ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Securing Mobile Ad Hoc Networks with Intrusion Detection System: A Review

Dipamala Nemade[1], Ashish T. Bhole[2]

Post Graduate Student, Department of Computer Engineering, SSBT's COE & T, Jalgaon, Maharashtra, India[1]

Associate Professor, Department of Computer Engineering, SSBT's COE & T, Jalgaon, Maharashtra, India[2]

Abstract:From past few years, wireless networks are mostly preferred because of its mobility and scalability characteristics. Mobile Ad hoc network (MANET) is one of such wireless communication mechanisms. A MANET is an infrastructure-less network consisting of self-configuring mobile nodes connected by wireless link. The nodes communicate with each other directly or indirectly with the help of neighbours to store and forward packets. The open medium and wide distribution of nodes makes MANET vulnerable to malicious attacks. To address the security, it is essential to develop an Intrusion Detection System (IDS) specially designed for MANET which can detect malicious attacks before they do any significant damage to the network. For this concern a secure intrusion detection system, EAACK is developed which solves the limitations of earlier systems. The proposed system evaluates EAACK with AODV routing protocol thereby providing better performance for large size MANET.

Keywords: Wireless network security, Mobile Ad Hoc Network (MANET), Intrusion Detection System (IDS), EAACK, AODV

I. INTRODUCTION

The MANET is a highly challenging network environment due to its unique characteristics such as decentralization, dynamic topology and neighbour based routing. Mobile Ad-hoc Network (MANET) consists of group of wireless mobile nodes that communicate with each other via bidirectional wireless links [1] without any fixed infrastructure. Mobile nodes are equipped with a wireless transmitter and a receiver that communicate directly with each other or forward message through other nodes [2]. One of the key advantages of wireless networks is its ability to agree data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is outside the communication range of their own. MANET solves this difficulty by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multi hop [3]. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi hop network, nodes rely on other intermediate nodes to transmit if the destination node is not in their radio range. MANET is infrastructure less network, thus all nodes are free to move remotely. MANET is able to creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery [3].The topology of MANET may change uncertainly and speedily due to high mobility of the independent mobile nodes. Also due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs [4]. An intrusion detection system does not include preventing the intrusion from occurring; it can only be detected and reported to each node in network [5]. Intrusion detection can be classified based on data as either host based or network-based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. Packet Drop attack is one of the most important security problems in Mobile adhoc network [2].Both routing packets and data packets forwarding function would be affected in the presence of misbehavingnodes. The node misbehaviour can be classified as malfunctioning, selfish and malicious. Malfunctioning nodes suffer from hardware or network failures. Selfish nodes refuse to forward or drop data packet. Malicious nodes use their resource and aims to fail other nodes or whole network, by trying to participate in all established routes thereby forcing other nodes to use a malicious route which is under their control [3].

The Figure 1 shows each incoming packet is dropped by malicious node in network

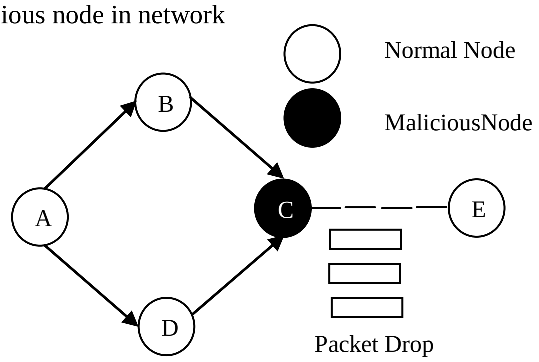

Figure1. Packet Drop Attack by Malicious Node

DOI 10.17148/IJARCCE.2015.4337

The source node A is trying to establish a connection to destination node E. Node A broadcast RREQ message, Node B and D receives RREQ and update a route to its previous hop and send RREQ to Node C. Node C is a malicious node which drops the received request so node A cannot communicate with node E. In this way Node C receives any packet will not forward and drop all the packets. One of the fundamental challenges of MANETs is the design of dynamic routing protocols with good performance and less overhead [6]. In mobile ad hoc networks, the major role is played by routing protocols in order to route the data from one mobile node to another. Due to the limited wireless transmission range, the routing generally consists of multiple hops. These routing protocols are having the functionality of forwarding the data packets from sender to the intended recipient. In such type of networks routing is mostly challenging because typical routing protocols do not operate efficiently in the presence of frequent movements. Mobile Ad-Hoc network routing protocols are commonly divided into three main types Proactive, Reactive and Hybrid protocols [7].

