International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

Academic Science

Detecting Multiple Malicious Node in Mobile Adhoc Network (MANET)

Soni Priti R.
PG Student, EXTC Department,
Datta Meghe College of Engineering Airoli,
Navi Mumbai, India

Dr. S.R. Devane
Head of IT Department,
Datta Meghe College of Engineering Airoli,
Navi Mumbai INDIA

Abstract

Security of network is a challenging assignment in MANET due to active topology and decentralized control. Therefore it is important to develop suitable intrusion detection scheme (IDS) to protect MANET from malicious attackers .As many Intrusion Detection Systems (IDSs) for MANETS rely on the Watchdog technique. To prevent the attackers from forging the acknowledgement packets and to solve the issues regarding receiver collision, limited transmission power and false misbehavior problem of watchdog scheme an innovative Intrusion-detection system named modified Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to existing approaches, EAACK determines higher Malicious Behavior of nodes and provides better the network performances.

Keywords: Enhanced Adaptive Acknowledgment (EAACK), Mobile Adhoc Networks (MANET)

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of nodes equipped with transmitter and a receiver that communicate with each other via bidirectional wireless link. They can communicate either directly or indirectly. These nodes are constrained in power consumption, bandwidth, and computational power. MANETs has decentralized monitoring system, so the security concerns are different than that of wired networks [1]. As there is no any physical connection in between nodes, So MANETs are more susceptible to attacks The major attacks in MANETs are denial of service, eavesdropping, impersonation, man in the middle, warm hole , grey hole attacks [2]. Most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious Therefore, only one compromised node can cause the failure of the entire network [4]. Here we work on detection of two malicious nodes in MANETs. MANETs are classified in to two groups: closed and open. In a closed MANET, all mobile nodes cooperate with each other towards a common goal, such as emergency search/ rescue or military and law enforcement operations. In an open MANET, various mobile nodes with different goals share their resources for global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called misbehaving nodes and their behavior is termed as misbehavior [5].

II. BACKGROUND

IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches. Anantvalee and Wu presented a very thorough survey on contemporary IDSs in MANETs. So it is vital to address its security issues. Such existing IDSs in MANETs are Watchdog, TWOACK and AACK.

Watchdog [7] enhances the rate of production of the network even in the presence of attackers. It has two parts namely Watchdog and Path rater. It detects malicious nodes by overhearing next hop's transmission. A timer is initiated if the next node fails to forward the data packet. When the timer value surpasses a predefined threshold, the node is marked as malicious. The major drawbacks are ambiguous collision, receiver collision, limited transmission power, false misbehavior report, partial dropping and collusion.

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

TWOACK [8] checks the receiver collision and limited transmission power limitation of Watchdog. Here acknowledgment of every data packet over every three consecutive nodes is sent from source to destination. If ACK is not received in a predefined period, the other two nodes are marked as malicious. It is essential to works on routing protocols such as Dynamic Source Routing (DSR)[9] The major drawbacks are increased overhead, limited battery power and degrade the life span of entire network.

In earlier methods all the IDS detects malicious node in case of all misbehaving scenario such as ambiguous collision, receiver collision, limited transmission power, false misbehavior report and partial dropping except collusion. Incollusion attack if there are two malicious nodes in path, the second node can send acknowledgment dropping the data packet. The next node will not get the data packet but the 1st malicious node never reports the misbehavior of second node because both nodes are malicious. In this case these methods failed to detect the malicious misbehavior. Even if there is one malicious node in the path and the malicious node if does not send the acknowledgement back then the node report next two node as malicious even if the next node is not malicious node. The proposed method detects malicious node in all above misbehaving activities along with it, it provides high level of packet security using RSA and DSA which makes the proposed IDS better with respect to many aspects for MANET.

III. PROPOSED SYSTEM DESCRIPTION

The proposed scheme is designed to address the issues of watchdog such as receiver collision, limited transmission power, and false misbehavior of node. The focusis on detection of multiple malicious nodes in collision attack.

A. Design and Implementation

In this section, we propose a strong and light-weight enhanced Intrusion detection mechanism called EAACK protocol using digital signature which requires less cost, low power. EAACK is consists of three major parts called: ACK, S-ACK and MRA (misbehavior report authentication). In order to distinguish different schemes, we included a 2-bit packet header in EAACK. e.g.For general data 00, ACK 01 , S-ACK 10 , MRA 11.

