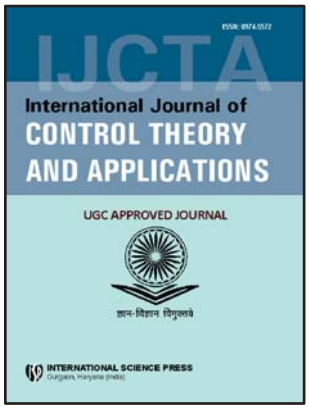


**International Journal of Control Theory and Applications**

ISSN : 0974-5572



**Volume 10 • Number 30 • 2017**

# Comparison and Parameter Adjustment of Topology Based (S-EA3ACK) for MANETs

**K. Thamizhmaran[a] M. Anitha[a] and Alamelu Nachiappan[b]**

[a]*Dept. of ECE, Annamalai University, Annamalai Nagar – 608 002, Tamilnadu, India*

[b]*Dept. of EEE, Pondicherry Engineering College, Puducherry-605014, India*

***Abstract :*** - In Mobile Ad-hoc Networks (MANET), there is no fixed infrastructure to observe or assign the resources used by the mobile nodes. They connect or disconnect from the active network any time and transfer packets in a single or a multicast mode. Nodes are connected by way of wireless links and form a random topology. This research paper focuses on, a new Intrusion Detection System (IDS), Secure-Enhanced Adaptive 3 Acknowledgement (S-EA3ACK), using EAACK with hybrid cryptography specially designed for MANET. Furthermore, all the above mentioned protocols are compared based on several important performance metrics which are Packet Delivery Ratio (PDR), end-to-end delay and average energy via Network Simulator 2 (NS2) is used to implement and test the suggested system under various size of topology with different sets of nodes as well as comparing the results with the results of some closely existing IDS mechanism.

***Keywords:*** *MANET, Watchdog, EAACK, S-EA3ACK, MRA, MARS4, PDR, DELAY, ENERGY.*

## 1. INTRODUCTION

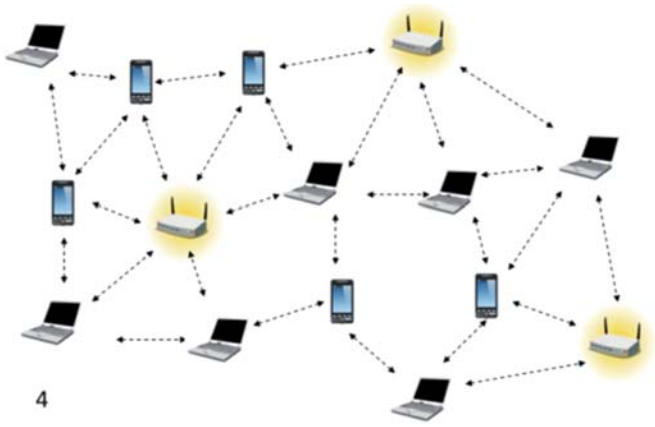


**Figure 1: Mobile Adhoc Network**

A MANET is a collection of all independent mobile nodes that communicate with each other via radio waves. The mobile nodes that are in the radio range of each other communicate directly. These networks are fully dynamically distributed, and 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 like battery power and bandwidth of topology as shown in Fig 1. Different approaches have already been proposed to detect and prevent the misbehaviour in MANET.

## 1.1. Routing Protocol

A 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. The two main types of routing are static routing and dynamic routing. The router learns how to get to the remote network either through static or dynamic routing. Generally, there are two different stages in routing-they are route discovery and

forwarding data packets. In route discovery, the route to a destination is discovered by broadcasting the query. Then, once the unbreakable route has been established, data forwarding is 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 transmitting control messages, optimization of the size of headers and efficient active route reconfiguration are considered when developing a routing protocol (Fig 2).

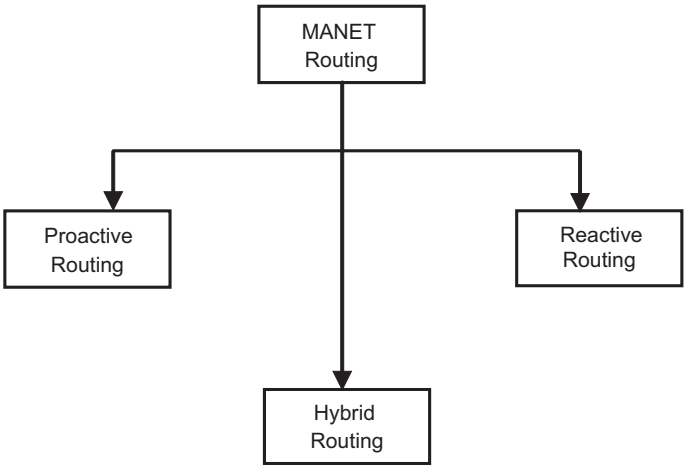


**Figure 2: MANET Routing Protocols**

The attacks in MANET are divided into two major types, internal and external.

## 1.2. Internal Attacks

Internal attacks directly lead to the attacks on nodes present in network and link interface between them. This type of attacks may broadcast a wrong type of routing information to the other nodes. Internal attacks are sometimes more difficult to handle compared to external attacks because internal attacks occur due to more number of trusted nodes. The wrong routing information generated by compromised nodes or malicious nodes are difficult to identify. This is due to the compromised nodes that are able to generate the valid signature using their private keys.

