EAACK Based Security in MANETs Using ECC and MAES Algorithms

[1] Brijal J Patel, [2] Prof. Krunal Panchal
[1]Student of Gujarat Technological University, Department of Information Technology Engineering,
L. J. Institute of Engineering and Technology, Gujarat Technological University, Ahmedabad,
Gujarat, India
[2]Assistant Professor at L. J. Institute Of Engineering & Technology, Ahmedabad, Gujarat, India
[1]brijalpatel59@gmail.com, [2]krunaljpanchal@gmail.com

ABSTRACT

A Mobile ad hoc network (MANET) is an autonomous system of wireless mobile nodes that can be dynamically setup anywhere and anytime[13]. MANET differs from cellular networks or conventional wired networks as there is no centralized access poin. MANET allows multi-hop communication[10] among nodes that are not in direct transmission range through intermediate nodes. Nodes are free to move randomly thus form arbitrary network topology. There is various type of attacks MANETs. Providing security against the intruder is a challenging task in MANET[10]. In my literature review, we present the Enhanced Adaptive Acknowledgment (EAACK) based Intrusion Detection system that is used to mitigate[13] the attacks. And Increase a performance[2] or Packet delivery ratio, throughput and In my proposed work different security algorithms such as ECC and MAES are used with EAACK which reduce network overhead and provide high level of security in the network.

Keyword: ***Enhanced Adaptive Acknowledgement (EAACK);ECC; Modified AES;***

1. INTRODUCTION

Due to increasing use of Mobile Ad-hoc Network (MANET) that is emerging as a very popular technology in the wireless network due to its dynamic topology and reduced cost with improved technology. Limited characteristics that make the Ad-hoc wireless networks, vulnerable to intruders and attacks that damage the integrity of the network. Providing security against the intruder is a challenging task in MANET. Therefore it is crucial to develop suitable intrusion detection scheme (IDS) to protect MANET from malicious attackers. ECC, Modified AES algorithms provides security to the data that is sent between nodes when used on EAACK technology which is term as Enhanced Adaptive Acknowledgement[10]. The basic EAACK architecture is mentioned fig.1

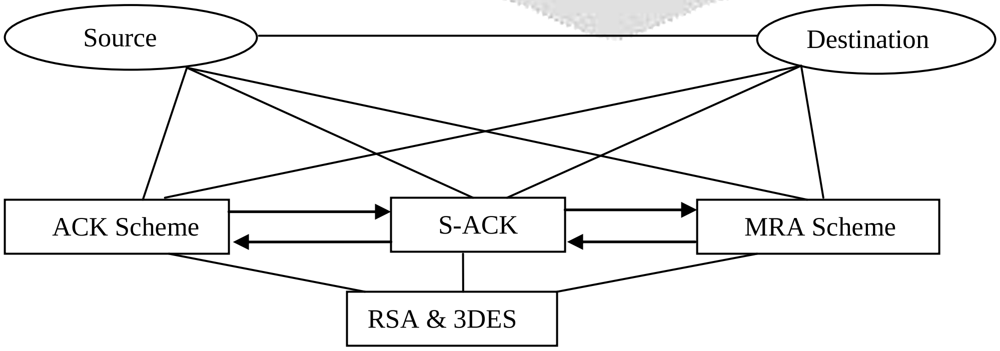


Fig.1 Enhanced Adaptive Acknowledgment

2. BACKGROUND THEORY

An Ad hoc network is a collection of mobile nodes, which forms a temporary network without the aid of centralized administration or standard support devices regularly available as conventional networks. Various MANET's routing protocols that are reported as fig.2