i) Proactive Protocols

This type of routing protocol, maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. An example of proactive routing protocol is Destination sequenced distance vector (DSDV).

ii) Reactive Protocols

This type of routing is also known as on-demand routing protocol. If a node wants to send a packet to another node then this protocol finds the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing (DSR).

iii) Hybrid Protocols

This type of routing protocol combines the advantages of reactive and proactive routing protocols. Examples of Hybrid routing protocols are ZRP [6].

The related work is discussed in section II. Section III elaborates the proposed work and conclusion is derived in section IV.

II. Related work

The section provides an overview of the background information and related work that is important for the understanding of proposed system. The existing Intrusion Detection Systems for MANET is briefly introduced, which are used for detecting malicious nodes andmitigating routing misbehaviour. The respective strengths and weaknesses are also discussed.

A. Literature Survey

The various techniques that have been applied to detect malicious node in network are discussed in this section. Following are several different approaches for intrusion detection system.

S. Marti, T. J. Giuli, K. Lai, and M. Baker [8] proposed a watchdog and pathrater scheme of intrusion detection system for MANET is introduced that aims to improve the throughput of network with the presence of malicious nodes [12]. Watchdog is able to detecting malicious nodes rather than links. The watchdog is based on reactive feedback that is overhearing to confirm whether the next node has forwarded the packet or not. Pathrater works as response system. Once Watchdog node identifies malicious node in the network, the pathrater cooperates with the routing protocols to avoid the reported node in the future transmission. The standard is Dynamic Source Routing protocol (DSR) in that the routing information is defined at the source node [2].So because of this it might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehaviour report, collusion and partial dropping.

N. Nasser and Y. Chen [9] proposed ExWatchdog which extends from Watchdog proposed in that solving the problems of the Watchdog scheme which is the false misbehaving problem, where a malicious node falsely reports other nodes as misbehaving while in fact it is the real intruder. When the source receives a report about misbehaving node, it will find another path to ask the destination node about the number of received packets. If it is equal to the packets that the source has sent, then the real malicious node is the node that reports other nodes as misbehaving. Otherwise node being reported malicious do misbehave. But there is limitations in this scheme if the true misbehaving node is in the all available paths from source to destination then it is impossible to confirm and check the number of packets with the destination.

K. Liu, J. Deng, P. K. Varshney and K. Balakrishnan [10] proposed a TWOACK scheme which aims to solve the problem of receiver collision and limited transmission power of Watchdog. TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from source to destination. But the acknowledgment process required in every packet transmission process added a considerable amount of unwanted network overhead.TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) [12].

Al-Roubaiey, T. Sheltami, A. Mahmoud , E. Shakshuki and H. Mouftah [11] proposed a AACK is a network layer acknowledgement based scheme which detects misbehaving node instead of misbehaving link and an end to end acknowledgment based scheme, to reduce the routing overhead of TWOACK. The AACK scheme may not work well on long paths that will take a significant time for the end to end acknowledgments. This limitationwill give the misbehaving nodes more time for dropping more packets. AACK still suffers from the partial dropping attacks and false misbehaviour report.

N. Kang, E. Shakshuki and T. Sheltami [3] proposed EnhancedAdaptive Acknowledgment scheme which consist of three parts Acknowledgment, Secure-

Acknowledgment, misbehaviour report authentication. This scheme is capable of detecting malicious nodes despite the existence of false misbehaviour report.

Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami [1] proposed EAACK scheme with digital signature to prevent the attacker from forging acknowledgment packets.All acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver, because of that it causes the network overhead.