## 1.3. External attacks

This type of attacks tries to cause traffic in the network, denial of services, and advertising incorrect routing information etc. External attacks prevent the network from normal communication and produces additional overhead to the network.

### 1.4. Watch dog

A monitoring method used for ad-hoc and sensor networks, is the basis of many misbehaviour detection algorithms and trust or reputation systems. If a watchdog identifies that a packet is not delivered within a definite period or is forwarded but altered by its neighbour, it deems the neighbour as misbehaving. When the misbehaviour rate of a node surpasses certain threshold, the source is notified and subsequent packets are forwarded along the routes which exclude that node. Infrastructure less networks, attack detection and reaction are the key issues to the whole network. The suggested approach S-EA3ACK is designed to tackle proved authors four of the six weaknesses of watchdog scheme, namely, receiver collision, limited transmission power, false misbehaviour, and partial dropping.

## 2. LITERATURE REVIEW

The quality of service in ad-hoc on-demand distance vector routing was done by C.E. Perkins et al. (2001). The dynamic source routing protocol for mobile ad-hoc networks was taken up by Johnson et al. (2002). The malicious node detection in AODV- based mobile ad-hoc networks was analyzed by Jongoh Choi et al. (2005). A novel fast hybrid cryptographic system was designed by Sheena Mathew et al (2006). An acknowledgment based approach for the detection of routing misbehaviour in MANET was highlighted by K. Liu et al. (2007). The detection of packet dropping attack using improved acknowledgement based scheme in MANET was discussed by Aishwarya Sagar et al (2010). Secure routing for wireless mesh networks was analyzed by Celia Li et al. (2011). Secure routing protocol in MANET survey was displayed by K.Thamizhmaran et al. (2012). EAACK - A secure intrusion detection system for MANET was analyzed by Shakshuki et al. (2013). The implementation of A3ACKs intrusion detection system under various mobility speeds was discussed by Abdulsalam et al. (2014). Energy efficient routing in mobile adhoc network via edge node selection using ESPR algorithm was highlighted by Prabu, K. and Subramani, A. (2014).

## 3. PROBLEM STATEMENT

Network wide routing in MANET is a vital task of transferring data from a source to the destination. The A3ACKs improve network performance in the presence of consecutive collaborative misbehaving nodes in a route of active and passive path. So it also becomes essential to monitor the constraints in the intermediate nodes. Consequently, an efficient routing scheme may generate route failures. The simplest scheme routing in MANET is the one to find a route without malicious nodes. Further, there is need to reduces the energy consumption through the period of key exchange. In this technical research paper aims to provide an unbreakable route for secured transmission. So a new routing algorithm named S-EA3ACK using EAACK with hybrid cryptography is suggested. This S-EA3ACK provides better performance compared to the existing EAACK without any misbehavior at intermediate nodes.

## 4. EXISTING METHOD

### 4.1. RSA

1. Choose two higher prime numbers P and Q, and find N = P*Q.
2. Select the encryption (public key) E & Select the decryption (private key) D. The following equation is true. (D*E) mod (P-1) * (Q-1) = 1
3. Encrypt the PT to CT = PTE mod N
4. Send CT to the receiver.

### 4.2. MAJE4

1. Encryption for a long period.
2. Uses only primitive computational operations.
3. Suitable for handheld type devices with restricted memory.
4. Use of more than one arithmetic and / or Boolean operator complicates cryptanalysis. The secured choice is with the key sizes of 128 or 256 bits.

### 4.3. MARS4

1. A encrypts the plain text (PT) with the help of MAJE4 and the symmetric key (K1) and forms the cipher text (CT).
2. Encrypt K1 (CT) to (K2) of B using RSA.
3. B now uses the RSA algorithm and its private key (K3) to decrypt K1.
4. Then B uses K1 and the MAJE4 algorithm to decrypt the CT for the plain text (PT).

## 5. METHODOLOGY

### 5.1. Hybrid cryptography

The symmetric ciphers are significantly faster than the asymmetric ciphers, but require all parties to somehow share a secret key. The asymmetric algorithms allow public key infrastructures and key exchange systems, but at the cost of speed. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient. The receiver diffusion the secret key first, uses his/her personal private key, and then uses that key to decrypt the message. The both cryptographic designs algorithms are used with a view to obtain the merits of the systems. The method is completely secure. The encryption / decryption process does not take a longer time. The generated cipher text is compact in size. The key exchange problem is solved by MAJE4.

### 5.2. Simulation methodology

This research better investigates the performance of S-EA3ACK under different topology size with different set of malicious nodes.

