Implementation of Enhanced Adaptive Aknowledgement for Mobile Adhoc Networks

Vinnarasi Tharania. I[1] M.Kanchana[2] V.Kavitha[3]
[1,2,3]Assistant Professor
[1, 2, 3]Department of Information Technology
[1,2,3] Karpaga Vinayaga College Of Engineering & Technology, China Kolambakkam, Madurantakam Taluk,Kanchipuram-603308, Tamilnadu, India

Abstract--- The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Mobile Adhoc Network (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behaviour-detection rates in certain circumstances while does not greatly affect the network performances.

Keywords: Mobile Adoc NETwork(MANET),Network Simulator 2(NS2),Auto Working Kit(AWK),Tool Command Language(TCL),Constant Bit Rate(CBR), Network Animato (NAM)

I. INTRODUCTION

The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks.

With the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such trend, we strongly believe that it is vital to address its potential security issues. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

II. RELATED WORK

Securing zone routing protocol in Ad-Hoc networks is developed by Ibrahim, Abuhaiba, Hanan, Abu- Thuraia in 2012[12] has observed, security analysis on mobile ad-hoc networks, and security requirements of applications. For digital signature they use a special scheme to perform the security on MANETs.

A recent secure intrusion detection system for MANETs is developed by Sharmila Beham, Murugaboopathi in 2013[9] has observed, mobile ad-hoc network is collection of wireless mobile nodes forming a network without using any existing infrastructure. MANET is collection of mobile nodes equipped with both a wireless –transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly.

Identification of critical node for the efficient performance in MANET is developed by, Shivashankar, Sivakumar, Varaprasad in 2012[8] has observed. The nodes are connected randomly in a network and fail at random times. The critical node test detects nodes, whose failures are malicious behavior, disconnects or significantly degrades the performance of the network. The critical node is an element position or control entity whose distribution, is immediately degrades the ability of a force to command, control of effectively conducts combat operation.

A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network Prajeet Sharma, Niresh Sharma, Rajdeep Singh in 2012 [4] has observed, There are many security attacks in MANET and DDoS (Distributed denial of service) is one of them. Our main aim is seeing the effect of DDoS in routing load, packet drop rate, and end to end delay. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks developed by Yih-Chun Hu David B. Johnson Adrian Perrig in 2012 [3] has observed, a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV). In order to support use with nodes of limited CPU processing capability, and to guard against Denial-of-Service (DoS) attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios we tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

Privacy protection using unobservability and unlinkability against wormhole attacks in manet is developed by N.Sugumar, K.Jayarajan in 2012 [7] has observed, An efficient privacy-preserving routing protocol USOR that achieves content un-observe ability by employing anonymous key establishment based on group signature. The setup of USOR is simple: In privacy-preserving communications can largely be divided into two categories: cryptosystem-based techniques and broadcasting-based techniques. The cryptosystem-based techniques include mix-based systems and secure multiparty computation-based systems, originating from mix net and DC-net respectively. Broadcasting based schemes provide communication privacy by mixing the real messages with dummy packets so that it is infeasible for the adversaries to identify the real packets and track the message source.

III. Existing Work

It is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches. In this section, we mainly describe three approaches, namely, Watchdog, TWOACK, and Adaptive ACKnowledgment (AACK).

Watchdog is capable of detecting malicious nodes rather than links. It aims to improve the throughput of network with the presence of malicious nodes. The Watchdog scheme fails to detect malicious misbehaviors with the presence of the following:
1) ambiguous collisions;
2) receiver collisions;
3) limited transmission power;
4) false misbehavior report;
5) collusion;
6) partial dropping.

TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead.

AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK which is identical to TWOACK and an end-to-end acknowledgment scheme called Acknowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

IV. Proposed Method

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), misbehavior report authentication (MRA) and digital signatures.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. The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

The S-ACK (Secure-ACKnowledgement) scheme is an improved version of the TWOACK scheme. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

A. Modules

The Enhanced Adaptive ACKnowledgment consist of three modules for the implementation of the process and they are,

1. Intrusion Detection System
2. Malicious Attacks
3. Enhanced Adaptive Acknowledgment [Eaack]

1) Intrusion Detection System

In a network some nodes can be selfish and malicious which leads to security concerns. Therefore, Intrusion Detection System (IDS) is required for MANETs. In MANETs, most of the Intrusion Detection Systems (IDSs) are based on watchdog technique. These watchdog techniques also called overhearing techniques and suffer from some problems. In this paper an effort has been made to overcome the problems of overhearing technique. Intrusion Detection Systems (IDSs) for Mobile Ad hoc NETworks (MANETs) are indispensable since traditional intrusion prevention based techniques are not strong enough to protect MANETs. However, the dynamic environment of MANETs makes the design and implementation of IDSs. Wireless ad-hoc networks need to be secured and use intrusion detection systems (IDS).

2) Malicious Attacks

Malicious attackers can easily capture and compromise nodes to achieve attacks. Watchdog scheme fails to detect malicious misbehaviors. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop’s transmission, fals4 misbehavior, limited transmission power, and receiver collision. EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

3) Enhanced Adaptive Acknowledgment [Eaack]

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), misbehavior report authentication (MRA) and digital signatures 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. The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.

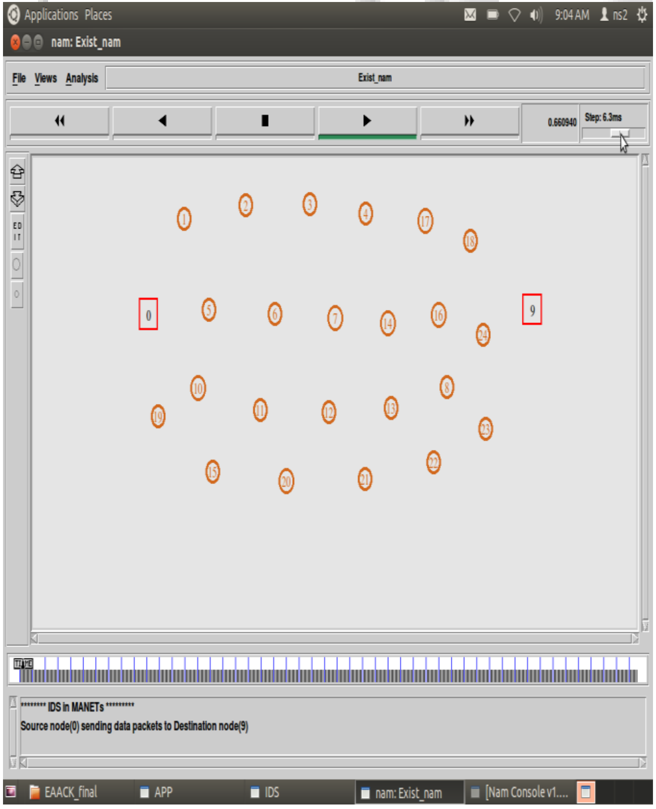
The S-ACK (Secure-ACKnowledgement) scheme is an improved version of the TWOACK scheme. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

