VOL. 12, NO. 9, MAY 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

PERFORMANCE ANALYSIS OF ENERGY-EFFICIENT ENHANCED ADAPTIVE 3 - ACKNOWLEDGEMENT (EE-EA3ACK) USING ECC IN MANET

K. Thamizhmaran[1], M. Anitha[1] and Alamelunachippan[2]
[1]Department of Electronics and Communication Engineering, Annamalai University, Tamil Nadu, India
[2]Department of Electrical and Electronics Engineering, Pondicherry Engineering College, Puducherry, India
E-Mail: tamil5_happy@yahoo.co.in

ABSTRACT

Emerging technology allows the users to access information and services anywhere regardless of their geographic location. Mobile Ad hoc Network is the significant technology among various wireless communication technologies where all the nodes are mobile and which can be connected to dynamically used wireless link in a random manner. The self-configuring ability of nodes in MANETs made it popular among critical applications like military use or natural emergency recovery. Most of the proposed protocols assume that all nodes in the network are cooperative, and do not address any security issue. To adjust to such trend, it is vital to address its potential security issues. The main objective of this paper is to define the path for security and to further improve throughput, routing overhead, packet delivery ratio and at the same time to create energy enhanced way with excellent security. Implementation of cryptographic algorithm for the information is done in such a way that it is impossible for the attackers to knock the resources of information sent on the web. In this paper, a new intrusion detection system, Energy Efficient Enhanced Adaptive 3 Acknowledgement (EE-EA3ACK), using EA3ACK with Elliptical curve cryptography is (ECC) specially designed for MANET. In this ECC there is a two key encryption technique based on elliptic curve based theory that can be used to create faster, smaller, and more energetic and efficient cryptography. Network Simulator (NS2) is used to implement and test the proposed system. The proposed cryptography provides secured transmission, further it reduces routing overhead, improves packet delivery ratio and throughput.

Keywords: mobile ad-hoc networks, watchdog, misbehavior node, EAACK, A3ACK, EE-EA3ACK, MRA, ECC.

1. INTRODUCTION

A Mobile Ad-hoc Network is a collection of all independent mobile nodes that can communicate with each other through radio waves. The mobile nodes that are in the radio range of each other can directly communicate, whereas others need the aid of intermediate linked nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully dynamically distributed, and can work at any place without the help of any fixed infrastructure as base stations. MANET suffers from a great efficiency loss due to the misbehaving nodes which may be constrained by the resources as battery power and bandwidth of topology. Different approaches have already been proposed to detect and prevent the misbehaviour in MANET.

1.1 Routing protocol

A static routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two active nodes on a computer network. Routing algorithms determine the specific choice of route. Each router only has a prior knowledge of networks attached to it directly. Routing protocols share this information among other immediate neighbors, and then whole network. The two main types of routing are static routing and dynamic routing. The entire router learns about remote networks from neighbor routers or from an administrator and builds an update routing table. If the network is directly connected, then the router already knows how to get to the network. The router learns how to get to the remote network with either static or dynamic routing. If static routing is used, then the administrator has to change all routers in the network and therefore no routing protocol is used: Only Dynamic Routing Protocol (DSR) uses routing, which enables routers. Generally, there are two different stages in routing: they are route discovery and forwarding data packets. In route discovery, the route to a destination will be discovered by broadcasting the query. Then, once the un-breakable route has been established, data forwarding will be initiated and sent through the routes that have been determined. The power consumption, route relaying load, battery life, and reduction in the frequency and bandwidth of sending control messages, optimization of size of headers and efficient active route reconfiguration should be considered when developing a routing protocol.

1.2 Misbehaviour detection in MANET

All routing protocols perform two important functions- (i). Routing function (ii). Data-forwarding function: Routing function is involved in path discovery and path maintenance whereas Data-Forwarding function is involved in forwarding all the TX data packets towards the destination through already established route. Both routing, data forwarding and packet receiving function can be affected in the presence of certain nodes called misbehaving nodes which can cause different types of attacks like packet eavesdropping, active and passive attacks. So the primary challenge in MANET is not to

detect misbehaviour nodes and collision nodes. Misbehaving node is simply dropping all packets as shown in Figure-1. Misbehaving node drops the packets received and does not forward to other nodes in the path.

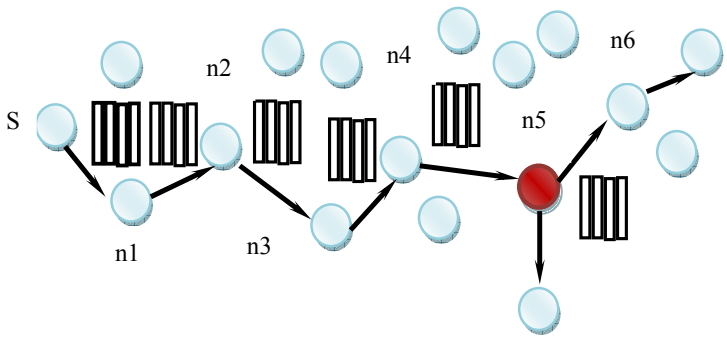

Figure-1. Misbehaving node.