Figure 1 presents flowchart describing the EAACK scheme. Please note that, in our proposed scheme, we assume that the link between each node in the network is bidirectional land for each communication process both the source node and the destination node are not malicious. Unless specified, all acknowledgment packets are required to be digitally signed by its sender and verified by its receiver. ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. According to this method, Refer Fig-1, If the receiver node does not send the ACK within predefined period, then ACK

assumes malicious may present and switch to S-ACK part to detect them. In S-ACK part, for every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first nodeThe intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. If malicious found, then MRA part suggests alternate path to the destination. Unlike theTWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA node and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

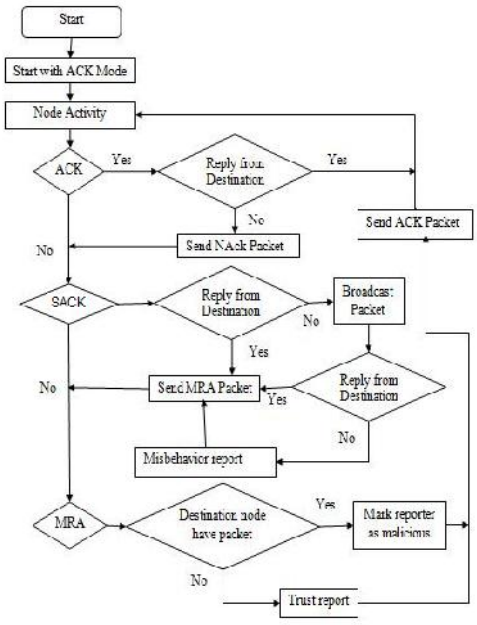

Fig.1 System control flow of EAACK scheme

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

1. ACK

As discussed before, ACK is basically an end-to-end acknowledgment scheme. In EAACK it aims to reduce network overhead when no network misbehavior is detected.

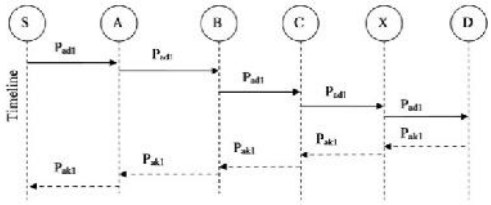

Fig2.ACKScheme.

In Figure 2, in ACK mode, node S first sends out an ACK data packet Pad1 to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along the same route but in a reverse order. Within a predefined time period, if node S receives Pak1, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

2.*S-ACK*

Suppose there is path from source to destination which contains malicious node that forward the control packets, but drop all data packets. For example, in figure 3 ns which is source is sending some packets to nd which is destination node through path P= (ns, n1, n5, n3, n4, nd). Node n3 is misbehavior node which drops the entire data packets passing through it. The goal of S-ACK is to identify n3 from Path (P) and reporting this misbehavior node to source node. Each node on the path, when receives a packet sets a timer, and then forward the packet. Before this timer reaches zero, the next node prove its honesty to the previous node by sending S-ACK packet of destination to previous node.

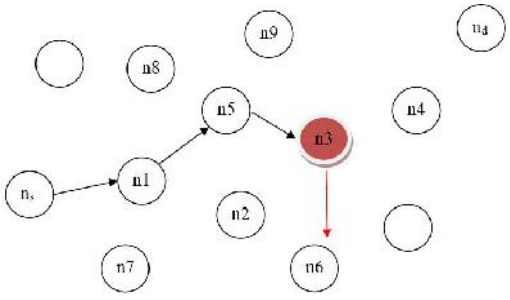

Fig.3Scenarios in presence of malicious node**.**

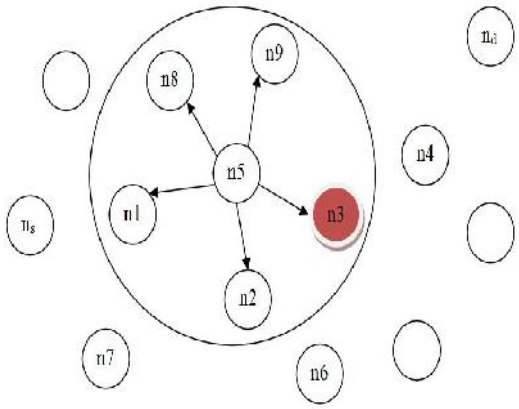

Fig .4 Scenarios in case of no acknowledgement from destination within time.