V. OUTPUT ANALYSIS

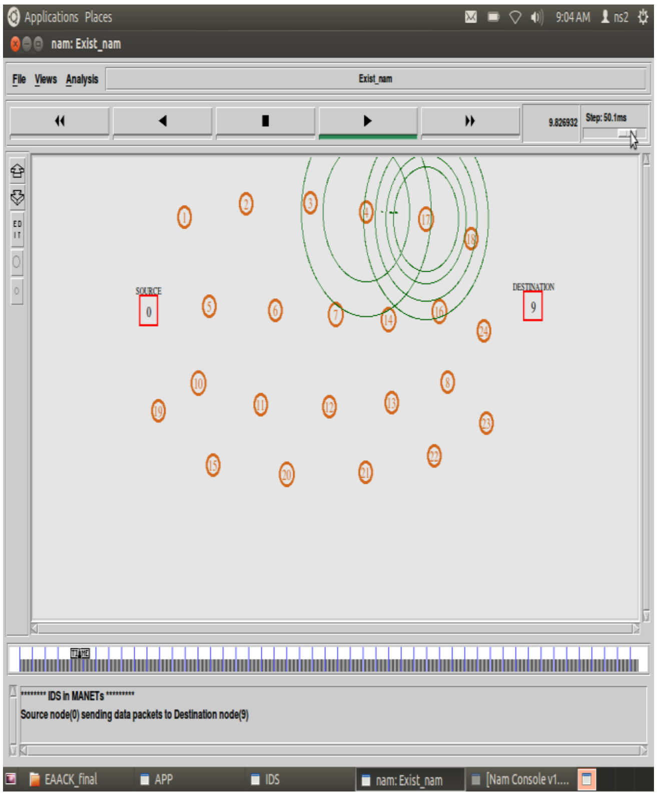
Screen Shots Are Used To Reflect The Output Of The Project That Is Implemented Using Different Modules; These Are The Screen Shots For The Project.



******** IDS in MANETs ********
Source node(0) sending data packets to Destination node(9)

Fig. 1: Configuration

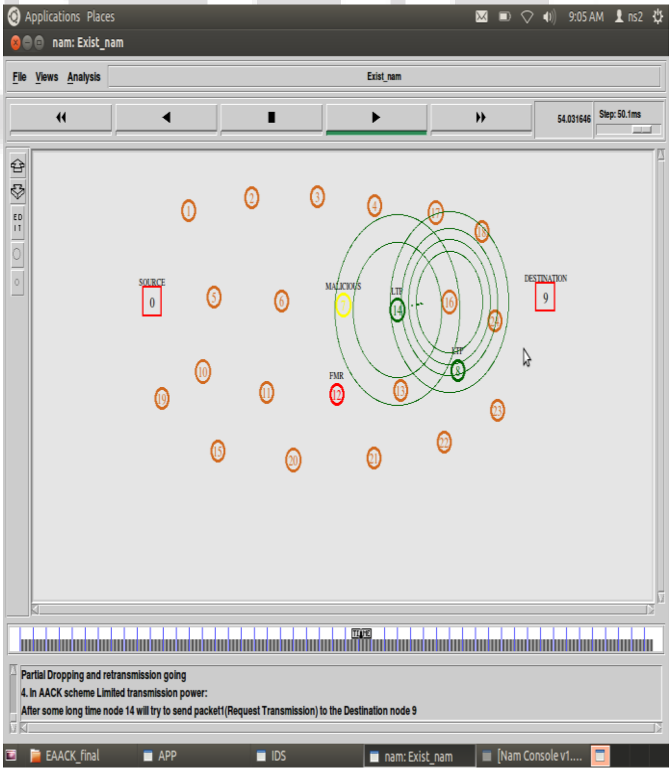
The screen shot is shows the configuration of the nodes in the MANETS and the source and destination of the networks.



******** IDS in MANETs ********
Source node(0) sending data packets to Destination node(9)

Fig. 2: Sending of packets.