DurgeshWadbude and VineetRichariya [13]proposed secureAd hoc On Demand Distance Vector Routing (AODV) a novel algorithm for the operation of such ad hoc networks. Each Mobile node operates as a specialized router and routes are obtained on demand.

After overviewing two intrusion detection techniques watchdog and TWOACK, the AACK still suffer from the problem thatthey fail to detect malicious nodes with the presence of falsemisbehavior report. So, the proposed EAACK system is designed to solve the problem of false misbehavior report.

B. Comparative Study of IDS Techniques

The comparison of reviewed intrusion detection techniques used to detect malicious nodes in MANET is shown in Table 1. The Table 1 also discuss strengths and weaknesses of respective IDS technique.

The discussion in related work section and Table 1 confirms that existing techniques cannot solve the problem of receiver collision, limited transmission power and false misbehaviour report. The existing EAACK system makes use of DSR routing protocol. As the network size increases, the performance of DSR is affected due to dynamic nature of MANET. Therefore the existing EAACK intrusion detection system can be evaluated with proposed AODV routing protocols in MANET.

III. Proposed Work

The section describes proposed EAACK scheme using AODV routing protocol that can give better than DSR performance for network of large size. The proposed work assumes the links between nodesto be bidirectional.

C. System Design

The proposed system approach of EAACK is designed to deal with three of six limitations of previous schemes, particularly, false misbehaviour, limited transmission power, and receiver collision. The EAACK system consists of following parts. Figure 2 shows system architecture of EAACK.

- ACK
- Secure Acknowledgment (S-ACK)
- Misbehavior Report Authentication (MRA)

TABLE I
Comparison of Intrusion Detection Systems for MANET

Name of Intrusion Detection System (Year)	**Algorithm / Protocols**	**Strengths**	**Weaknesses**
Watchdog and Pathrater (2000)	Dynamic Source Routing Protocol	Improves the throughput of network with the presence of malicious nodes.	Fails to detect malicious misbehaviours with the presence of ambiguous collisions receiver collisions limited transmission-power false misbehaviour-report collusion partial dropping
TWOACK (2007)	Dynamic Source Routing Protocol	Solves the receiver collision and limited transmission power problems of Watchdog.	The acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead
AACK (2010)	Dynamic Source Routing Protocol	Compared to TWOACK, AACK significantly reduces network overhead while still capable of maintaining or even surpassing the same network throughput	It is crucial to guarantee that the acknowledgment packets are valid and authentic.
EAACK (2013)	Digital Signature algorithm and DSR	i. Solves the three weaknesses of Watchdog scheme, false misbehaviour, limited transmission power and receiver collision ii. Prevents the attacker from forging acknowledgment packets	This scheme produces more routing overhead if numbers of malicious nodes are increased.

DOI 10.17148/IJARCCE.2015.4337

i) ACK

In the ACK, the aim is to reduce the network overhead when no network misbehaviour is detected. It is anend to end acknowledgment scheme. The basic flow is, if Source node S sends an ACK data packet P_{ad1} to destination Node D, and if all the intermediate nodes between S to destination node D are cooperative and successfully receives the P $_{ad1}$, then for node D it is necessary to send back ACK acknowledgment packet P_{ack1} from the same route but in reverse order. If the P_{ack1} packet is received to node S in the predefined time period, then the packet transmission is successful from source node S to destination node D. Otherwise it switch to S-ACK mode and send out S-ACK data packet to detect misbehaving node in the route.