If n3 does not send the S-ACK of destination to n5, it will be considered as probable misbehavior node which drops the data packet or the acknowledgement packet. Since n3 is malicious node, n5 will not receive acknowledgement then, according to figure 4, n5 broadcasts the packet to all the neighbors including node n3 and receive acknowledgment from destination.This is because, in case if n3 does not receive previous packet due to collision will get second chance to forward the packet and receive acknowledgement. Thus it will help to detect malicious node in case of collision.

Algorithm utilized by Mobile Node.

While (true) do

Read Data Packet;

Process it;

If (node is destination node)then

Send SAck packet to previous node

Else

Start timer for PckID and wait for SAck packet to be received

If(NAck packet received in time)

If(PckID in SAck is in list)

Remove PckID and its timer from list

Send SAck to previous node

End

Else

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

Academic Science

Send PckID data Packet to all neighbors and start timer and wait

Receive acknowledgement from neighbor

If(SAck Packet is from net node)

Remove PckID and its timer from list

Send SAck to Previous node

Else

Report next node as malicious node

End while

3. MRA

The MRA scheme works same as in EAACK to detect misbehaving nodes with the presence of false misbehavior report which can be generated by malicious attackers to falsely report innocent nodes as malicious. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route In MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted. Thus using MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

4. *Digital Signature*

EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. So here digital signature concept is introduced. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented RSA [14] digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

B. System Architecture

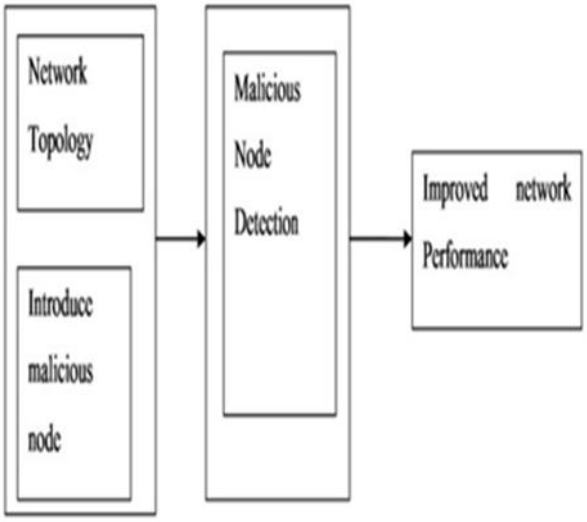

Fig 5: Architectural View

The above Figure 5 is the system architecture for IDS in MANET. It consists of three stages. A MANET network having N number of mobile nodes which are free to move is created in the 1st Stage and malicious nodes are inserted in the network in ns2 with TCL Script [18][19]. In the second stage the using proposed approach the malicious nodes are detected and marked as malicious node [20][21]. The third stage shows the result of the proposed system and existing system with respect to various performance parameters of the MANET [22]. Till now all previous methods failed to remove all problems which are not solved by watchdog method, so we proposed a new method EAACK removes all problems ensuring security with improved network overhead in MANET.

IV. SIMULATION AND RESULTS

A. Simulation Environment

In order to show the effectiveness of the proposed approach, a set of simulation experiments are carried out using NS-2 version 2.35.

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

Table 1 Experimental setup

Protocol	AODV
Radio propagation model	Two ray ground
Antenna model	Omnidirectional
No of nodes	21
Map size	1300m x 800m
Simulation time	70 mseconds
MAC type	IEEE 802.11
Packet size	512 bytes
Traffic type	Constant bit rate(CBR)

The IEEE 802.11 distributed coordination function (DCF) is used as medium access control (MAC) protocol. In the simulation experiments, a network with 1300m x 800m area and 21 mobile nodes was simulated. The simulation time is 10 seconds. The mobile nodes move within the network space according to the Two Ray Ground radio propagation model. The communication patterns used are 6 Constants Bit Rate (CBR) connections with a data rate of 10 packets per second. The total number of nodes (nn) placed randomly in this area is 21 characterizing networks with different densities. The data traffic used is CBR (Constant Bit Ratio). Each source node generates 4 packets/sec with a packet size of 512 bytes. The total simulated time was 70 mseconds. Based on the simulation parameters defined, the mobile ad hoc network is designed as in fig. The EAACK algorithm is implemented in this environment and its performance is analyzed.