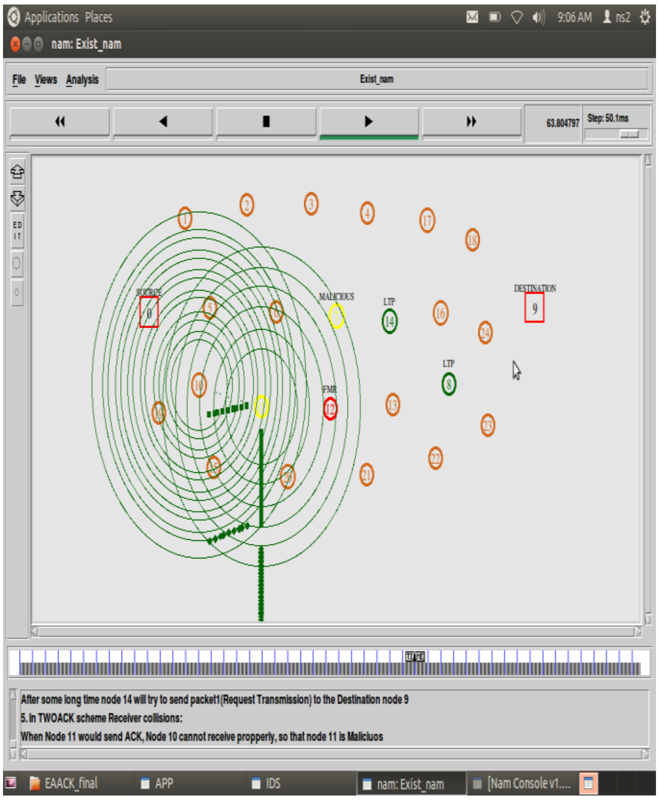
The source sends a packet to the destination via the intermediate nodes in the network. Then the acknowledgement is send back to the source via same path.



Partial Dropping and retransmission going
4. In AACK scheme Limited transmission power:
After some long time node 14 will try to send packet1(Request Transmission) to the Destination node 9

Fig. 3: Identifying malicious nodes.

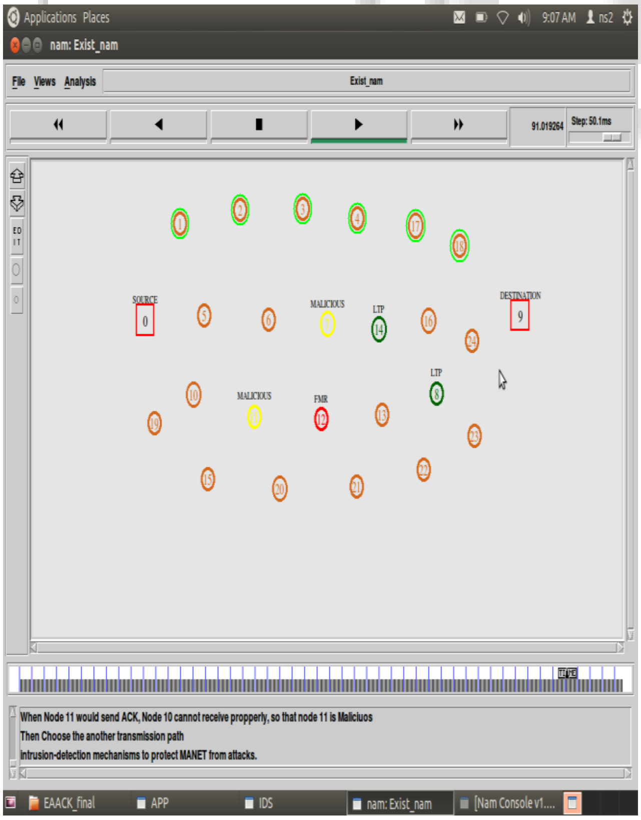
In the MANET there are many malicious nodes and we want identify that kind of nodes by Watchdog scheme and the limited transmission power by TWOACK scheme.



After some long time node 14 will try to send packet1(Request Transmission) to the Destination node 9
5. In TWOACK scheme Receiver collisions:
When Node 11 would send ACK, Node 10 cannot receive propperly, so that node 11 is Maliciuos

