International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

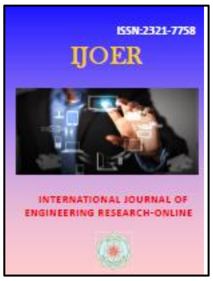
Vol.5., Issue.2, 2017
March-April

RESEARCH ARTICLE

ISSN: 2321-7758

A SECURE INTRUSION DETECTION SYSTEM FOR MOBILE ADHOC NETWORK

ADSUL R.D[1], Prof. SHAHA A.V[2]
[1]PG Student, Dept. of Electronics, D.K.T.E College, Ichalkaranji, India
[2]Assistant professor, Dept. of Electronics, D.K.T.E College, Ichalkaranji, India



ABSTRACT

In early years a Mobile Adhoc Network (MANET) is Gaining Popularity in research topics. It is possible to use Mobile Adhoc Network in various critical mission applications such as military due to its characteristics like mobility, scalability and self-configuring ability. As MANET is infrastructure less system and due to this open medium structure MANET is vulnerable to malicious attackers. In this case it is necessary to develop network security of MANET and in order to fulfil this requirement there is need to develop effective and efficient intrusion detection system to protect MANET from attackers in order to enhance the applications of MANET in Industrial area also. Here in the proposed work a secure acknowledgement based Intrusion detection system will be designed for MANET using signature technique. It will give higher malicious behaviour detection rates in certain circumstances while maintaining the improved throughput and minimum network overhead.

KEYWORDS: Mobile Adhoc Network (MANET), Intrusion Detection System (IDS), Enhanced Adaptive Acknowledgement based system (EAACK), ACK

I. INTRODUCTION

Mobile ad-hoc network (MANET) is a self-configuring network of wireless links connecting mobile nodes. The mobile nodes communicate directly with each other and without the aid of access points, and therefore have no fixed infrastructure. Its infrastructure less network and self-configuring capability makes it ideal for many critical applications. Due to mobility and scalability features of mobile nodes wireless network has gain advantage that to allow data communication between different parties and still maintain their mobility. Minimal configuration and quick deployment are some other characteristics of MANET. Due to these unique characteristics, MANET is becoming more and more widely implemented in industry.

Due to its open medium, changing topology and lack of centralized monitoring, the characteristics of MANET make it vulnerable to passive and active attacks. As MANET is popular for various critical mission applications, network security is of vital importance .Hence, security is now a major concern in many Manet's applications. Several intrusion detection systems have been proposed such as watchdog, TWOACK, AACK. The paper, EAACK—A Secure Intrusion-Detection System for MANETs has been reported by Elhadi M. Shakshuki [1].The intrusion detection system by introducing signature scheme to it in order to ensure the security in MANET.

II. SYSTEM MODEL AND ASSUMPTIONS

From the paper [10] the proposed block diagram of a secure Intrusion detection System EAACK scheme consists of three parts, which are

ACK, S-ACK and MRA & signature scheme is used at the time of packet transmission as shown in figure 1.

Here the Assumption is made that the link between each node in the network is bidirectional. Start with ACK mode, the function of source node is to forward the ACK data packet.

In ACK mode if packet transmission from source none S to destination D is not successful then node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes.

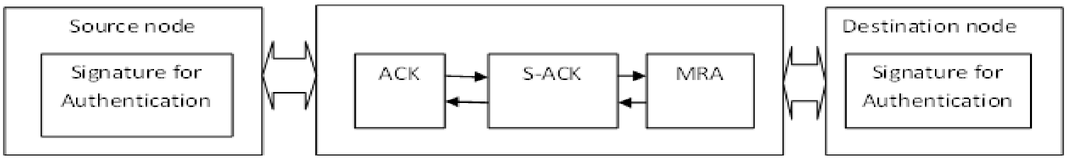


Figure 1: Block Schematic of EAACK Scheme

In S-ACK mode, the three consecutive nodes work in a group to detect misbehaving nodes in the network. If misbehaviour report is generated then it will send an MRA data packet otherwise it will send an ACK data packet.