1.3 Misbehaviour Report Authentication (MRA)

MRA is designed to reactivate the weakness of watchdog when it fails to detect misbehaving nodes in the presence of false misbehaviour report. Every false misbehaviour report can be generated by fake attackers to falsely report the innocent nodes as malicious. These attacks can be lethal to the entire topology when the attackers link breakage sufficient nodes and thus cause a network division. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the unknown reported packet is received or already received, then it is safe to conclude on a false misbehaviour report and whoever receives this report is marked as malicious. Otherwise, the received report is trusted and accepted. By the adoption of MRA report scheme, EA3ACK is capable of detecting malicious nodes despite the existence of false misbehaviour report.

1.4 Problem description

The A3ACKs improves network performance in the presence of consecutive collaborative misbehaving nodes in a route of active and passive path for both low speed and high speed networks. Even though in A3ACK, the network security is more robust, the utilized energy and network routing overhead increases. EE-EA3ACK, with the implementation of MRA along with elliptical cryptography increases the remaining energy, throughput and reduces memory allocation and time taken, overhead of the routing network. Further, there is need to decrease the energy consumption through the period of key exchange.

2. LITERATURE SURVEY

Elliptic curve cryptosystems were done by N. Koblitz *et al* (1987). An elliptic curve implementation of the finite field digital signature algorithm was taken up by Neil Koblitz et al (1998). Selecting cryptographic key sizes was analyzed by A. K. Lenstra *et al* (2001). On the unpredictability of bits of the elliptic curve Diffie-Hellman scheme was done by D. Boneh *et al* (2001). Elliptic curves and side-channel attacks in public key cryptography was highlighted by E. Brier et al (2002). An elliptic curve cryptography (ECC) cipher suite for transport layer security was completed by S. Blake-Wilson et al (2006). An acknowledgment-based approach for the detection of routing misbehaviour in MANETs was done by Balakrishnan *et al* (2007). Bits security of the elliptic curve Diffie-Hellman secret keys were displayed by D. Jetchev et al (2008). Design of a new security protocol using hybrid cryptography algorithms was discussed by S. Subasree *et al* (2010). Public keys were found by A. K. Lenstra *et al* (2012). EAACK - a secure intrusion detection system for MANETs was done by Shakshuki *et al* (2013). Implementation of A3ACKs intrusion detection system under various mobility speeds was analyzed by Abdulsalam *et al* (2014). An enhanced intrusion detection system for MANETS using hybrid key cryptography was done by B.Suruthi *et al* (2014). Performance comparison of routing protocol in MANET was analyzed by K.Prabu *et al* (2012). Energy efficient routing in MANET through edge node selection using ESPR algorithm was analyzed by K.Prabu *et al* (2014). Energy efficient routing protocol with Ad hoc On-Demand distance vector for MANET was done by K.Thamizhmaran *et al* (2015).

3. EXISTING SYSTEM

3.1. EAACK (Enhanced Adaptive Acknowledgement) scheme

EAACK tackles problems such as false misbehaviour, limited transmission power and receiver collision. EAACK consists of 3 parts, acknowledgement ACK, S-ACK and Misbehaviour Report Authentication (MRA). This scheme is capable of detecting malicious nodes even in case of false misbehaviour report. In this scheme, the source node does not trust misbehaviour report without confirming the misbehaviour of nodes. During MRA mode, source node seeks for alternate routes to destination using DSR routing. In order to ensure the integrity, all the acknowledgement packets in this scheme are digitally signed by nodes.

3.2. A3ACKs (Adaptive Three Acknowledgements) scheme

It is an extension of the T-ACK scheme which aims to solve three weaknesses of the watchdog scheme, which are limited transmission power, received collision and collaborative attacks especially if there are two consecutive collaborative misbehaving nodes in a route path. In this existing scheme we assume that the misbehaving nodes cooperative to forward routing packet but they drop all data packets. The A3ACK technique is an acknowledgement scheme based on one of the reactive routing protocol. It consists of three main models, named, 1-Ack, 2-Ack and 3-Ack models. The T-ACK model works similar to TWOACK scheme that detects misbehaving nodes instead of links. In T-ACK model, the third node for every three consecutive nodes in active route path has to send back a T-ACK packet to first node. This process is carried out by every three linked nodes in a route path.

4. PROPOSED SYSTEM

4.1. Elliptical curve cryptography

The method for obtaining public and private keys has generated considerable interest since key sizes can be made very smaller (in bits) while offering the same level of security algorithm. The smaller key size also implies much lower processing and power requirements for encryption and decryption of each data. Elliptic curve cryptography system, whose security rests on the discrete algorithm problem over the points on elliptic curve. ECC hybrid cryptography can be used to provide both an encryption scheme and a decryption scheme. The elliptic curve cryptography discrete algorithm problem can be stated as a prime p and an elliptic curve xP as shown in Figure-2.

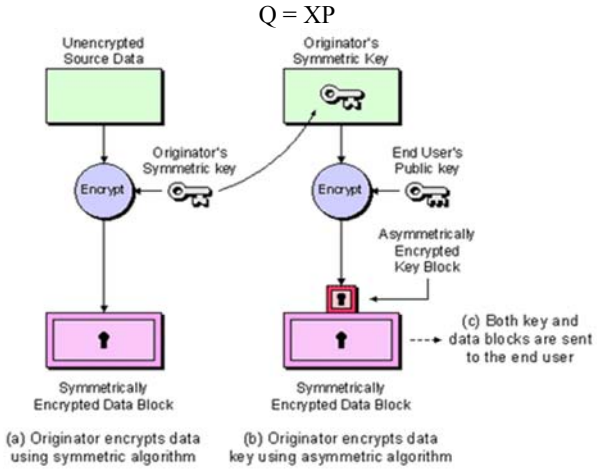

Figure-2. Elliptical curve cryptography.

