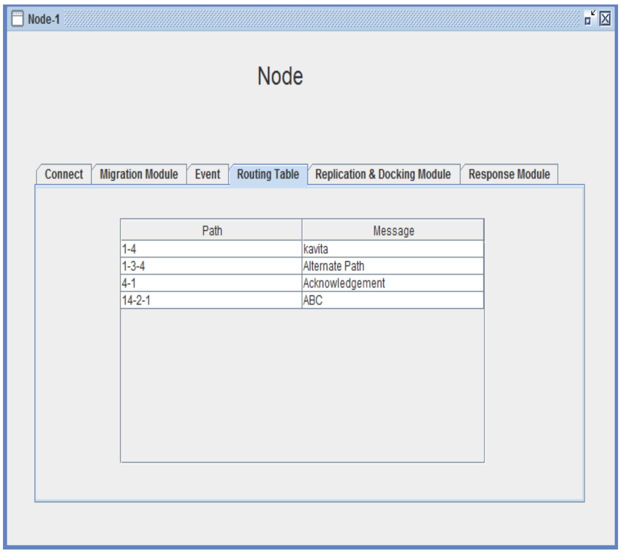
Path	Message
14-8-1	ABC
14-2-1	Alternate Path
1-14	Acknowledgement

Figure 10- Senders routing table



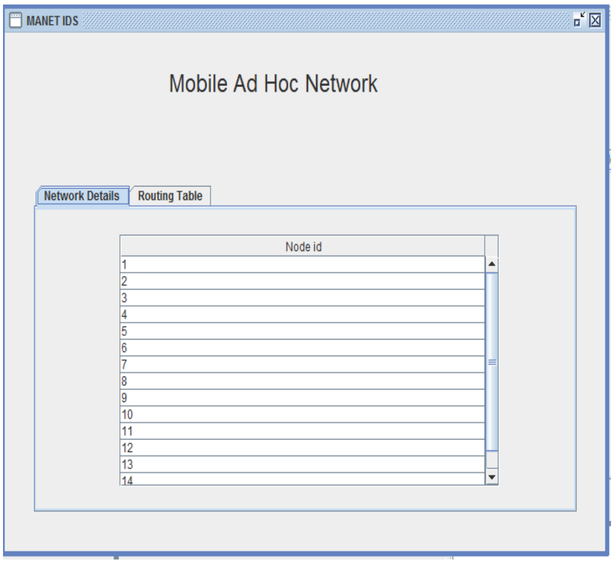
Node	Type of Attacks
8	DoS Attack

Figure 11- Senders response table



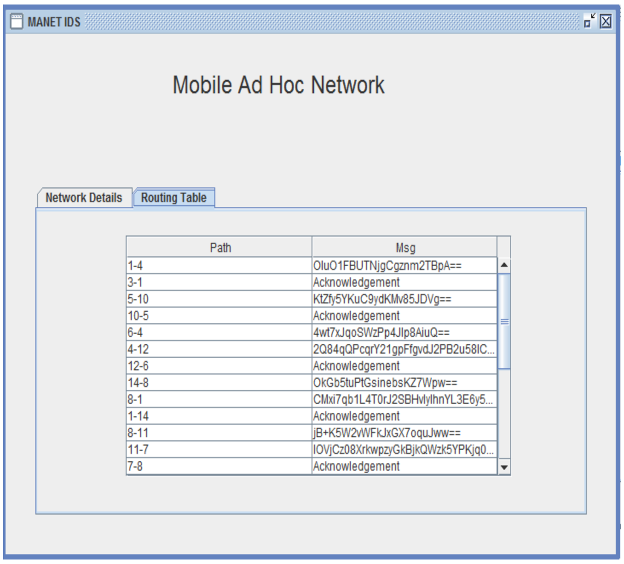
Path	Message
1-4	kavita
1-3-4	Alternate Path
4-1	Acknowledgement
14-2-1	ABC