In this section, the suggested S-EA3ACK scheme is described in detail. The approach described in this technical research paper is based on the previous work (10) where the backbone of S-EA3ACK was developed and evaluated through implementation. It is extended with the introduction of MARS4 Hybrid cryptography to prevent the attacker from forging acknowledgment packets. EA3ACK consists of four major parts, namely, ACK, S-ACK, 3-ACK and MRA. In order to distinguish various packet types in different schemes in S-EA3ACK, 3*b* of the different types of packets is used. The details are listed in Table 1 and Fig 3 and a flowchart describing the S-EA3ACK scheme is also presented. Unless specified, all acknowledgment packets described in this research require public key and private key, one key for the transmitter and the other verified 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 |

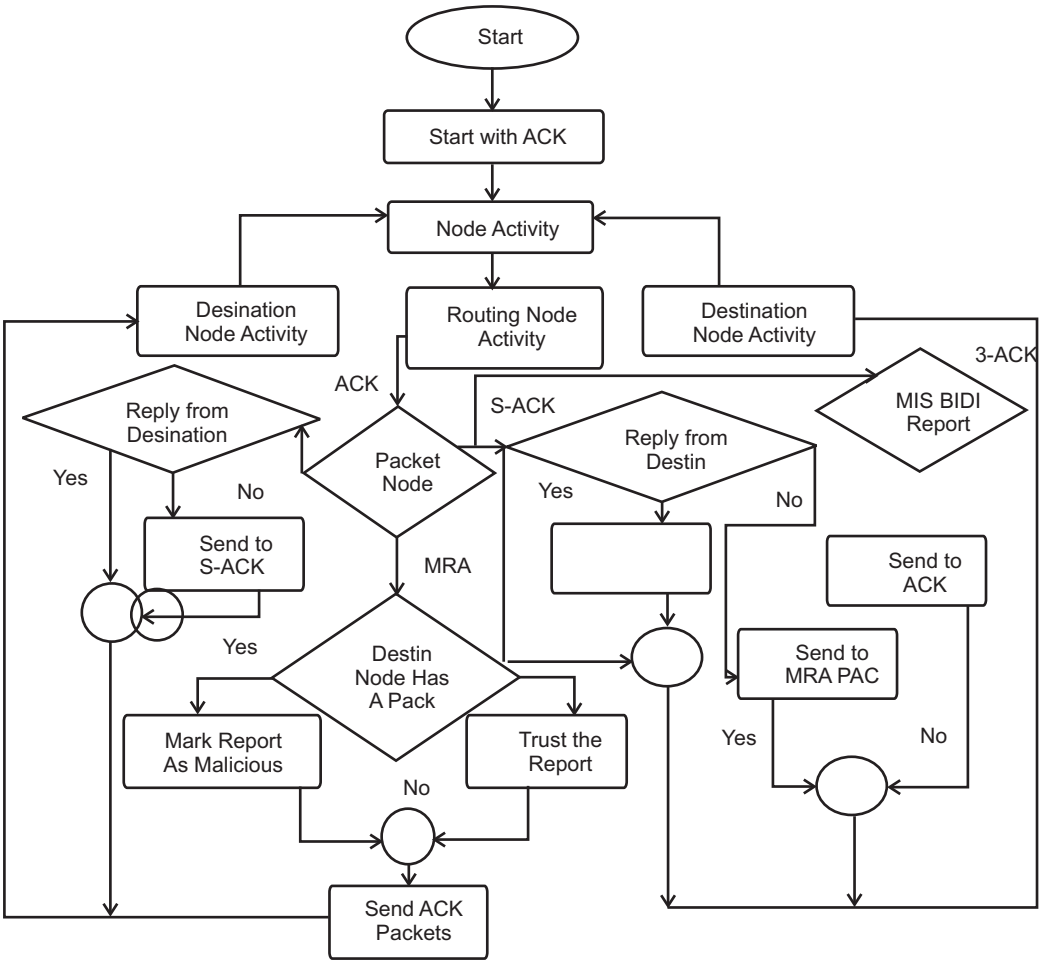


**Figure 3: Flow chart for S-EA3ACK**

## 5.3. Experimental set up

In this section, the performance of routing protocol of MANET in an open environment is evaluated. The simulations are carried out using network simulator (NS 2.34). The mobile ad-hoc routing protocols are simulated using this simulator by varying the number of nodes. The IEEE 802.11 distributed coordination function (DCF) is used as the medium access control protocol. The traffic sources are UDP. Initially, nodes are placed at certain specific locations. The simulation parameters are specified below.

**Table 2**
**Simulation Parameters**

| *Parameter* | *Values* |
|---|---|
| Simulation area | 1000m, 2000m |
| Number of nodes | 50, 100 |
| Number of malicious nodes | 10, 20 |
| Average speed of nodes | 0–25 meter/second |
| Mobility model | Random waypoint |

| *Parameter* | *Values* |
|---|---|
| Number of packets sender | 40 |
| 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, 750 sec |

## 6. RESULTS AND DISCUSSES

In this work, the malicious nodes are provided with the ability to forge acknowledgement packets. By this way, the malicious nodes simply loss all the packets that they receive and send back forged positive acknowledgement packets to their previous node whenever necessary. This is a common method for attackers to degrade network performance while still maintaining their reputation. To better investigate the performance of S-EA3ACK under two different types of topology size, two different set of nodes and two different set of malicious nodes are taken to simulate via network simulator 2. The suggested method S-EA3ACK is designed to tackle four defect of watchdog scheme, namely, receiver collision, limited transmission power, false misbehaviour, and partial dropping.

$$\text{Topology Size} = 1000\text{M},$$
$$\text{Number of nodes} = 50,$$
$$\text{Malicious nodes} = 10$$