4.2. Mathematical details of implementation

When setting up an elliptic curve cryptography system, there are three basic decisions that need to be made in the selection of

- The underlying finite field Fp.
- The representation for the elements of Fp.
- The elliptic curve E over Fp.
- The curve point.

4.3. Key exchange

The purpose of the Diffie-Hellman key exchange is to generate a point, which will act as an elliptical key algorithm for a classic cryptography system. The public key cryptography is used only to exchange key and subsequently conventional cryptography is used. The key exchange procedure in ECC is as follows. Suppose 2 persons, X and Y, need to communicate via system, a key is exchanged secretly between X and Y and further communication takes place using conventional cryptosystem.

4.4. Encryption and decryption

a) System entities

- A Galois finite field GF is elliptical curve cryptosystem P (x) with an access point P lying in GF.
- Zp denotes the order of P.
- GF, P (A), P and Zp are made public key.

b) Secret key generation

- Generate a random number k, Zp-1
- Compute Q=KP.
- Point Q is made Public.
- K is made private or secret key.

c) Encryption process (Suppose X sends a message m to Y)

- Look up B's Public Key: Q.
- Represent the TX message 'm' as a pair of the field elements (m1, m2), m1 GF, m2 Zp-1.
- Select a random integer, such that Zp-1
- Compute the point (A1, B1) = P
- Compute the point (A2, B2) = Q.
- Combine both the field elements m1, m2 with A2, and B2 with an algorithm to give two field elements c1 and c2.
- Transmit the data m = (A1, B1, c1, c2) to Bob.

d) Decryption process (B gets the text m = (A1, B1, c1, c2) from A)

- Compute the point (A2, B2) = k (A1, B1), using its private key k.
- Decrypt m1 and m2 from m. The prime p used in the ECC hybrid system can be smaller than the numbers required in all the other types of cryptograms, so

another advantage of the ECC is that the modified calculations required are carried out over a smaller modified operation. This leads to a significant improvement in efficiency in the operation of the ECC over both integral factorization and discrete algorithm cryptograms.

5. METHODOLOGY

5.1. Elliptical hybrid cryptography

Symmetric key ciphers are significantly faster than asymmetric ciphers, but require all parties to somehow share a secret (the key). The asymmetric key algorithms allow public key infrastructures and key exchange systems, but at the cost of speed. The message itself is then encrypted using the symmetric key cipher and the secret key. Both the encrypted secret key and the encrypted secure message are then sent to the recipient. The recipient decrypts the secret key first, using his/her own plane private key, and then uses that key to decrypt the message. Elliptical cryptographic algorithms are used with a view to obtain the merits of the systems. The method should be completely secure. The encryption / decryption cryptography process should not take longer time. The generated cipher text should be compact in size. The key exchange problem should be solved by the new method.

5.2. Simulation methodology

To better investigate the performance of EE-EA3ACK scenario, it is used to test the Intrusion Detection System (IDS) performance, when the attackers are smart enough to acknowledge packets and claim positive result while, in fact, it is negative. As watchdog is a un-acknowledgment-based scheme, it is not eligible for this scenario setting.

Scenario 1: In this scenario, a low level basic packet dropping attack is simulated. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario type is to test the performance of IDSs against three weaknesses of watchdog, namely, receiver collision, collaborative and limited transmission power.

Scenario 2: This scenario is designed to test IDSs' performance against false misbehaviour report. In this case, malicious nodes always drop the packets that they receive and send back a false misbehaviour report whenever it is possible.

Scenario 3: This scenario is used to test the new IDSs' system performances when the attackers are smart enough to acknowledge packets and claim positive result while, in fact, it is negative.