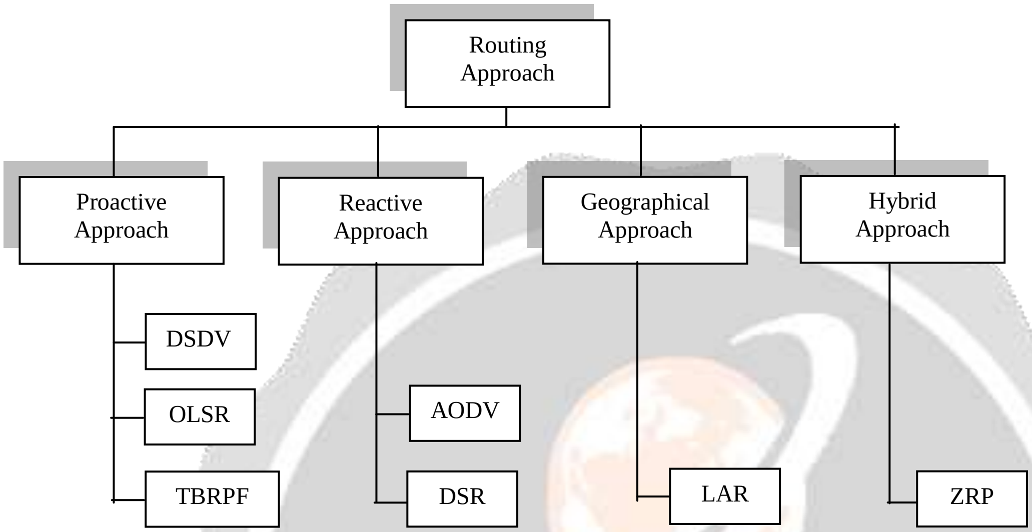


Fig.2 MANET Routing Protocols

In our work Reactive type(AODV) protocol is used. MANET'S have various characteristics that are:

1. Open network boundary
2. Dynamic topology
3. Hop by hop communication
4. Easy and quick set up

Proposed system overcome the watchdog weaknesses also. The various advantages are as follows:

a) **Low cost of deployment**: As the name suggests, ad-hoc networks can be deployed on the fly, thus demanding no expensive infrastructure such as copper wires, data cables, etc.[10]
b) **Fast deployment**: When conceded to WLANs, ad-hoc networks are very convenient purpose and easy to deploy requires less manual intervention since there are no cables involved[10].
c) **Dynamic Configuration**: Ad hoc network configuration changes dynamically with time. For scenarios such as data sharing in classrooms, etc., this is a useful feature. When compared to configuration of LANs, it is very easy to change the network topology.[10]

The disadvantage is a) vulnerable channels ,b) No infrastructure so that difficult to maintain on-line servers and centralized authority, c) dynamic topology ,d) different requirements for different type of applications ,e) MANETs Vulnerable to malicious attackers because of open medium and wide distribution thereby they are is easily attacked to improve security they develop IDS. IDS detect and report the malicious activity in ad hoc networks.[10]

Applications

Enhanced Adaptive Acknowledgment main application is based on wireless networking in MANET's. The set of applications for MANET is as large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Below are various EAACK applications:

a)Business Sector
b)Local Level
c) Personal Area Network (PAN) and Bluetooth
d)MANET-VoVoN
e) Military Battlefield
f)Educational Sector

3. IDS TECHNIQUE IN MANETS

In MANETs mainly three type of IDs technique ensure secure communication of data packets in the network. Thay are as mentioned:

1. TWOACK
2. AACK
3. Watchdog

TWOACK: TWOACK scheme in MANET successfully solves the receiver collision and limited transmission power problems faced by Watchdog. However, the acknowledgment process required in every packet transmission process added a unwanted network overhead. Due to the limited battery power nature of MANETs, such process can easily degrade life span of the entire network.[9]
AACK: It overcomes the two problems of watchdog and improves the performance of TWOACK by reducing the routing overhead while maintaining better performance [4]. AACK is a combination of TACK and ACK. It reduces network overhead, it fails to detect malicious nodes with false misbehavior report.[8]

Watchdog- proposes two techniques (Watchdog and Pathrater) that improve the network throughput having selfish or misbehaving nodes. Consisting of two techniques Watchdog and Pathrater. Watchdog serves as IDS cooperates with routing protocols. Detects malicious nodes by overhearing next hop's transmission. A false counter is occurs if the next node fails to Forward the data packet [3]. When exceeds a predefined threshold node or marked it is malicious node. The drawback of watchdog are 1) ambiguous collisions, 2) receiver collisions 3) limited transmission energy, 4) wrong misbehavior report, 5) partial dropping [4].