**Table 3**
**Results of Parameter Values - 1**

| | | | | | |
|---|---|---|---|---|---|
| | | | *Packet delivery ratio* | | |
| Protocol/NN | 10 | 20 | 30 | 40 | 50 |
| EAACK (DSA) | 0.92 | 0.81 | 0.72 | 0.72 | 0.69 |
| S-EA3ACK | 0.93 | 0.82 | 0.74 | 0.74 | 0.70 |
| | | | *End – to – End delay* | | |
| EAACK (DSA) | 0.68 | 0.62 | 0.56 | 0.53 | 0.51 |
| S-EA3ACK | 0.45 | 0.41 | 0.36 | 0.29 | 0.27 |
| | | | *Remaining energy* | | |
| EAACK (DSA) | 0.88 | 0.85 | 0.74 | 0.60 | 0.57 |
| S-EA3ACK | 0.78 | 0.70 | 0.65 | 0.57 | 0.52 |

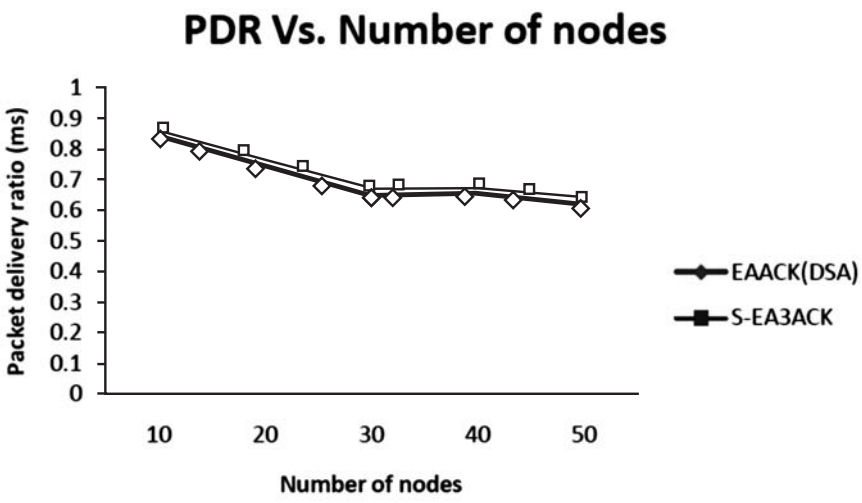


**Figure 4: PDR Vs. NNs**

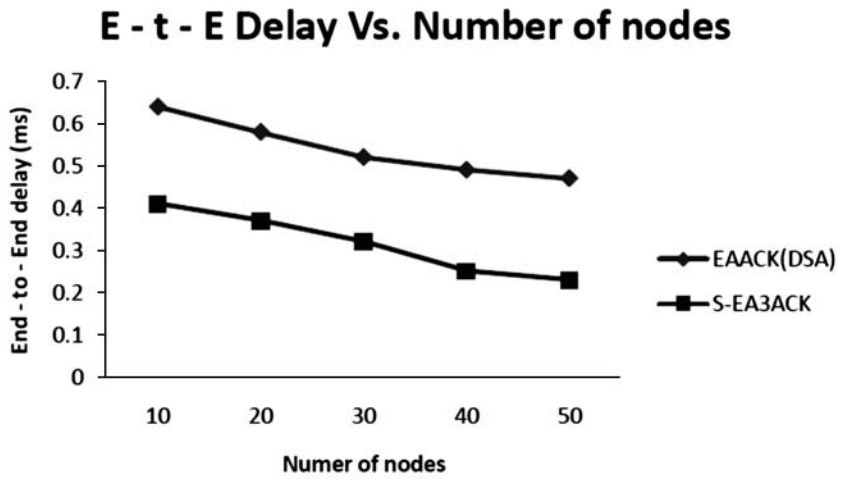


**Figure 5: End–to–End delay Vs. NNs**

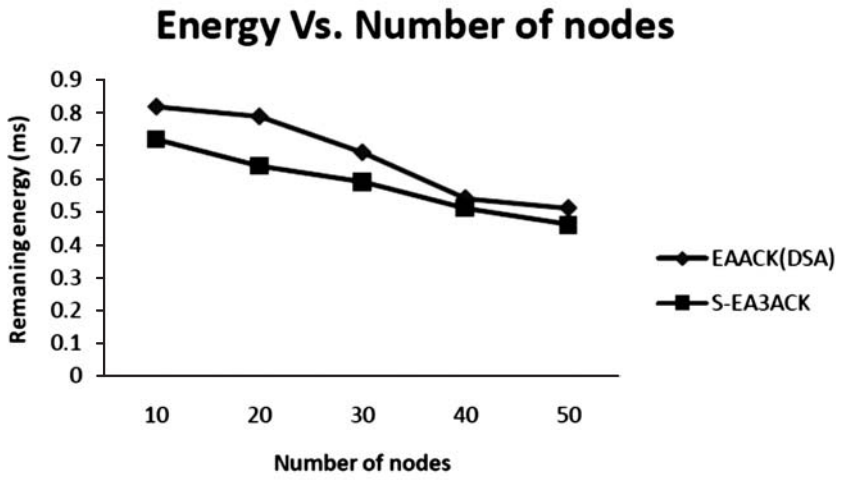


**Figure 6: Remaining energy Vs. NNs**

Fig 4 shows the graph of PDR when the topology size is 1km, the number of malicious nodes 10 and the number of nodes is increased from 10 to 50, Fig 4 and Table 3, it is clear that in all acknowledgements based IDS, the suggested scheme S-EA3ACK surpasses the performance of EAACK (DSA) which increases PDR by 1.2% when there are 10 to 50 nodes in the network. As the proposed algorithm finds more secure routes with retransmit loss packets frequently, it is possible to increase the delivery ratio.