Fig. 4: Packet Dropping

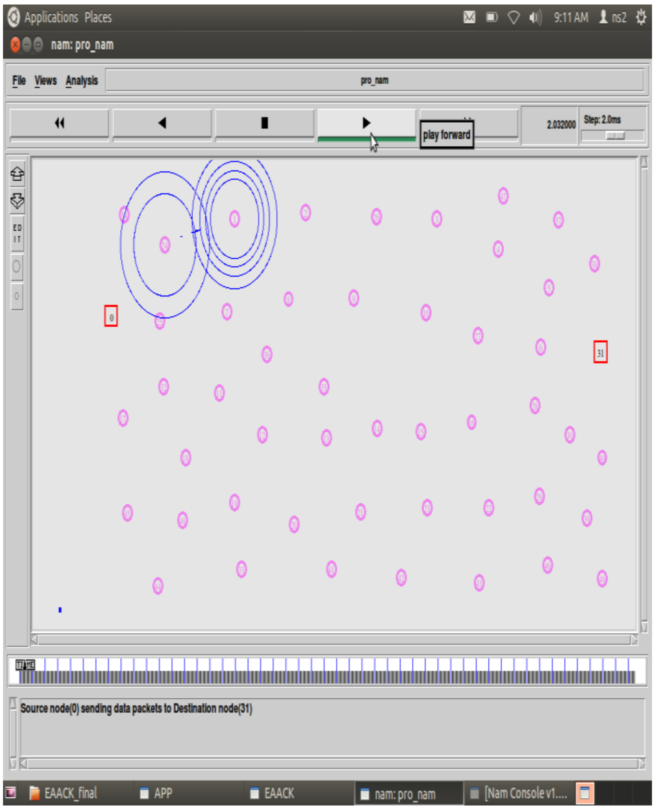
The malicious node in the network is having the characteristics of dropping the packet which is send by source of the network. This gives malicious node of the network.



When Node 11 would send ACK, Node 10 cannot receive propperly, so that node 11 is Maliciuos
Then Choose the another transmission path
Intrusion-detection mechanisms to protect MANET from attacks.

Fig. 5: Secure path

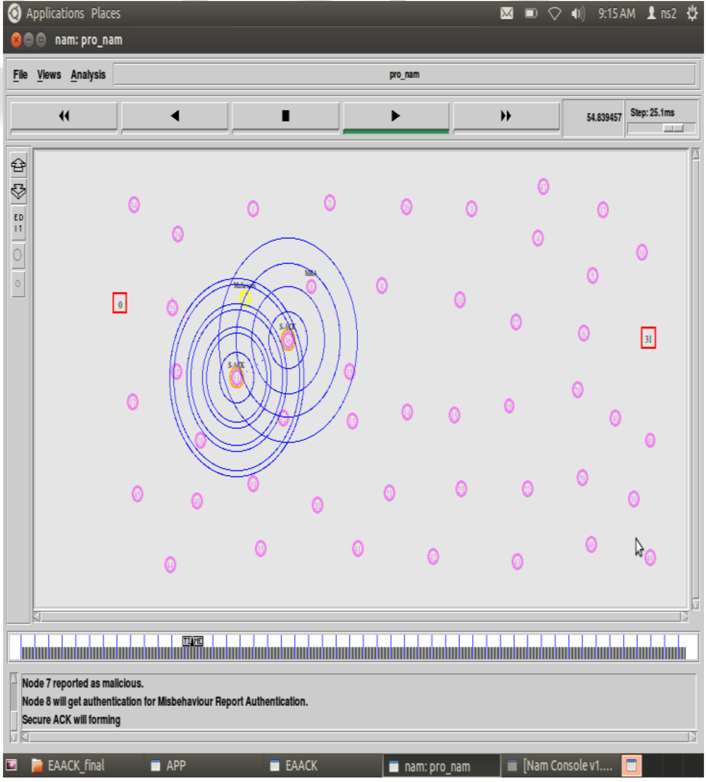
The green color node in the network are shows the secure path for the source and the destination.