4. LITERATURE SURVEY

There have been many researchers who have attempted in Enhanced Adaptive Acknowledgement System. Parth Patel, Rajesh Bansode et al. [10] proposed Enhanced Adaptive Acknowledgement(EAACK) Technique which is the combination of two cryptography system such as RSA and Triple DES, as the researchers provide security during data transmission with the existence of malicious node . And they also stated that this EAACK technique can be lead to the some another cryptographic security algorithms. Some reviews are presented in Table I.

Table -1: Analysis of different approach of Face Recognition

Researchers	Method Used	Advantages	Disadvantages
Poonam Joshi, Pooja Nande [1]	IDS,EAACK	A better malicious-behavior-detection than the traditional approaches.	This system is resolve only 3 weakness of watchdog.
Ashish Patil,Nilesh Marathe [2]	EAACK, IDS and ECDSA	Provide secure and reliable communication and provide same level of security as compare to RSA	Increased overhead
Dipamala Nemade, Ashish T. Bhole [3]	EAACK and Routing algorithms	AODV give batter performance as compare to DSR	Network overhead. it could be improved using IDS technique. extract component need to be used

Deore Suvarna , Erande Pallavi [4]	EAACK, DSA and clustering algorithm	Provide security using clustering ,prevent from fake acknowledgement attack	Network overhead because of DSA
Elizabeth Sherine.M [5]	EAACK and DSA	Higher malevolent conduct location rates in specific circumstances while does not significantly influence the system exhibitions.	Increase network overhead
Elhadi M. Shakshuki, Nan Kang [6]	EAACK ,DSA and RSA	Prevent from forge ack attacks . positive performance against watchdog, TWOACK,AACK, Improve PDR	Increase network overhead .
G. Santhi [7]	EAACK and DSA	EAACK-DSA gives better malicious Behaviour-detection than the conventional approaches	Increase network overhead .
D. Sandhiya, K. Sangeetha [8]	EAACK ,Diffie-hellman key exchange algorithm.	Prevent from forging ack packets, one hop is improve detection rate . eliminate the requirement of Predistributed keys	Increased overhead
Mrs. Rashmi K. Mahajan , mr. Sanjay. M. Patil [9]	EAACK and ECDSA	ECDSA gives authenticity without compromising security	Reduce control overhead
Parth Patel, Rajesh Bansode[10]	EAACK,RSA 3DES,	Increase network security, RSA &3DES less Cost , low Power	Network overhead ,time consuming