To confirm this misbehavior report EAACK requires the source node to switch to MRA mode. When destination node receives an MRA packet it searches its local knowledge base and compares it to check whether the reported packet was received. If it is received then sends an ACK packet as the reporter is malicious and if it is not received then sends an ACK packet as trust the report. By using MRA scheme, EAACK is capable of detecting malicious nodes as specified in the paper [10].

Part 1- Acknowledgement (ACK) Mode: Part-1 focuses on implementation of Acknowledgement mode for detecting malicious node and in order to reduce network overhead. The experimental procedure followed for Acknowledgement mode is as shown in flow chart of Acknowledgement scheme of figure 2.1.

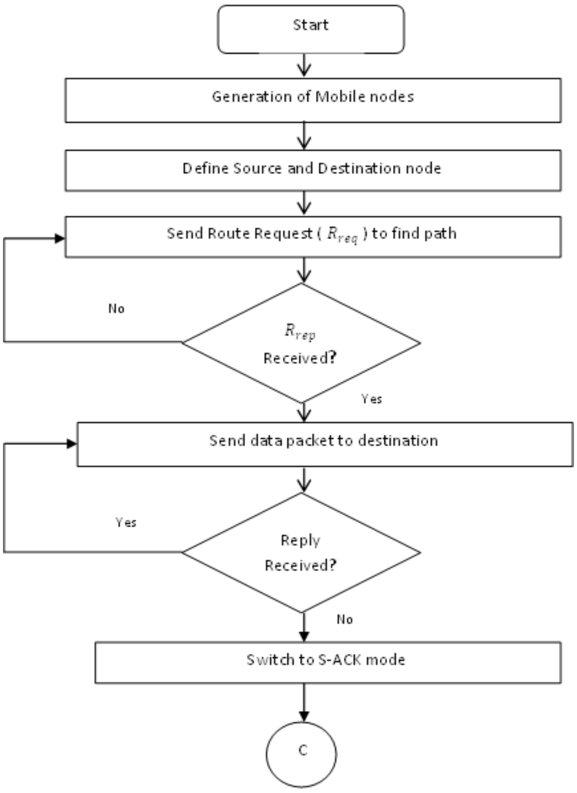

Start
Generation of Mobile nodes
Define Source and Destination node
Send Route Request (R_{req}) to find path
No
R_{rep}
Received?
Yes
Send data packet to destination
Yes
Reply
Received?
No
Switch to S-ACK mode
C

Figure 2.1: Acknowledgement Scheme

In order to carry out communication in Mobile Adhoc Network by using Network Simulator-2 (NS-2), the first step is to generate the mobile nodes. Here we generate 50 stationary mobile nodes by considering the assumption that the nodes are bidirectional.

Then we define source node and destination node for performing communication. To identify these nodes we define source node by magenta colour and destination by orange colour. Here for communication we used DSR protocol therefore in order to communication the source node broadcasts the route request to all other neighboring nodes in order to find the shortest path for communication.

After broadcasting the route request the source node waiting for the route reply from destination node. When source node receives the route reply from destination node which gives the information regarding forwarding nodes in the path; the source node sends an ACK data packet to the destination otherwise the source node checks its knowledge database for alternative path and if there is no path present then source node again broadcasts the route request to find forwarding path.

After sending the ACK data packet to the destination node the source node has to wait for the ACK Acknowledgement packet from destination node. If the destination node receives the ACK data packet send by the source node then it sends back an ACK acknowledgement packet to the source node after verifying the packet with reference to signature.

If destination node do not receives the ACK data packet within a predefined time it means a misbehaving node is present in the path therefore the system will switch to the S-ACK mode in order to find out the misbehaving node present in the path.

Part 2- Secure-Acknowledgement(S-ACK) Mode: Part-2 focuses on implementation of Secure-Acknowledgement mode for detecting malicious node and in order to reduce the weaknesses of Watchdog scheme. The experimental procedure followed for Secure-Acknowledgement scheme is as shown in figure 2.2.