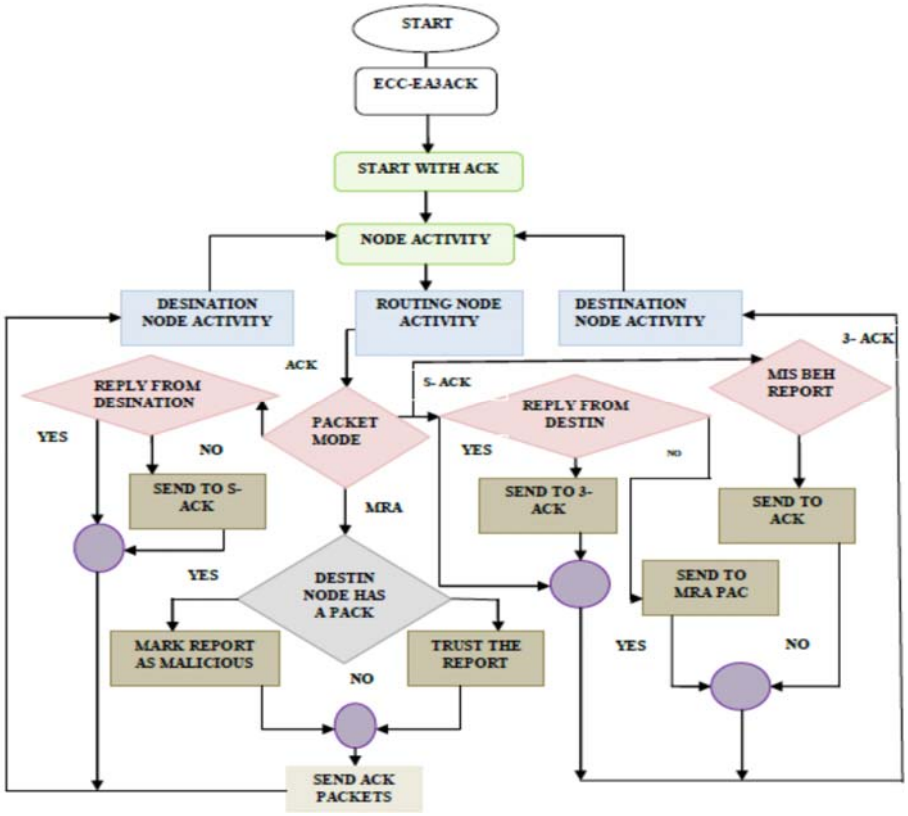

Figure-3. Flow diagram of EE-EA3ACK.

In this section, the proposed EE-EA3ACK scheme is described in detail. The approach described in this research paper is based on the previous work (Shakshuki *et al.* 2013), where the backbone of EE-EA3ACK was proposed and evaluated through implementation. It is extended with the introduction of MARS4 Hybrid cryptography to prevent the attacker from forging acknowledgment packets. EE-EA3ACK consists of four major parts, namely, ACK, secure ACK (S-ACK), 3-ACK and misbehaviour report authentication (MRA). In order to distinguish different packets in different types of schemes, in EE-EA3ACK, 3 b of the different types of packets is used. Details are listed in Table-1 and Figure-3 describes the EE-EA3ACK scheme. It should be noted that, in the proposed effective secure scheme, it is assumed that the link between every node in the network is full duplex bidirectional. Furthermore, for each communication process, both the transmitted node and the receiver node are not malicious, unless all acknowledgment and message packets described in this research are required to have two different keys (public and private), one key for the sender and the verified other key for the receiver.

Table-1. Packet type indicators.

Packet type	General data	ACK	S-ACK	3-ACK	MAR
Packet flag	001	010	011	100	101

5.3. Simulation configurations

To facilitate the comparison of the simulation results with other research works, the default scenario setting in NS 2.34 has been adopted. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the non-wired extension of NS2, where the total bits transmitted is calculated using application layer data packets only and total energy.

Table-2. Simulation parameter.

Parameter	Value
Simulation area	1,000 m * 1,000 m
Number of nodes	60
Average speed of nodes	0–25 meter/second
Mobility model	Random waypoint
Number of packet senders	40
Transmission range	250 m
Constant bit rate	2 (packets/second)
Packet size	512 bytes
Node beacon interval	0.5 (seconds)
MAC protocol	802.11 DCF
Initial energy/node	100 joules
Antenna model	Omni directional
Simulation time	500 sec

6. RESULTS AND DISCUSSIONS

Scenario 1

In scenario 1, all malicious nodes are set to drop all the packets that pass through it. Table-3 shows the simulation results of scenario 1.

Table-3. Results of scenario - 1.

Scenario - 1 Packet delivery ratio					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	1	0.96	0.97	0.93	0.91
EA3ACK	1	0.97	0.97	0.96	0.95
EE-EA3ACK	1	0.98	0.97.5	0.96	0.95
Scenario - 1 Routing overhead					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	0.15	0.28	0.35	0.44	0.58
EA3ACK	0.14	0.26	0.32	0.40	0.55
EE-EA3ACK	0.12	0.22	0.27	0.30	0.53
Scenario - 1 Throughput					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	0	0.27	0.40	0.53	0.57
EA3ACK	0	0.37	0.50	0.63	0.58
EE-EA3ACK	0	0.43	0.58	0.68	0.71
Scenario - 1 Remaining energy					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	1	0.95	0.89	0.80	0.76
EA3ACK	1	0.92	0.84	0.76	0.72
EE-EA3ACK	1	0.98	0.94	0.86	0.81

From Figure-4 and Table-3 it is clear that our proposed scheme EE-EA3ACK surpassed EA3ACK performance by above 95% when there are 10% and 20% of malicious nodes in the network. EE-EA3ACK is able to detect misbehaviours in the presence of receiver collision, limited transmission power and partial dropping.

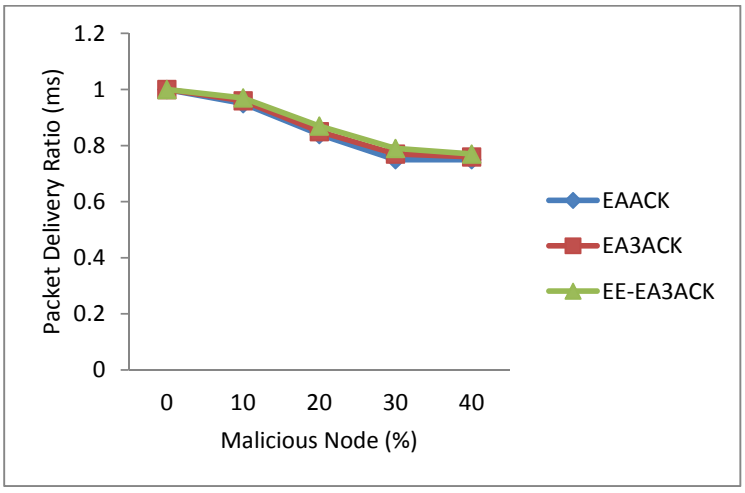

Figure-4. PDR vs. malicious nodes.