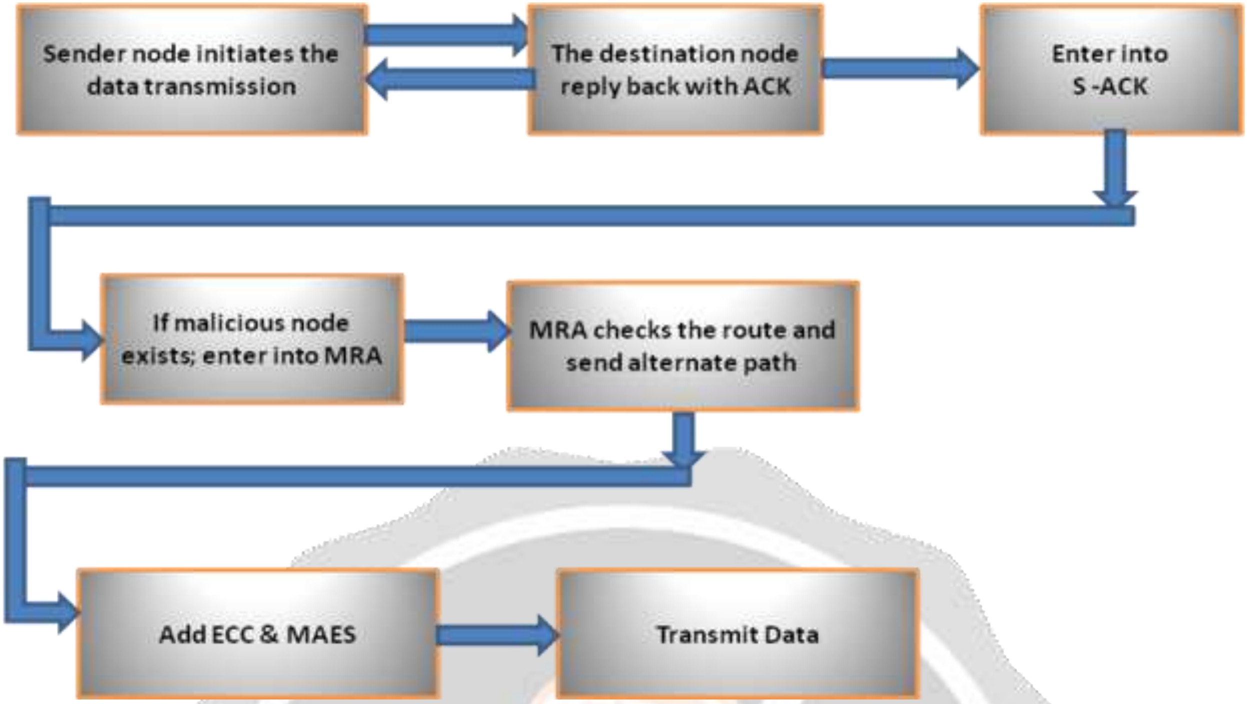
5. PROPOSED SYSTEM

Earlier IDSs techniques in MANETs adopt acknowledgment-based scheme, including TWOACK and AACK etc. The function of such detection schemes largely depends on the acknowledgment packets [10]. Hence, it is very import to guarantee that the acknowledgment packets are valid and authentic as well as secure it.

A powerful and light-weight technique enhanced Intrusion detection mechanism called EAACK Scheme using ECC & Modified AES algorithm which requires less cost, low power. EAACK consists of three major operations called: ACK, S-ACK & MRA. ACK is a end-to-end acknowledgment scheme. aiming to reduce network overhead when malicious node is detected in network [6]. In this method, if the receiver node does not sends the Acknowledgement within predefined time period, then ACK assumes malicious node may be present and switch it as to SACK part to detect the nodes.

In S-ACK module, every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment to first node packet. By introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power [1]. If malicious found, then MRA part suggests alternate path to the destination. When compared with other the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source to switch to MRA module and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

Along with the above procedure add Cryptography mechanism such as ECC and Modified AES which secure the flow of data transmission in MANETs. Hence a secure network path will have less computation of data rates [10]. The Below shown Fig.3 is architecture of EAACK scheme with security algorithms.


Sender node initiates the data transmission
The destination node reply back with ACK
Enter into S -ACK
If malicious node exists; enter into MRA
MRA checks the route and send alternate path
Add ECC & MAES
Transmit Data

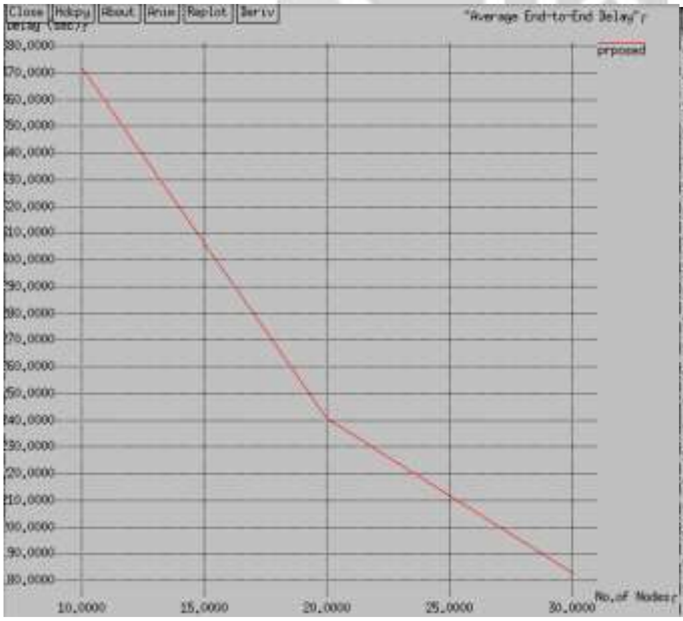
.