Figure 12- Receivers routing table



Node id
1
2
3
4
5
6
7
8
9
10
11
12
13
14

Figure 13-Network Details



Path	Msg
1-4	OluO1FBUTNjgCgznm2TBpA==
3-1	Acknowledgement
5-10	KtZfy5YKuC9ydKMv85JDVg==
10-5	Acknowledgement
6-4	4wt7xJqoSWzPp4JIp8AiuQ==
4-12	2Q84qQPcqrY21gpFfgvdJ2PB2u58IC...
12-6	Acknowledgement
14-8	OkGb5tuPtGsinebsKZ7Wpw==
8-1	CMxi7qb1L4T0rJ2SBHvlylhnYL3E6y5...
1-14	Acknowledgement
8-11	jB+K5W2vWFkJxGX7oquJww==
11-7	IOVjCz08XrkwpzyGkBjkQWzk5YPKjq0...
7-8	Acknowledgement

Figure 14-Routing table

4. CONCLUSION

An Intrusion Detection System aiming the securing and monitoring the three important layers i.e. Transport layer, Network layer and data link layer has been developed using specification-based technique. It is based on a previous work done by Christoforos Panos, Christos Xenakis and Ioannis Stavrakakis [1]. From the results obtained, it can be concluded that this IDS can effectively detect the most critical types of attacks on this layers like DoS, session hijacking, etc. In the existing system malicious nodes are detected but it doesn't performs the retransmission by selecting another alternative path. Here I try my best for performing rerouting so that by skipping the malicious node communication can be completed.

5. REFERENCES

[1] Christoforos Panos, Christos Xenakis and Ioannis Stavrakakis,"A novel intrusion detection system for MANET", Proceedings of the International Conference on Security and Cryptography (SECRYPT), July 2010.

[2] Ketan Nadkarni and Amitabh Mishra," A Novel Intrusion Detection Approach for Wireless Ad hoc Networks", IEEE Communications Society, WCNC 2004.

[3] Hao Yang, Haiyun Luo, Fan Ye , Songwu Lu and Lixia Zhang," Security in mobile Ad-Hoc network: Challenges and Solutions", IEEE Wireless Communications, February 2004.

[4] Amitabh Mishra,Ketan Nadkarni and Animesh Patcha,Virginia Tech," Intrusion detection in wireless Ad-Hoc networks", IEEE Wireless Communications, February 2004.

[5] Djamel Djenouri and Lyes Khelladi ," A survey of security issues in mobile Ad-Hoc and sensor network", IEEE Communications Surveys & Tutorials, Fourth Quarter, 2005.

[6] Da Zhang, Chai Kiat Yeo," A Novel Architecture of Intrusion Detection System", IEEE CCNC proceedings, 2010.

[7] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi, Seung-Jo Han,” A Novel Cross Layer Intrusion Detection System in MANET”, 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[8] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C-Y. Tseng, T. Bowen, K. Levitt and J. Rowe, “A General Cooperative Intrusion Detection Architecture for MANETs”, Proceedings of the Third IEEE International Workshop on Information Assurance (IWIA’05), 2005.

[9] Sen, S., Clark, J. A.,” Intrusion Detection in Mobile Ad Hoc Networks Guide to Wireless Ad –Hoc Networks”, Springer, p. 427-454.2009.

[10] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami,” EAACK—A Secure Intrusion-Detection System for MANETs”, IEEE Transaction on Industrial Electronics, VOL. 60, NO. 3 MARCH 2013.

[11] Kavita Varule and Sachin Bojewar,” Evaluation of various IDS techniques for MANET”, ICETTA- March, 2014.

[12] Christoforos Panos , Ioannis Stavrakakis , Platon Kotzias , Christos Xenakis,” Securing the 802.11 MAC in MANETs: A Specification-based Intrusion Detection Engine”, 9th Annual Conference on Wireless On-demand Network Systems and Services (WONS), 2012.

[13] Adnan Nadeem and Michael P. Howarth,” A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER, 2013.

[14] Saleh Ali K.Al-Omari, Putra Sumari,” An Overview of Mobile Ad-Hoc Networks for The Existing Protocols and Applications”, International Journal on applications of graph theory in wireless ad hoc networks and sensor networks(Graph-Hoc),Vol.2,No.1,March 2010 .

[15] Elizabeth M. Royer, Santa Barbara Chai-Keong Toh,” A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, IEEE Personal Communications, April 1999.

[16] Kavita Varule, Sachin Bojewar,” An Intrusion Detection System for MANETs”, International Journal of Computer Applications (0975 – 8887) Volume 112 – No. 7, February 2015.

[17] Herve Debar,” An Introduction to Intrusion-Detection Systems”, IBM Research, Zurich Research Lab