Simulation results of routing overhead in first scenario are shown in Figure-5 and Table-3 It is noted that EE-EA3ACK has the lowest overhead compared with EA3ACK & EAACK when there are 10% to 30% malicious nodes.

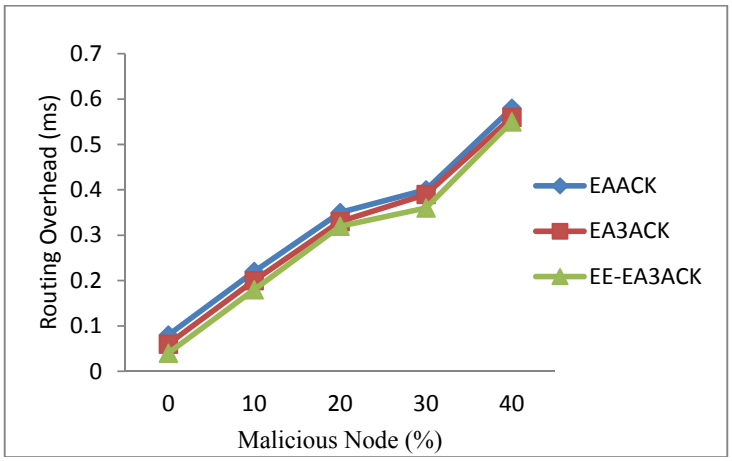

Figure-5. Routing performance vs. malicious nodes.

It is observed from Figure-6 and Table-3 that when compared with DSA algorithm, EE-EA3ACK shows throughput increased with increase in the number of malicious nodes.

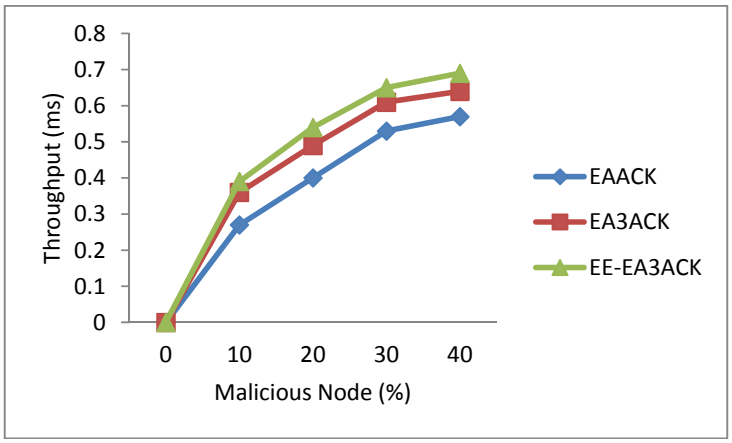

Figure-6. Throughput vs. malicious nodes.

From Figure-7 and Table-3 it is evident that the proposed EE-EA3ACK increases the remaining energy with the increasing malicious nodes compared to EA3ACK and EA3ACK algorithms.

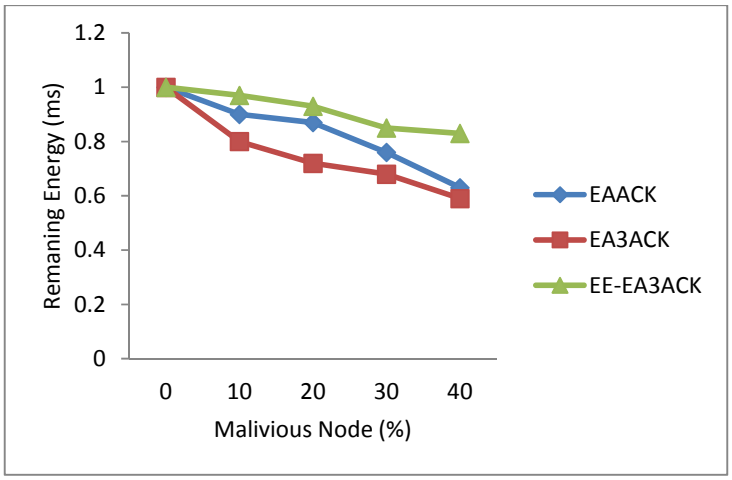

Figure-7. Remaining energy vs. malicious nodes.

Scenario 2

In this scenario, all malicious nodes are set to send out false misbehaviour report to the source node whenever possible. This scenario setting is designed to test the performance of IDS's under the false misbehavior report.

Table-4. Results of scenario - 2.

Scenario – 2 Packet delivery ratio					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	1	0.95	0.92	0.87	0.79
EA3ACK	1	0.96	0.93	0.87.5	0.80
EE-EA3ACK	1	0.96	0.94	0.89	0.83
Scenario - 2 Routing overhead					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	0.22	0.25	0.33	0.32	0.64
EA3ACK	0.20	0.24	0.32	0.31.5	0.63
EE-EA3ACK	0.18	0.22.5	0.31.5	0.30	0.61
Scenario - 2 Throughput					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	0	0.37	0.48	0.53	0.54
EA3ACK	0	0.39	0.52	0.61	0.59
EE-EA3ACK	0	0.40	0.54	0.63	0.63
Scenario - 2 Remaining energy					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	1	0.92	0.87	0.79	0.71
EA3ACK	1	0.81	0.76	0.71	0.63
EE-EA3ACK	1	0.99	0.95	0.87	0.84

Figure-8 and Table-4 show achieved simulation results based on PDR. When malicious nodes are 15% to 35%, EE-EA3ACK performs 1.5% better than EAACK & EA3ACK.