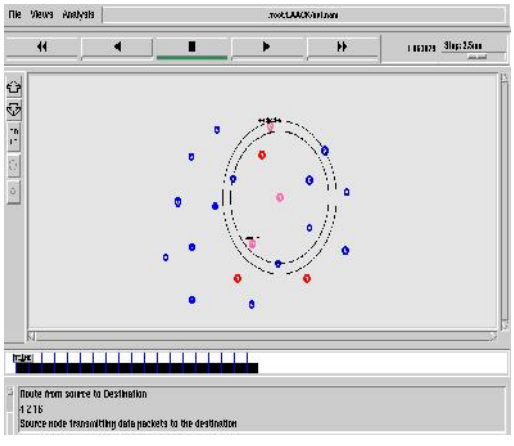

Fig 6. Data transmission from source to destination

From figure.6 there are 21 nodes, of which the source node is node 4 and the destination node is node 16.The data is being transferred from source node 4 to destination node 16 via the route 4-2-16. Based on the behavior of algorithm, graphs are generated for the performance metrics delay, packet Delivery ratio and packet loss ratio.

Fromfig 7. Source node 4 sends packet to destination node 16 Acknowledgement packet is not send back to source through feasible path as node 2 is malicious node detected. Destination sends acknowledgement message (ACK) to source for confirmation of data delivery And it does not receives the S-ACK packets from source also. Secure ACK (S-ACK) process started when source does not receives ACK message. Node has a limited transmission and not a malicious node.

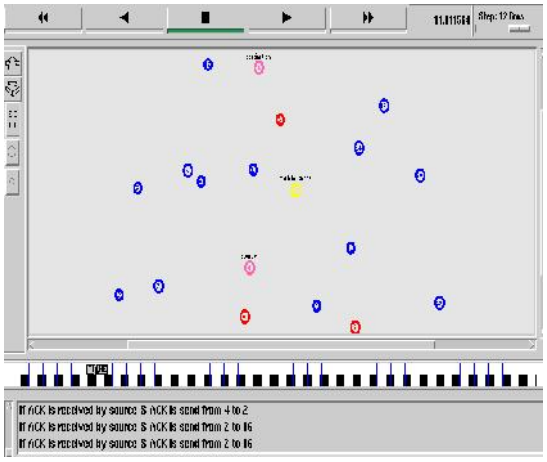

Fig 7. Data transmission in the presence of limited transmission power

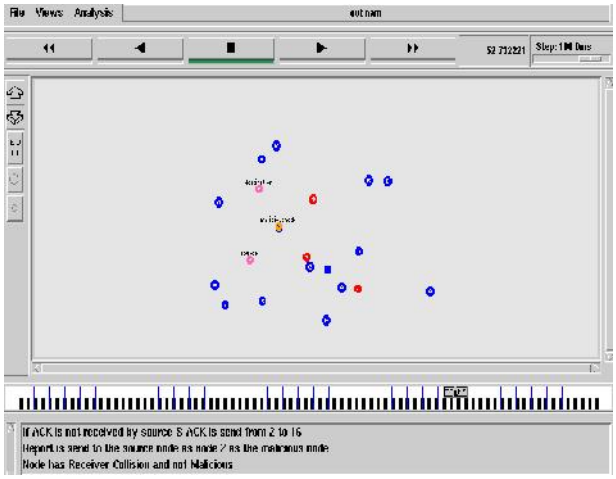

Fig8. Data transmission in presence of receiver collision.

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

S-ACK begins for three consecutive nodes for malicious node detection. Means third intermediate node 2 sends acknowledgement packet to node 16, but node 2 does not send ACK packet to node 16.Hence intermediate node sends misbehavior report to source node.

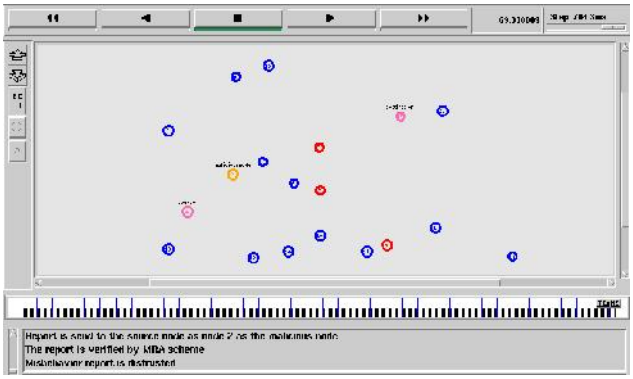

Fig 9.MRA scheme

The report is send to the source node 4 as node 2 is a malicious node as it does not sends S-ACK packets to node.so this report is verified by using MRA scheme and that misbehavior report is considered as distrusted**.**