It is observed from Fig 5 and Table 3 that when compared with EAACK (DSA) algorithm, S-EA3ACK decreases the delay by 22.4% with the increase in the number of nodes from 10 to 50. The proposed algorithm S-EA3ACK finds the primary and secondary highest forward capacity route in between the sender and receiver.

The impact of the number of nodes on the average energy is analysed using the two algorithms and the simulation results are shown in, Fig 6 and Table 3 describe the increase in the average energy obtained by the proposed S-EA3ACK when there are 10 to 50 nodes. S-EA3ACK algorithm reduces the energy by 8.4% as the proposed algorithm to increases no of connections and this system is capable of finding the minimum link failed unbreakable short route between the source and destination.

Topology Size = 1000M,
Number of nodes = 100,
Malicious nodes = 20

**Table 4**
**Results of Parameter Values - 2**

| | | | | | |
|---|---|---|---|---|---|
| | | *Packet delivery ratio* | | | |
| Protocol/NN | 20 | 40 | 40 | 60 | 100 |
| EAACK | 0.88 | 0.77 | 0.69 | 0.68 | 0.65 |
| S-EA3ACK | 0.89 | 0.79 | 0.70 | 0.70 | 0.67 |
| | | *End – to – End delay* | | | |
| EAACK | 0.66 | 0.60 | 0.54 | 0.51 | 0.49 |
| S-EA3ACK | 0.43 | 0.39 | 0.34 | 0.27 | 0.25 |
| | | *Remaining Energy* | | | |
| EAACK | 0.84 | 0.81 | 0.70 | 0.56 | 0.53 |
| S-EA3ACK | 0.74 | 0.66 | 0.61 | 0.53 | 0.48 |