Fig 3: Proposed System

6. Result Analysis

For implementation of proposed Flow work has been experimented through Network Simulator 2[NS2], which is running on laptop with a 2 GHz Core2duo with 2 GB RAM and Windows 7 Operating System.

For experiment the 4 different parameters such End to End Delay, Packet Delivery Ratio, Throughput, Network Overhead . And the result of these parameters given below.



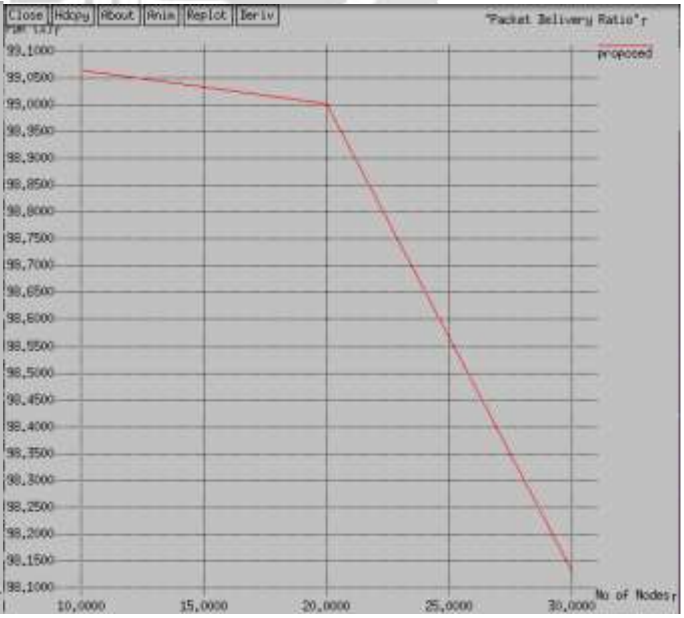


Fig. 4 :End to End Delay

Fig 5: Packet Delivery Ratio

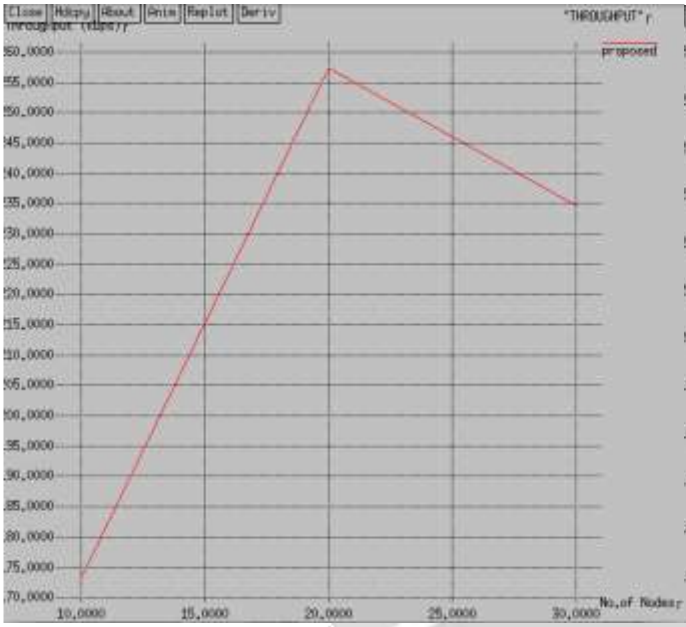


Fig. 6 :Throughput

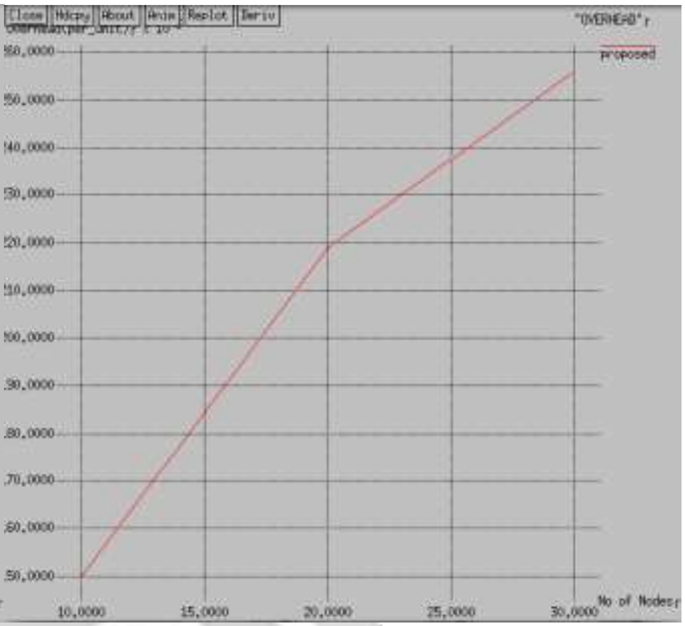


Fig 7:Network Overhead

By this Result we can say that overall End to End Delay and Network Overhead is reduce, And Throughput and Packet Delivery Ratio is increase by using ECC and Modified AES algorithm which we can see in Fig 5, Fig 6, Fig 7 and Fig 8.

7. CONCLUSION

Our Proposed EAACK scheme reduce the network overhead in the case of authentication and also overcome watchdog limitation such as receiver collisions, limited transmission power, false misbehavior report. In my proposed work, We are using ECC and Modified AES instead of RSA and Triple DES. ECC and MAES with EAACK scheme in result it provide us high level of security as compare to RSA and Triple DES. And also reduce network overhead and Delay, improve a system performance and increase packet delivery ratio.

REFERENCES

[1] Poonam Joshi, Pooja Nande, "EAACK – A secure intrusion detection and prevention system for MANETs" 978-1-4799-6272-3/15@2015 IEEE International Conference on Pervasive Computing (ICPC).pp.1-6, 2015.

[2] Ashish Patil,Nilesh Marathe,**"**Improved EAACK scheme for detection and isolation of a malicious node in MANET**"**,978-1-4673-9223-5/15@2015 IEEE International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).pp.529-533, 2015.