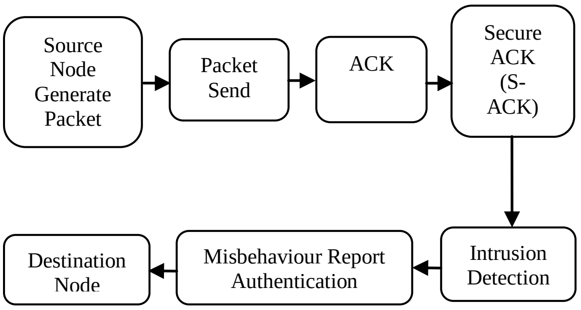

Figure2. Architecture of Proposed System

ii)Secure acknowledgment (S-ACK)

In the S-ACK, the principle is to allow every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send back an S-ACK acknowledgment packet to the first node. The purpose of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power

iii) Misbehaviour report acknowledgment (MRA)

This MRA scheme is designed to resolve the limitations of watchdog where it fails to detect the misbehaving node with the presence of false misbehaviour report. This false misbehaviour report can be generated by the attackers by reporting falsely for the innocent nodes as malicious. The goal of MRA scheme is to authenticate whether the destination node has received the reported missing packet from a different route.

In the MRA mode source node find for a alternate route to the destination node. If there is no other route is exists, the source node starts a AODV routing request to find another route. By adopting the alternate route for the destination node then it can avoid the misbehaviour reporter node. When the destination node receives the MRA packet it searches it's knowledge base and compares to that the reported packet was received or not, if it is already received then it conclude that this is a false misbehaviour report and whoever send it, is marked as malicious. Otherwise the false misbehaviour report is trusted and accepted.

The Figure 3 shows an attack scenario. The source node S sends ACK data packet to Destination node D, then for node D it is necessary to send back ACKacknowledgment packet to S. If packet is not received in predefined time period then it switches to S-ACK mode and send out S-ACK data packet to detect misbehaving node in the route. In S-ACK mode it detects two misbehaving nodes in network. In MRA mode it authenticate whether the destination node has received the reported missing packet from a different route and also it finds out the real malicious node in network.

D. General Flow of Proposed System

The section discusses the algorithmic steps of proposed system which will elaborate on how the EAACK system will be implemented using AODV routing protocol

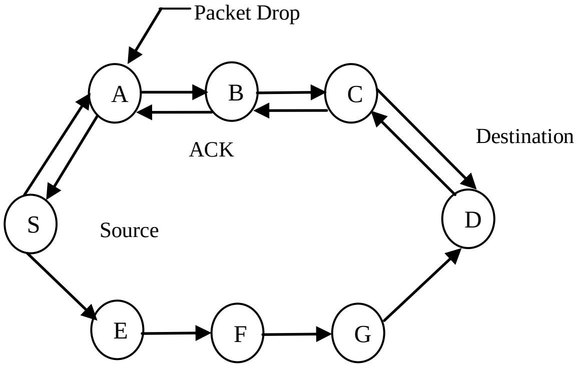

Figure3. Attack Scenario in MANET

i)Algorithm for Proposed System

```
Step 1: The source node broadcasts a RREQ packet to find a route to the destination across node
Step 2: If (RREQ seq. No<= Corresponding RREQ Seq. No)
RREP packets send back to source node
Else
Rebroadcast the RREQ packet across node
Step 3: If RREP received from all nodes then
        Source updates routing information
        Else
        Send RERR Packet when link fail
Step 4: Send packet to Destination
Step 5: If Received ACK packet then,
        Reached packet at destination successfully
 Else
        Switch to S-ACK packet mode
Step 6: If get Misbehaviour Report then
          Switch to MRA packet mode
        Else
        Send ACK Packet to Source node
Step 7: If Send Packet ID== Received Packet ID
        Mark Reporter as Malicious
Else
        Trust the Report
Step 8: Send ACK Packet to Source node
Step 9: Calculate Packet Delivery Ratio (PDR)
Step 10: End
```