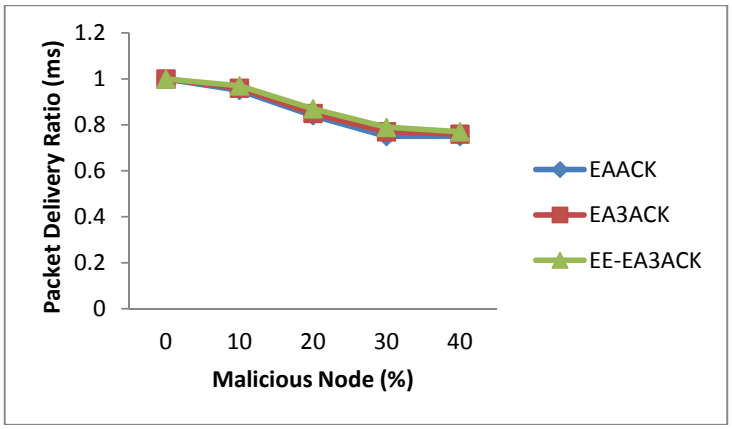

Figure-8. Packet delivery ratio vs. malicious nodes.

Figure-9 and Table-4 display the proposed EE-EA3ACK results which provide better performance when malicious nodes are 15% to 40% compared to the existing 3% routing overhead which is decreased than EAACK and EA3ACK.

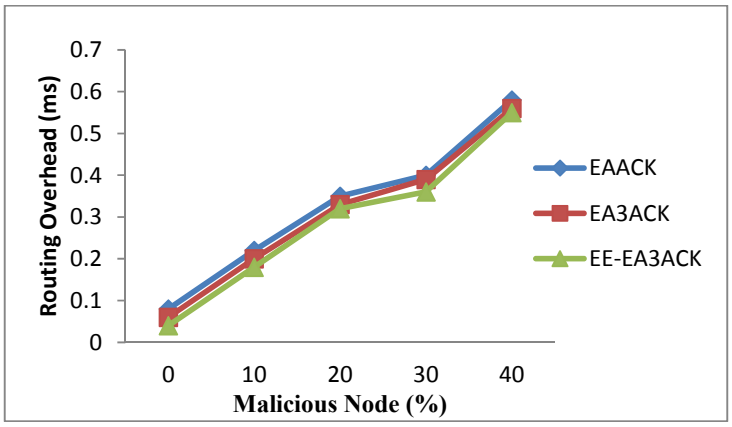

Figure-9. Routing performance vs. malicious nodes.

According to Figure-10 and Table-4 it is clear that the proposed EE-EA3ACK provides better performance with 30% to 40% malicious nodes, compared to EAACK and EA3ACK with throughput increased.

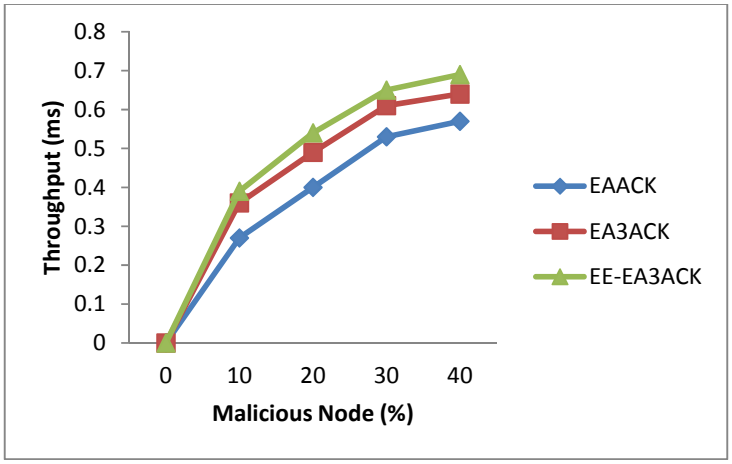

Figure-10. Throughput vs. malicious nodes.

Figure-11 and Table-4 proves that the proposed EE-EA3ACK provides better performance of the remaining energy when there are 15% to 40% of malicious nodes compared to EAACK and EA3ACK.

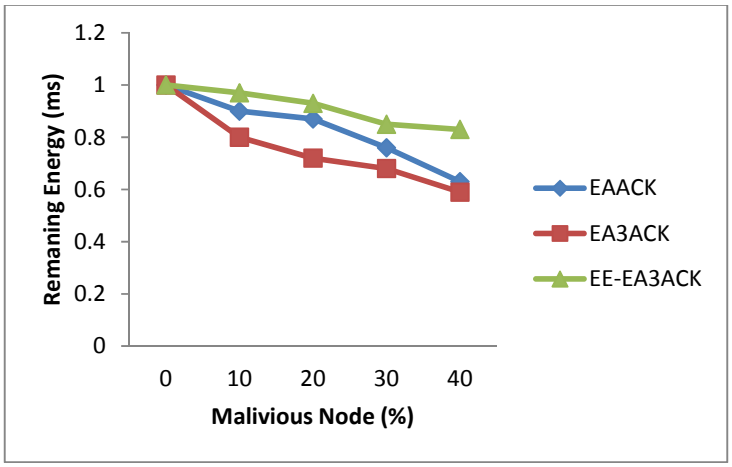

Figure-11. Remaining energy vs. malicious nodes.