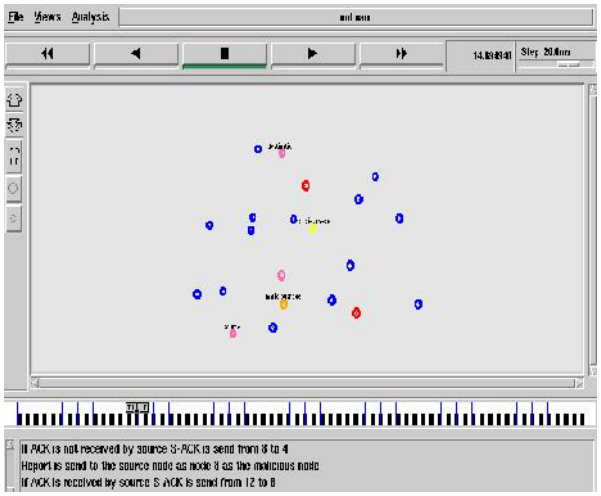

Fig10.Detection of two malicious nodes.

B. Performance evaluation

For evaluating the performance of proposed system three commonly used metrics are packet delivery ratio (PDR), end to end delay (E2E) and packet.

1. Packet delivery ratio (PDR) - PDR defines the ratio of the number of packets received by the destination mobile node to the number of packets sent by the source mobile node.

2. Packet loss: It is defined as the no of packets dropped during transmission over a communication channel. All malicious mobile nodes to send out false misbehavior report to the source node whenever it is possible. This type of scenario setting is designed to test the IDS's performance under the false misbehavior report

3. End to End Delay (E2E): The end-to-end delay

for allsuccessfully received packets at the destination. It is calculated for each data packet b subtracting the sending time of the packet from the received time at final destination. Then the average represents the E2E.