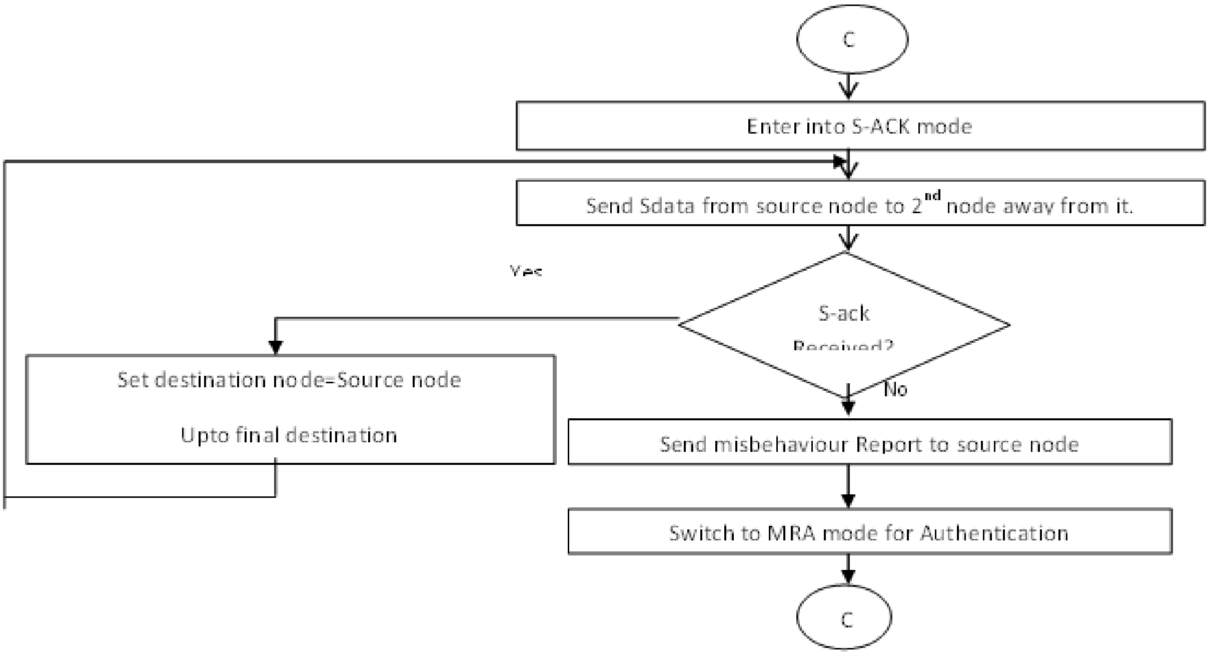

C
Enter into S-ACK mode
Send Sdata from source node to 2nd node away from it.
Yes
S-ack Received?
No
Set destination node=Source node
Upto final destination
Send misbehaviour Report to source node
Switch to MRA mode for Authentication
C

Figure 2.2: Secure-Acknowledgement Scheme

Here in order to check and detect whether any malicious node is present or not in forwarding path the scheme enters into the S-ACK mode which is 2nd mode of EAACK scheme. This scheme works in a group of three nodes; hence for that we make a group of three nodes in the network.

In this mode the source node sends an Sdata packet to the node which is two hops away from it and wait for the S-ACK Acknowledgement packet from that destination node in a predefined time period. The node which is two hops away from source node 1 receives S-data; it sends back an S-ACK acknowledgement packet to the source node.

After this successful transmission it make a group of next three nodes; that means the destination node in previous transmission is set as source node and the destination node is two hops away from it. The transmission process is carried out in the same way.

If the source node do not receives S-ACK acknowledgement packet from the set destination node in a predefined time period then the source node generates misbehavior report and sent it to the earlier source node and the scheme switches to the misbehavior Report Authentication (MRA) mode for authentication of the report generated by the node. Here time period is set to 0.25sec.