Scenario 3

In this scenario, the malicious nodes were provided the ability to intermediate forge acknowledgment packets. This way, malicious nodes simply drop all the fake report packets that they receive and send back forged positive acknowledgment packets to their previous node whenever necessary. This is an overall common method for attackers to degrade network performance while still maintaining its reputation.

Table-5. Results of Scenario - 3.

Scenario - 3 Packet delivery ratio					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	1	0.95	0.84	0.75	0.75
EA3ACK	1	0.96	0.85	0.77	0.76
EE-EA3ACK	1	0.97	0.87	0.79	0.77
Scenario - 3 Routing overhead					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	0.08	0.22	0.35	0.40	0.58
EA3ACK	0.06	0.20	0.33	0.39	0.56.5
EE-EA3ACK	0.04	0.18	0.32	0.36	0.55
Scenario - 3 Throughput					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	0	0.27	0.40	0.53	0.57
EA3ACK	0	0.36	0.49	0.61	0.64
EE-EA3ACK	0	0.39	0.54	0.65	0.69
Scenario – 3 Remaining energy					
Routing / Malicious node	**0%**	**10%**	**20%**	**30%**	**40%**
EAACK	1	0.90	0.87	0.76	0.63
EA3ACK	1	0.80	0.72	0.68	0.59
EE-EA3ACK	1	0.97	0.93	0.85	0.83

Scenario 3 is pictured in Figure-12 and Table-5 with the achieved simulation results. In all acknowledgment-based IDSs, the proposed scheme EE-EA3ACK surpasses EA3ACK and EAACK performance by above 95% when there are 30% and 40% of malicious nodes in the network. EE-EA3ACK is able to detect misbehaviors in the presence of receiver collision, limited transmission power, collision and partial dropping.

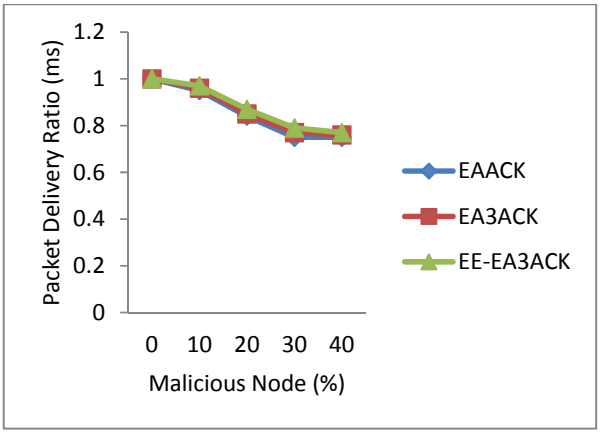

Figure-12. PDR vs. malicious nodes.

Figure-13 and Table-5 clearly show DSR scheme achieve the best performance, as they do not require acknowledgment scheme to detect misbehaviours. For the rest of the IDSs, EE-EA3ACK has the lowest overhead

than other algorithms when the malicious nodes are increased.

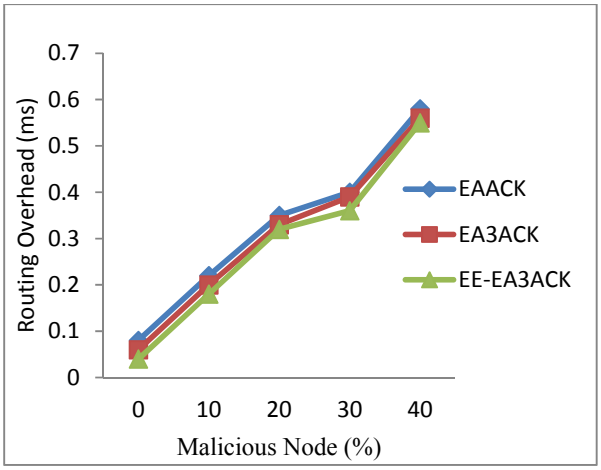

Figure-13. RO vs malicious nodes.

Figure-14 and Table-5 clearly depict comparison of EA3ACK & EAACK with corresponding RSA and DSA algorithm along with EE-EA3ACK where it shows the throughput increased with increase in the number of malicious nodes on by 30% and 40%.

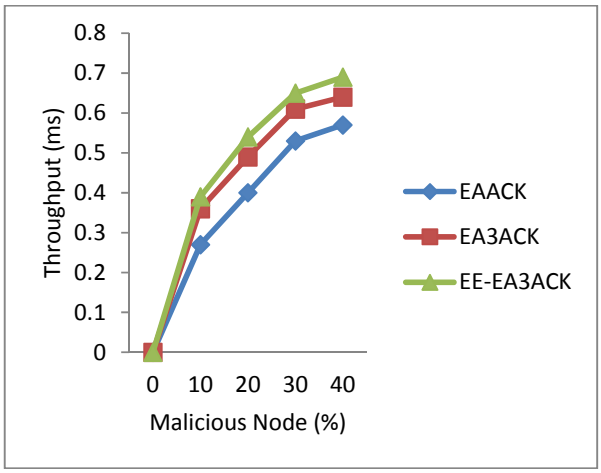

Figure-14. Throughput vs. malicious nodes.