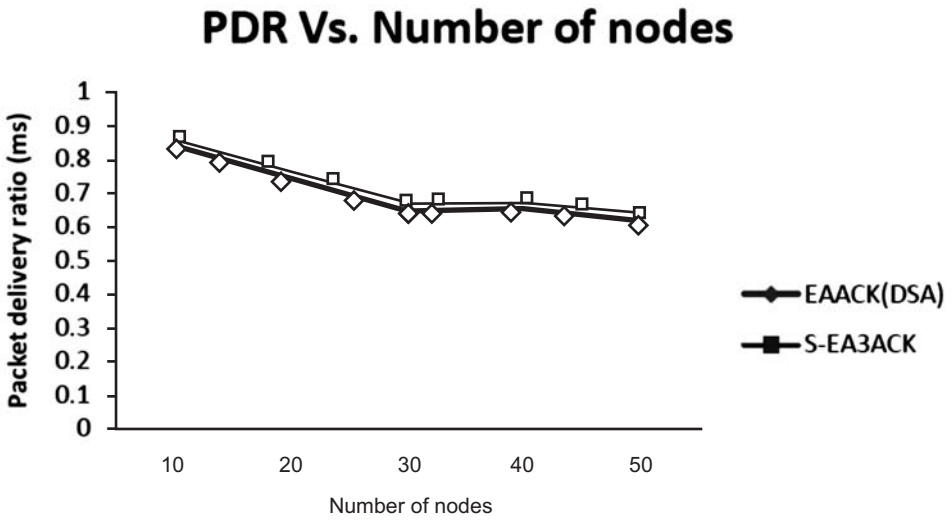


**Figure 7: PDR Vs. NNs**

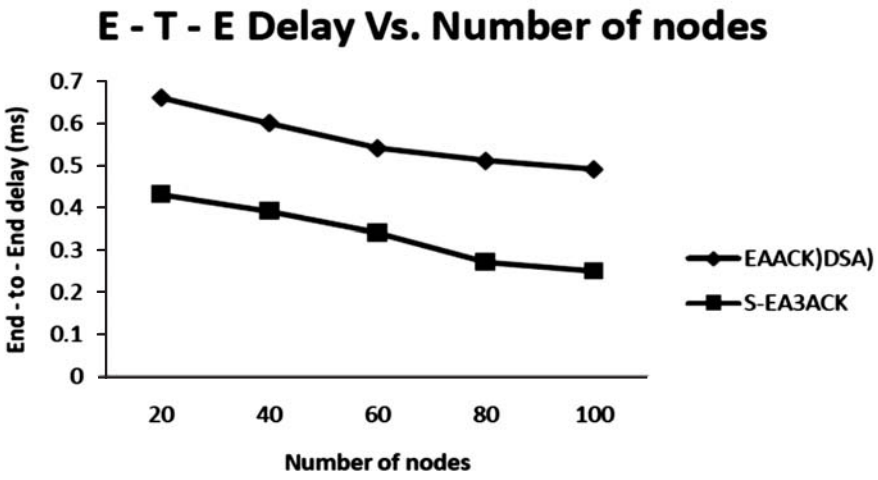


**Figure 8: End–to–End delay Vs. NNs**

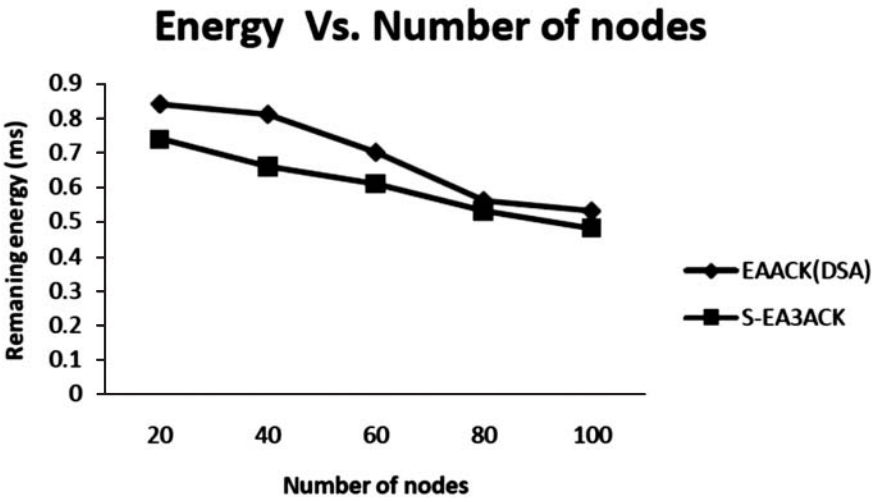


**Figure 9: Remaining energy Vs. NNs**

Table 4 & Fig 7 shows the graph of the PDR when the topology size is 1000m, the number of malicious nodes 20 and the number of nodes. The malicious node is varied from 1 to 20 and simulation is carried out to It is clear from the simulation results that the S-EA3ACK has the highest delivery ratio in comparison with EAACK (DSA), when there are 10 to 100 nodes. When the number of nodes increases, the connectivity among the nodes also increases; this enables the proposed method to identify efficient paths which in turn increase the PDR using EAACK (DSA) & S-EA3ACK methods.

It is observed from Fig 8 and Table 4 that when compared with EAACK (DSA) algorithm, S-EA3ACK decreases the delay by 22.4% with increase in the number of malicious nodes from 1 to 20 out of 100 nodes. If find misbehaviour node is detected, immediately the S-EA3ACK algorithm to use secondary highest forward capacity shortest route in between the sender and receiver.

Proposed S-EA3ACK increases the remaining energy with the increasing number of malicious nodes from 1 to 20 compared to EAACK algorithms. Fig 9 and Table 4 describe the increase in the average energy obtained by the proposed S-EA3ACK when there are 10 to 100 nodes. S-EA3ACK algorithm reduces the energy by 8.4% as the proposed algorithm to increases no of connections and this system is capable of reduce route failed between source and destination.

Transmission topology = 2000M,
Number of nodes = 50,
Malicious nodes = 10

**Table 5**
**Results of Parameter Values - 3**

| | | | | | |
|---|---|---|---|---|---|
| | | *Packet delivery ratio* | | | |
| Protocol/NN | 10 | 20 | 30 | 40 | 50 |
| EAACK | 0.85 | 0.74 | 0.66 | 0.65 | 0.62 |
| S-EA3ACK | 0.86 | 0.76 | 0.67 | 0.67 | 0.64 |
| | | *End – to – End delay* | | | |
| EAACK | 0.64 | 0.58 | 0.52 | 0.49 | 0.47 |
| S-EA3ACK | 0.41 | 0.37 | 0.32 | 0.25 | 0.23 |
| | | *Remaining Energy* | | | |
| EAACK | 0.82 | 0.79 | 0.68 | 0.54 | 0.51 |
| S-EA3ACK | 0.72 | 0.64 | 0.59 | 0.51 | 0.46 |