Part 3- Misbehavior Report Authentication(MRA) Mode:

Part-3 focuses on implementation of Misbehavior report Authentication mode for Authentication of misbehavior report in presence of false misbehavior report. The experimental procedure followed for Misbehavior Report Authentication is as shown in figure 2.3.

Here in order to authenticate the misbehavior report generated by the S-ACK scheme the EAACK enters into the MRA mode which is third mode of EAACK scheme.

In this mode the source node checks its database for finding an alternative path in order to send MRA_Chk packet to verify that whether the received misbehavior report is true or false.

The source node employs the path from its database and if no alternative path is available in its database then source node broadcasts the route request in order to find the forwarding path.

The MRA_Chk packet is forwarded towards the destination node by employing a forwarding path. When destination node receives an MRA_Chk packet it searches its database to check whether that data packet is received or not.

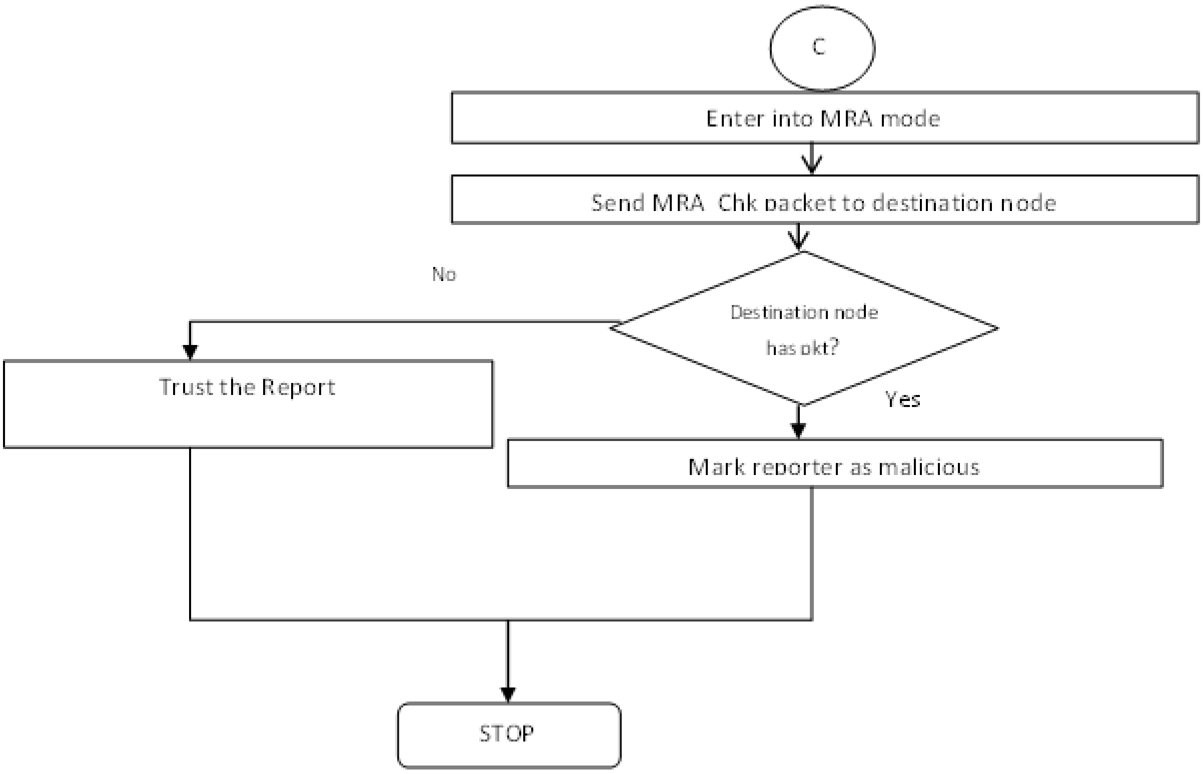


Figure 2.3: Misbehaviour Report Authentication Scheme

If the data packet is already received to the destination node then the system reported after the verification that the reporter node is malicious and it has been sent a false misbehaviour report. Whereas if the data packet is not received to the destination node then the system reported after the verification that the reporter node is not a malicious node and it has been sent a true misbehaviour report and trust the report.