[3] Dipamala Nemade, Ashish T. Bhole,"Performance evaluation of EAACK Ids using AODV and DSR routing protocols in MANET",978-1-4673-9563-2/15@2015 IEEE International Conference on Emerging Research in Electronics, Computer Science and Technology.pp.126-131,2015

[4] Deore Suvarna , Erande Pallavi, "Acknowledgement security for MANET using EAACK",978-1-4673-7910-6/15@2015 IEEE International Conference on Green Computing and Internet of Things (ICGCIoT).pp.671-678,2015.

[5] Elizabeth Sherine.M, "Effective intrusion detection method for MANETs Using EAACK", 978-1-4799-7075-9/15@2015 IEEE International Conference on Circuit, Power and Computing Technologies [ICCPCT].n.p,2015.

[6] Elhadi M. Shakshuki , Nan Kang, “EAACK – A Secure Intrusion-Detection System for MANETs”,978-1-4799-6272-3/15@2013 IEEE Transactions On Industrial Electronic .p.p.1089-1098 web. DOI:10.1109/pervasive.2013.7087032,March 2013.

[7] G.shanthi,“An Efficient Intrusion Detection System Based on Adaptive Acknowledgement with Digital Signature scheme in MANETs”,978-1-4503-4756-4/16 @2016 ACM.n.p,web.DOI:10.1145/2980258.2980464, October 2015.

[8] D.Sandhiya, K.Sangeetha, “Adaptive Acknowledgement Technique with Key Exchange Mechanism for MANET”,978-1-4673-9563-2/15@2014 IEEE Transaction on industrial Electronic .n.p,web.DOI:10.1109/ erect.2015.7499000,December 2014
.

[9] Mrs. Rashmi K. Mahajan, Mr. Sanjay M. Patil, “Protection against Data Drop, An Enhanced Security Model of Authentication Protocol for Ad-Hoc N/w”, 978-1-4799-7678-2/15@2015IEEE.n.p,web.DOI: 10.1109 /icgciot.2015. 7380548, October 2015.

[10] Parth Patel , Rajesh Bansode, “Performance Evolution of MANET Network Parameters using AODV Protocol for HEAACK Enhancement”, ScienceDirect,Elsevier p.p.923-939,web.DOI:10.1016/ j.procs.2016.03.118.