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

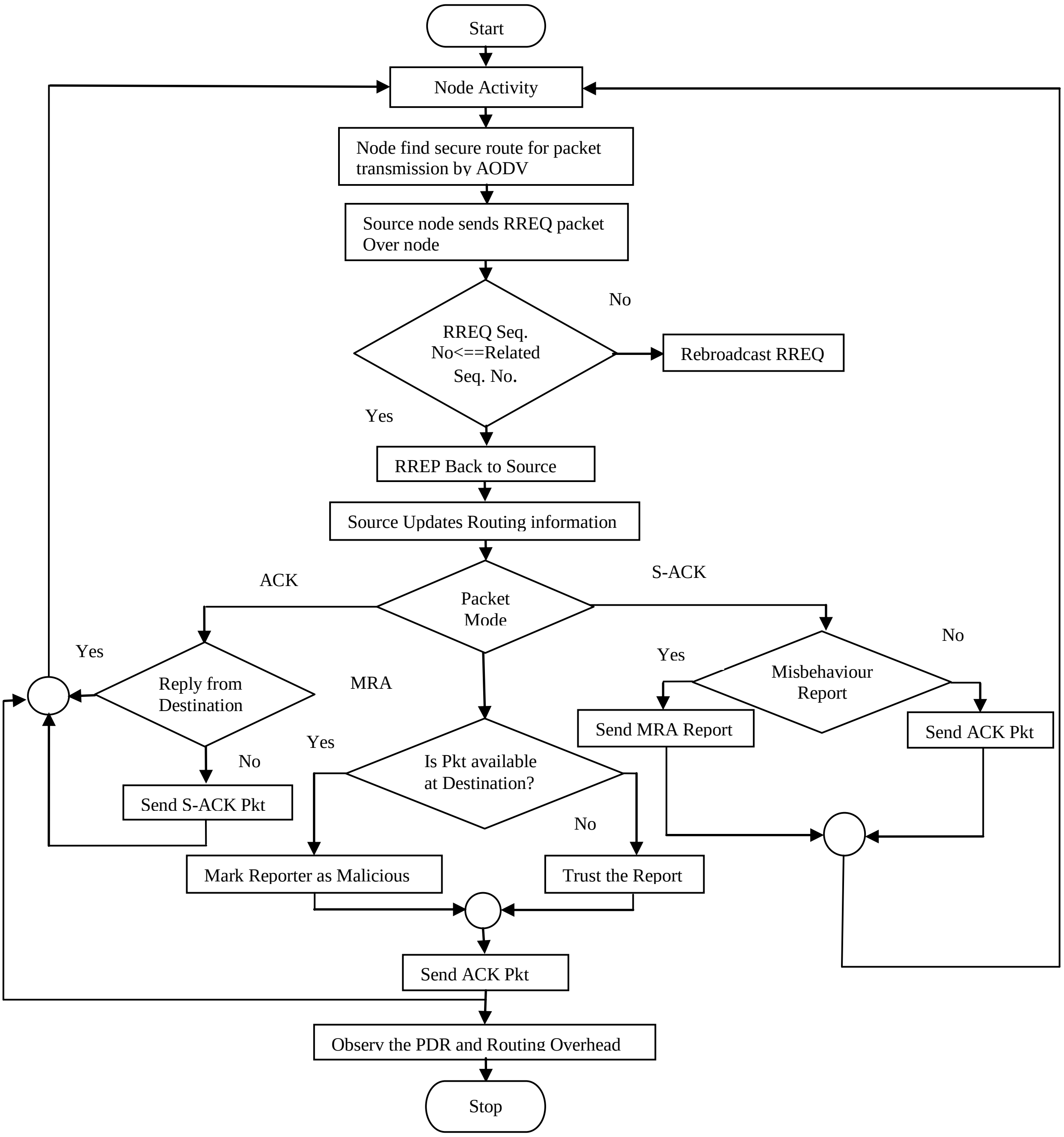
Start
Node Activity
Node find secure route for packet transmission by AODV
Source node sends RREQ packet Over node
RREQ Seq. No<==Related Seq. No.
No
Rebroadcast RREQ
Yes
RREP Back to Source
Source Updates Routing information
ACK
Packet Mode
S-ACK
Yes
Reply from Destination
No
Send S-ACK Pkt
MRA
Yes
Misbehaviour Report
No
Send MRA Report
Send ACK Pkt
Yes
Is Pkt available at Destination?
No
Mark Reporter as Malicious
Trust the Report
Send ACK Pkt
Observ the PDR and Routing Overhead
Stop

Figure4. General Flow of Proposed System

The Figure 4 shows flow of proposed system. The EAACK system uses AODV routing protocol for large area network that find the secure route on demand for data transmission and also detect the misbehaving node in the network.