Figure-15 and Table-5 clearly show that the proposed EE-EA3ACK increases the remaining energy with increasing malicious nodes compared to EAACK & EA3ACK.

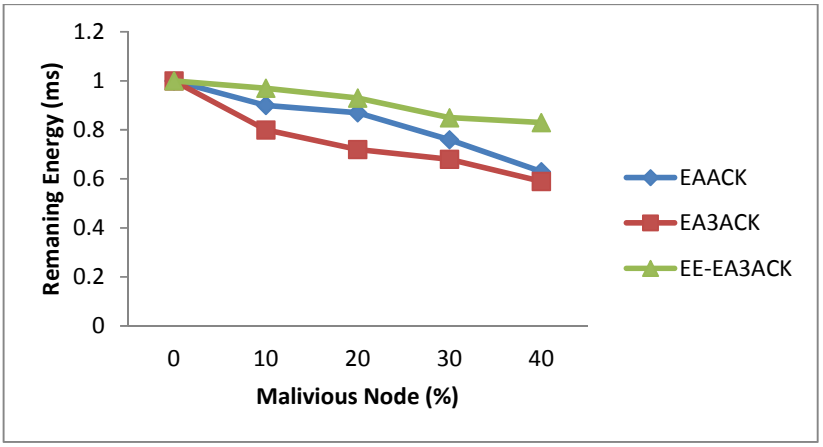

Figure-15. Remaining energy vs. malicious nodes.

7. CONCLUSION AND FUTURE WORK

Packet-dropping and loss attack have always been a major threat to the security in MANETs. In this research paper, a novel IDS approach named EE-EA3ACK protocol specially designed for MANETs is proposed in comparison with other popular techniques in different scenarios through simulations. The results demonstrated positive performance of the remaining energy in EE-EA3ACK than EAACK, EA3ACK in the cases of receiver collision, limited transmission power, and false misbehaviour report and collaborative attacks. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, the research was extended to incorporate elliptical curve cryptography in this proposed scheme. Although it generates more end-to-end delay in some cases, as demonstrated in this research, it can vastly improve the network's PDR to more than 1.5% compared to the existing EAACK and EA3ACK routing protocol and improve remaining energy by 6% compared to the existing EAACK and EA3ACK routing protocol when the attackers are smart enough to forge acknowledgment packets. Both MARS4 and ECC cryptography schemes were implemented in the simulation. Eventually, it is arrived to the conclusion that the EE-EA3ACK scheme is more suitable to be implemented in MANETs. To increase the merits of this

research work, there is a plan to investigate the following issues in our future research.

a) The same concept can be applied in satellite to reduce more congestion in the route and also to save more energy.

b) The possibilities of adopting the shortest path algorithm to eliminate the requirement of redistributed end to end delay can be examined.

c) The performance of EE-EA3ACK can be tested in real time network environment instead of software simulation.

REFERENCES

Abdulsalam, *et al*. 2014. Implementation of A3ACKs intrusion detection system under various mobility speeds. Proc. 5th International Conference on Ambient System, Networks and Technologies (ANT-2014).

Balakrishna, *et al.* 2007. An Acknowledgment-based Approach for the Detection of Routing Misbehaviour in MANETs. IEEE Conference. pp. 1-35.

Blake-Wilson S. *et al*. 2006. Elliptic curve cryptography (ECC) cipher suites for transport layer security. TLS. RFC 4492, pp. 1-32.

Boneh D. *et al*. 2001. On the unpredictability of bits of the elliptic curve Diffie-Hellman scheme. Springer. 2(13): 201-212.

Brier E. *et al*. 2002. Elliptic curves and side-channel attacks in Public Key Cryptography. Springer. 2(27): 335-345.

Jetchev D. *et al*. 2008. Bits security of the elliptic curve Diffie-Hellman secret keys. Springer. 5(157): 75-92.

Koblitz, N. *et al*. 1987. Elliptic curve cryptosystems. Mathematics of Computation. 48(177): 203-209.

Koblitz, N. *et al*. 1998. An Elliptic Curve implementation of the finite field digital signature algorithm. Springer. 14(62): 327- 337.

Lenstra A.K. *et al*. 2001. Selecting cryptographic key sizes. Journal of Cryptology. 14(4): 255-293.

Lenstra, A.K. *et al*. 2012. Public keys. Springer. 7(41): 626-642.

Prabu K. and Subramani A. 2012. Performance comparison of routing protocol in MANET. Int. J. of Adv. Research in Com. Sci. and Soft Engg. 2(9): 388-392.

Prabu K. and Subramani A. 2014. Energy efficient routing in MANET through edge node selection using ESPR algorithm. Int. J. Mobile Network Design and Innovation. 5(3): 166-175.

Shakshuki et al. 2013. EAACK - A Secure Intrusion Detection System for MANETs. IEEE Trans. 60(3): 1089-1098.

Subasree S. *et al*. 2010. Design of a New Security Protocol Using Hybrid Cryptography Algorithms. IJRRAS. 2(2): 95-103.

Suruthi B. et al. 2014. An Enhanced Intrusion Detection System for MANETS using Hybrid Key Cryptography. IJCSIT, IJCSIT. 5(2): 1152-1154.

Thamizhmaran, K. *et al.* 2015. Energy Efficient Routing Protocol with Ad hoc On-Demand Distance Vector for MANET. IEEE Explore. 2: 158-163.