III. RESULTS AND DISCUSSION

For simulation of EAACK system we choose Network Simulator NS2.35 environment and ubuntu 14.04. To measure the performance of EAACK system, we evaluate Packet Delivery Ratio (PDR) and Routing overhead (RO) in three different scenarios:

Table 1: Scenario 1: PDR & RO

Malicious Scenario 1: Packet Delivery ratio					
	Malicious Nodes: 0%	Malicious Nodes: 10%	Malicious Nodes: 20%	Malicious Nodes: 30%	Malicious Nodes: 40%
EAACK	1	0.94287	0.9	0.871429	0.871429
Malicious Scenario 1: Routing Overhead					
EAACK	0.137011	0.186715	0.20696	0.217228	0.217228
Malicious Scenario 2: Packet Delivery ratio					
EAACK	1	0.942857	0.9	0.871429	0.871429
Malicious Scenario 2: Routing Overhead					
EAACK	0.137011	0.186715	0.20696	0.217228	0.217228
Malicious Scenario 3: Packet Delivery ratio					
EAACK	1	0.942857	0.9	0.871429	0.871429
Malicious Scenario 3: Routing Overhead					
EAACK	0.137011	0.195671	0.223443	0.2397	0.2397

a) **Scenario 1:** In this scenario, the malicious node drop all data packets which are pass through it. This scenario is considered to test the performance of our EAACK system against the two weaknesses of watchdog system which is Receiver collision and limited transmission power. The simulation results on Packet Delivery Ratio (PDR) and Routing Overhead (RO) are as given below:

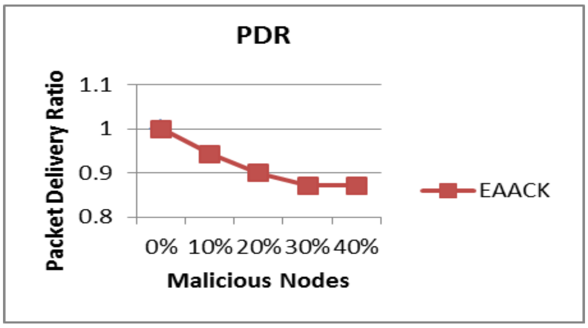


Figure. 3.1: Scenario 1-Packet Delivery Ratio

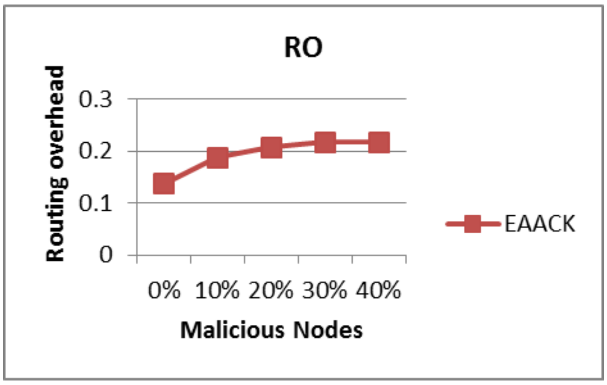


Figure.3.2: Scenario 1-Routing Overhead

The Figure 3.1 and 3.2 shows that our proposed scheme EAACK decreases the packet delivery ratio in case of increased malicious nodes; while in case of routing overhead the proposed scheme produces very low network overhead..

b) Scenario 2: In this scenario, the nodes are smart enough that whenever they receive packets, they drop it and send back a malicious report to the source node. The simulation results on Packet Delivery Ratio (PDR) and Routing Overhead (RO) are shown in figure below:

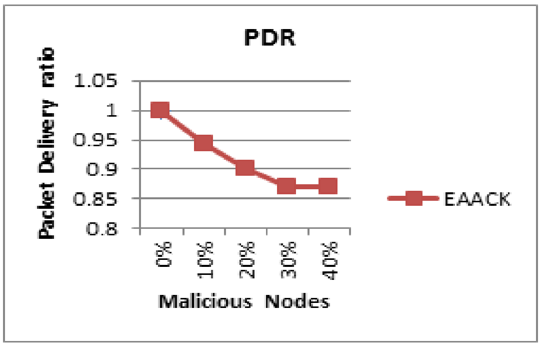


Figure 3.3: Scenario 2: Packet Delivery Ratio

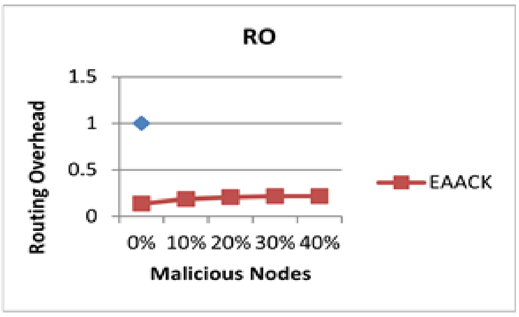


Figure 3.4: Scenario 2: Routing Overhead

The Figure 3.3 and 3.4 shows that in case of Packet Delivery ratio our proposed scheme EAACK produces the same PDR though the number of malicious nodes are increases; while in case of routing overhead our proposed scheme still produces very low network overhead.

c) Scenario 3:

This scenario is designed to test the ability to test forged acknowledgement packet. The simulation results on Packet Delivery Ratio (PDR) and Routing Overhead (RO) are shown in figure below:

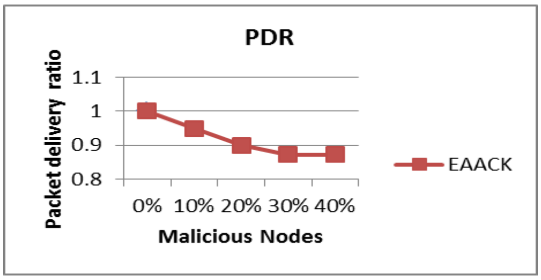


Figure 3.5: Scenario 3: Packet Delivery Ratio

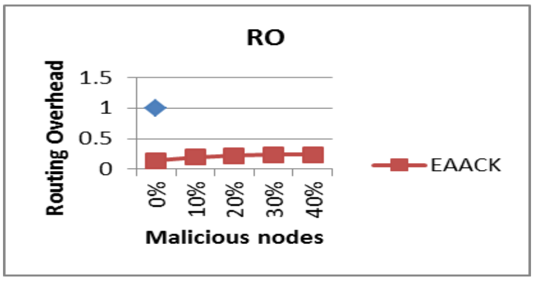


Figure 3.6: Scenario 3: Routing Overhead

The Figure 3.5 and 3.6 shows that in case of Packet Delivery ratio our proposed scheme EAACK produces the same PDR; while in case of routing overhead our proposed scheme still produces very low network overhead.

IV.CONCLUSION

In mobile Adhoc network a packet dropping attack has been a most dangerous problem for the security of MANET. In order to prevent and eliminate the packet dropping attack various different approaches were designed. An acknowledgement based intrusion detection system is one of the most important techniques against the packet dropping attacks. The performance of EAACK system has been tested through network simulator 2 (NS2). The Performance result shows that the EAACK has high packet delivery ratio among all the three malicious test scenarios. Also it reduces the routing overhead to a minimum level.

V. References

[1]. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE, "EAACK—A Secure Intrusion-Detection System for MANETs," IEEE transactions on industrial electronics, vol. 60, no. 3, march 2013.

[2]. D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[3]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw. Boston, MA, 2000, pp. 255–265

[4]. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[5]. T.Sheltami, A.Al-Roubaiey, E.Shakshuki, and A.Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[6]. Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[7]. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key crptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1983.

[8]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. ii WAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.

[9]. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[10]. Ms. Rasika D. Adsul, Prof. A. V. Shaha, "A Review on A Secure Intrusion Detection System for Mobile Adhoc Network", IJSRD, Vol. 4, Issue 08, 2016, ISSN:2331-0613.