Source node(0) sending data packets to Destination node(31)

Fig. 6: Proposed Systems

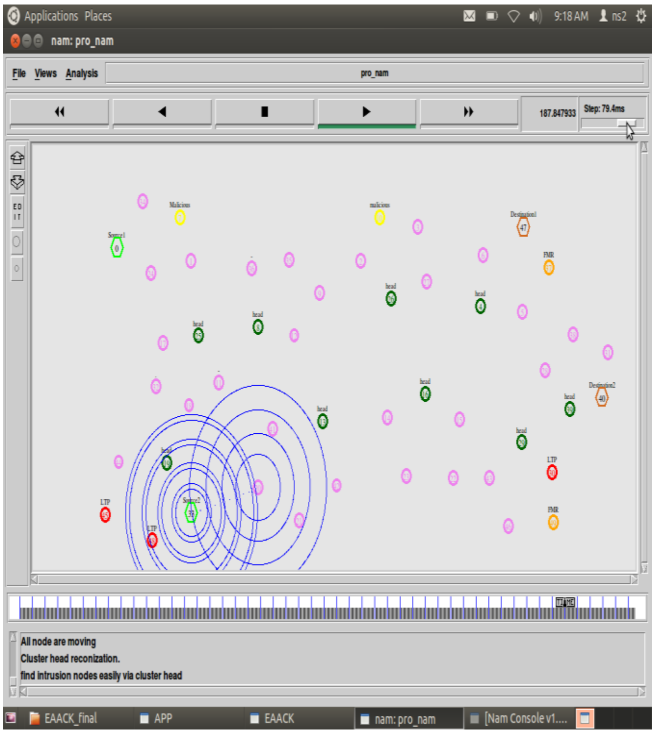
In proposed system shows the 50 nodes in the network and each knows the receiver and transmitter. The red rectangle box shows source and destination. Then the source sends a packet to the destination.



Node 7 reported as malicious.
Node 8 will get authentication for Misbehaviour Report Authentication.
Secure ACK will forming

Fig. 7: Secure Acknowledgements.

If any malicious node is detected during transmission the intermediate node uses the S-ACK scheme for sending a secure path to the destination.



All node are moving
Cluster head reconization.
find intrusion nodes easily via cluster head

Fig. 8: Cluster Head.

The cluster head is a node which is used to detect the receivers and transmitters in the network for making the secure path while sending.

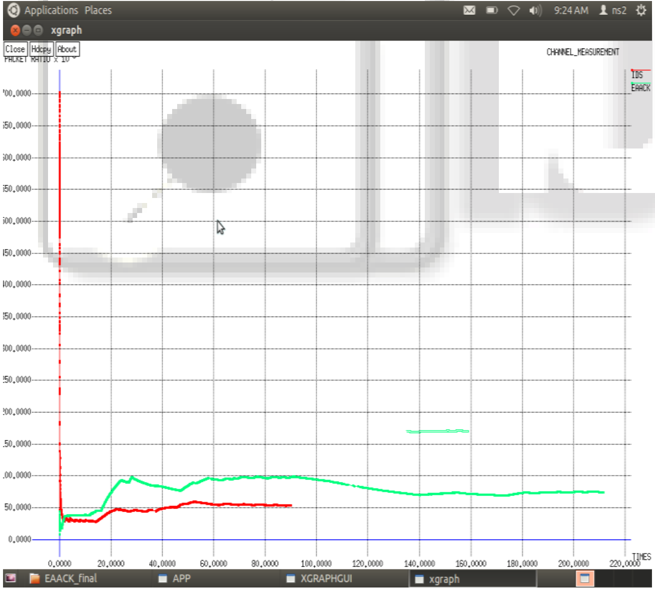


Fig. 9: Channel Measurement

The graph shows the channel measurement for the IDS and EAACK. This presented by x and y graph format.

VI. Conclusion

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. We think that this tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs.

References

[1] Akbani. R. H, Korkmaz .T, and Raju .G. V. S, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127.New York: Springer-Verlag, 2012, pp. 659–666.

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

[3] Buttyan. L and Hubaux. J. P, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[4] Hu. Y, Perrig. A, and Johnson. D, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[5] Jayakumar. G and Gopinath. G, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582,2007.

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

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

[8] Kuladinith. K, Timm-Giel. A. S, and Görg. C, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323,2004.

[9] Lee A. S, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4,pp. 1835–1841, Apr. 2008.

[10] Liu. K, Deng. J, Varshney. P. K, 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.

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

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

[13] Nasser. N and Chen. Y, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int.

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