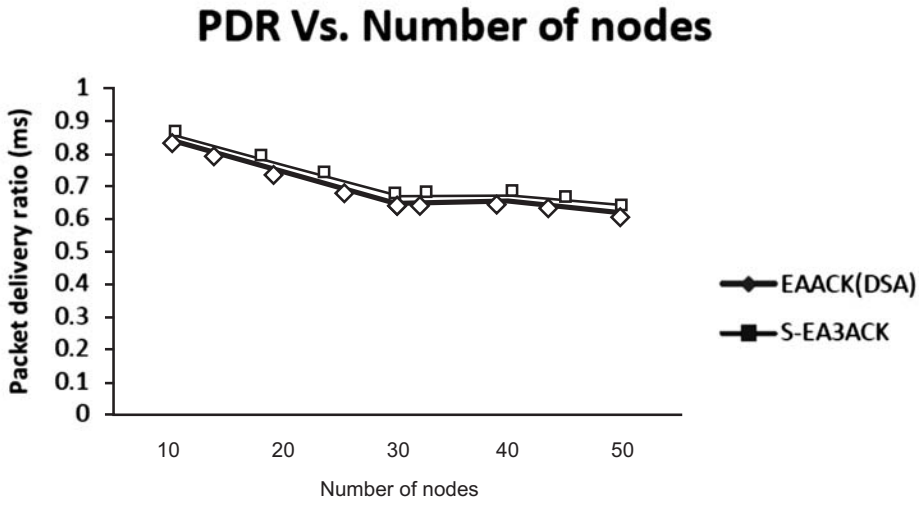


**Figure 10: PDR Vs. NNs**

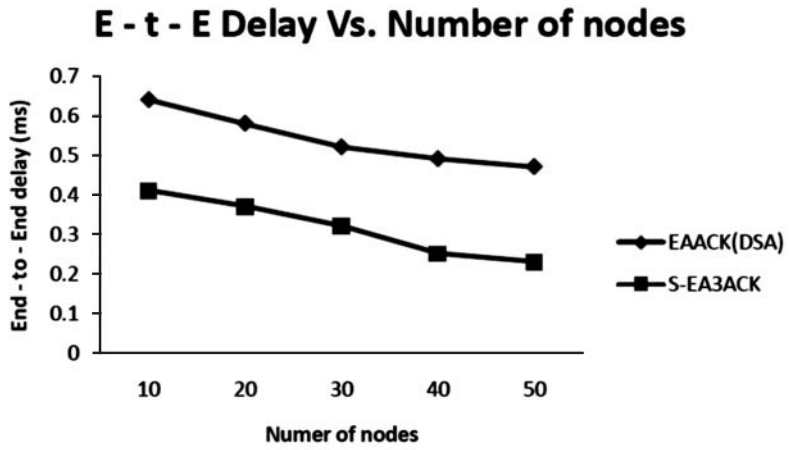


**Figure 11: End–to–End delay Vs. NNs**

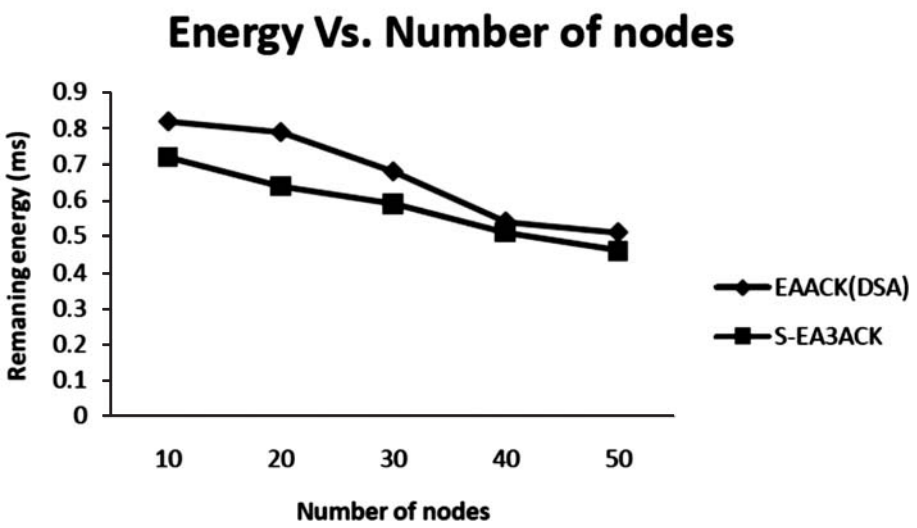


**Figure 12: Remaining energy Vs. NNs**

It is observed from Fig 10 and Table 4 that when compared with EAACK (DSA) algorithm, S-EA3ACK increases the delivery ratio by 1.6% with the increase in the number of nodes from 10 to 50. As the proposed algorithm finds maximum secure and lowest link failed route with minimum retransmit packets frequently, it is possible to increase the delivery ratio.

S-EA3ACK has the lowest delay in comparison with EAACK (DSA), when there are 1 meter to 2000 meters of transmission ranges. When the transmission range increases, the connectivity among the nodes also increases, which enables the proposed method to identify more number of alternate secondary paths which in turn reduces the delay. Fig 11 and Table 4 describe the decrease in delay obtained by the proposed S-EA3ACK when there are 10 to 50 nodes. S-EA3ACK algorithm reduces the delay by 22.4%.

Fig 12 shows the graph of the remaining energy when the topology is size 2km, the number of malicious nodes 20 and the number of nodes increased from 10 to 50. The proposed S-EA3ACK increases the remaining energy with the increasing topology size compared to EAACK. S-EA3ACK the proposed algorithm to increases no of connections and this system is capable of reduce route failed between source and destination.

Topology Size = 2000M,
Number of nodes = 100,
Malicious nodes = 20

**Table 6**
**Results of Parameter Values - 4**

| | | | | | |
|---|---|---|---|---|---|
| | | *Packet delivery ratio* | | | |
| Protocol/NN | 20 | 40 | 40 | 60 | 100 |
| EAACK | 0.79 | 0.68 | 0.60 | 0.59 | 0.56 |
| S-EA3ACK | 0.80 | 0.70 | 0.61 | 0.61 | 0.58 |
| | | *End – to – End delay* | | | |
| EAACK | 0.61 | 0.56 | 0.49 | 0.45 | 0.42 |
| S-EA3ACK | 0.39 | 0.35 | 0.30 | 0.21 | 0.19 |
| | | *Remaining Energy* | | | |
| EAACK | 0.76 | 0.73 | 0.62 | 0.48 | 0.45 |
| S-EA3ACK | 0.66 | 0.58 | 0.53 | 0.45 | 0.40 |