The performance of proposed work can be analysed and compared in terms performance metrics such as Packet delivery ratio and Routing overhead. Packet delivery ratio (PDR) defines the efficiency of the network and hence signifies the efficiency of the routing protocol used. The Packet delivery ratio (PDR) is computed as shown in Equation (1).

$$PDR = \frac{\text{Number of Received Packet}}{\text{Number of Sent Packet}} \quad \text{.......... (1)}$$

Routing overhead (RO)defines the ratio of the amount of routingrelated transmissions. It also signifies the stressthat a specific protocol offers. The Routing overhead (RO) is computed as shown in Equation (2).

$$RO = \frac{\text{NumberofRoutingPacketsSent}}{\text{NumberofDataPacketSent}} \quad \text{..........(2)}$$

The proposed work is implemented for varying number of nodes and number of misbehaving nodes for different scenarios and compares the performance in terms ofpacket delivery ratio and routing overhead in EAACKsystem using AODV protocol.

DOI 10.17148/IJARCCE.2015.4337

IV. CONCLUSION

The packet drop attack by malicious node has always been a major threat to the security in MANET. The proposed system focuses on detection of malicious node by authenticating misbehaviour report from MRA. The existing EAACK uses DSR routing protocol for network of small scale. As the network size increases due to dynamic nature of MANET, the performance of DSR protocol affects. Hence the proposed system uses EAACK with AODV routing protocol which can give better than DSR performance for large size networks in MANET.

REFERENCES

[1] Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami, " EAACK –A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, pp. 1089-1098, March 2013.

[2] Anantvalee, Tiranuch and Jie Wu., "A survey on intrusion detection in mobile ad hoc networks", in Wireless Network Security, pp. 159-180, Springer US, 2007.

[3] Kang, Nan, Elhadi M. Shakshuki, and Tarek R. Sheltami,"Detecting misbehaving nodes in MANETs", in Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services, pp. 216-222, ACM, 2010.

[4] Ranjitj. Bhosale and Prof. R.K.Ambekar, "A Survey on Intrusion detection System for Mobile Ad-hoc Networks", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5, No. 6, pp. 7330-7333, 2014.

[5] Ashish T. Bhole and Archana I Patil, "Intrusion Detection with Hidden Markov Model and WEKA Tool", International Journal of Computer Applications (IJCA), Vol. 85, No. 13, pp. 27-30, Jan 2014.

[6] M.Saravanan andD.Jagan, "A Neighbor Knowledge with Zonal Routing Protocol to Reducing Routing Overhead in MANETs", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5, No. 3, pp. 3503-3507, 2014.

[7] Prachee N. Patil and Ashish T. Bhole, "Black hole attack prevention in mobile Ad Hoc networks using route caching", in 10thIEEE International Conference on Wireless and Optical Communications Networks (WOCN), pp. 1-6, July 2013.

[8] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-265, ACM 2000.

[9] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network", in IEEE International Conference on Communications (ICC'07), pp. 1154-1159, Jun 24–28, 2007.

[10] K. Liu, J.Deng, P. K. Varshney and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs", IEEE Transactions on Mobile Computing, Vol. 6, No. 5, pp. 536–550, May 2007.

[11] Al- Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki and H. Mouftah, "AACK-Adaptive Acknowledge Intrusion Detection for MANET with Node Detection Enhancement", in 24thIEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 634-640, 2010.

[12] U. SharmilaBegam and Dr. G. Murugaboopathi, "A Recent Secure Intrusion Detection System for MANETs", International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol. 3, Special Issue 1, pp. 54-62, January 2013.

[13] DurgeshWadbude and VineetRichariya, "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, Issue 4, pp. 274-279. April 2012.

DOI 10.17148/IJARCCE.2015.4337