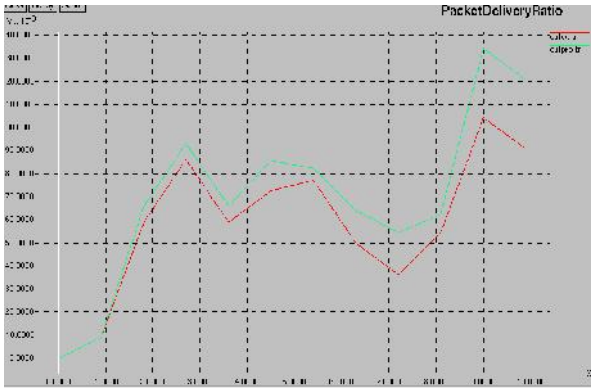

Fig .11 Packet Delivery Ratio

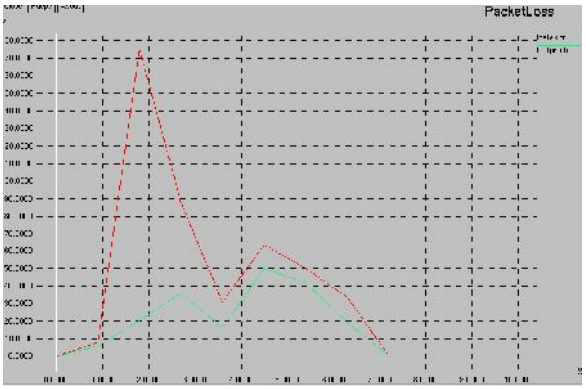

Fig .12 Packet Loss : time v/s no of packets in msec

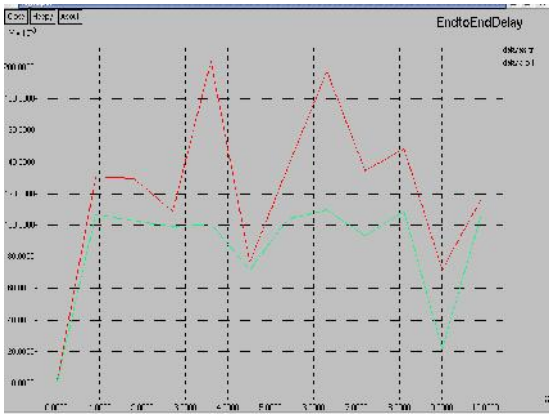

Fig .13End to End Delay: time v/s delay in msec

Academic Science

I. CONCLUSION

Intrusion detection has caused many threats in MANET for many years. Proposed system enhanced adaptive acknowledgement (EAACK) is based on acknowledgement method S-ACK which detects malicious node in case of collusion attack in MANET. The proposed system provides less packet loss due to packet dropping attack caused by malicious node in MANET. The proposed approach is designed to tackle the weaknesses of watchdog scheme, namely ambiguous collision, receiver collision, transmission power, false misbehavior report and partial dropping. Furthermore, to prevent the attackers from initiating forged acknowledgement attacks and to improve packet security RSA is used in EAACK. Apart from detecting malicious nodes in MANETs, the improved EAACK also takes care of network performance as the performance metrics packet loss and delay are reduced while packet delivery ratio is increased.

REFERENCES

[1] Rashid SheikhlMahakaSingh Chandee and Durgesh Kumar Mishra.*"Security Issues in MANET: A Review";*IEEE Transactions on Mobile Computing, 978-1-4244-7202-4, Sept 2010.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju,*"Mobile Ad hoc Network Security,"*Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, pp. 659666, 2012.

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "*DoS attacks in mobile ad hoc networks: A survey,"* Proc. 2nd International Meeting ACCT, Rohtak, Haryana, India, pp. 535541, 2012.

[4] B T. Anantvalee and J. Wu, "*A Survey on Intrusion Detection in Mobile Ad Hoc Networks,"* Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[5] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "*An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs*," IEEE Transactions on Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.

[6] S B. Sun, "*Intrusion detection in mobile ad hoc networks*," Ph.D. dissertation, Texas A Anf M Univ., College Station, TX ,2004.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "*Mitigating routing misbehavior in mobile ad hoc networks,"*; in Proc. 6th Annual International Conference of Mobile Computer Netwwork, Boston, MA, pp. 255265, 2000.

[8] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, *"An acknowledgment-based approach for the detection of routing misbehavior in MANETs*," IEEE Transactions on Mobile Computing, vol. 6, no. 5, pp. 536550, May 2007.

[9] D. Johnson and D. Maltz, "*Dynamic Source Routing in ad hoc wireless networks,"* in Mobile Computing. Norwell, MA: Kluwer, ch. 5, pp. 153181, 1996.

[10] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "*Video transmission enhancement in presence of misbehaving nodes in MANETs*," International Journal of Multimedia System, vol. 15, no. 5, pp. 273282, Oct. 2009.

[11] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, *"EAACK-A Secure Intrusion-Detection System for mantes,"* IEEE Transactions On Industrial Electronics, Vol. 60, No.3, March 2013.

[12] R. Rivest , A. Shamir, and L. Adleman, *"A methodfor obtaining digital signatures and public-key cryptosystems,"* Communication ACM, vol. 21, no. 2, pp. 120126, Feb.1983.

[13] A. Menezes, P. van Oorschot, and S. Vanstone, *"Handbook of Applied Cryptography"*. Boca Raton, FL: CRC, T-37, 1996.

[14] National Institute of Standard Technology, Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, Digital Signature Standard (DSS), 2009.

[15] http://openarchive.acadiau.ca/cdm/ref/collection/Theses/id/592

[16] G. Jayakumar and G. Gopinath, *"Ad hoc mobile wireless networks routing protocol-A review,"* Journal of Computer Science, vol. 3, no. 8, pp. 574-582, 2007.

[17] Wireless Communications And Networks -William Stallings, Pearson Education.

[18] http://enggedu.com/source-code/ns2/ns2/wireless/TCL-script-to-_nd-wireless-packetdropping-nodes.php

[19] http://_kirankubuntu.blogspot.in/2010/03/adding-malicious-node-in-aodv.html

[20-] http://_kirankubuntu.blogspot.in/2010/03/adding-malicious-node-in-aodv.htm network

[21] http://enggedu.com/source-code/ns2/ns2/wireless/TCL-script-to-_nd-wireless-packetdropping- nodes.php

[22] Dr. Sunilkumar S. Manvi, Mahabaleshwar S. Kakkasageri, *"Wireless and MobileNetworks"*, Wiley IndiaPOvt. Ltd., 2010.