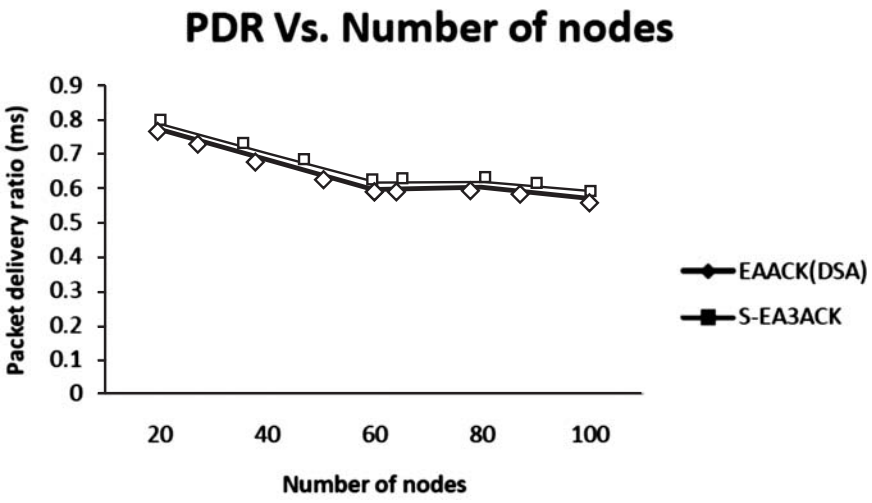


**Figure 13: PDR Vs. NNs**

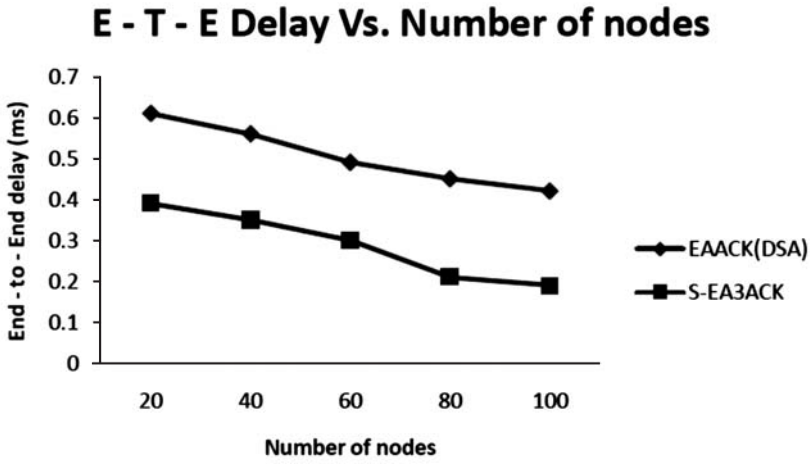


**Figure 14: End–to–End delay Vs. NNs**

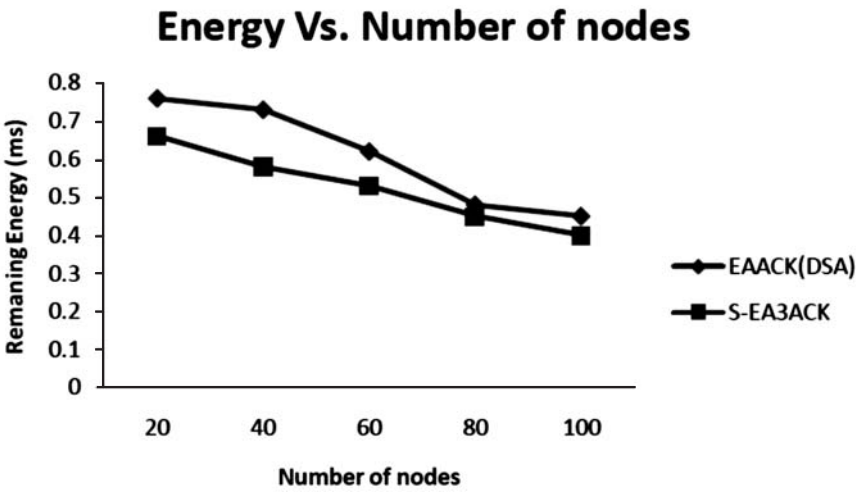


**Figure 15: Remaining energy Vs. NNs**

Fig 13 shows the graph of the PDR when the topology size is 2000m, the number of malicious nodes 20 and the number of nodes increased from 10 to 100. It is observed from Fig 13 and Table 5 that when compared with EAACK (DSA) algorithm, S-EA3ACK increases the delivery ratio by 1.6% with the increase in the number of malicious nodes.

The impact of the number of nodes on end–to–end delay is analysed using the two algorithms and the simulation results are shown in Fig 14 and Table 5. S-EA3ACK has the lowest delay in comparison with EAACK (DSA), when there are 1 meter to 2000 meters of transmission ranges with 20 malicious nodes out of 100 nodes. As the proposed algorithm finds the primary and secondary unbreakable maximum forward capacity secure link failed route, it is possible to reduce delay.

The topology size is varied from 1km to 2000m and simulation is carried out to calculate the average energy using EAACK (DSA) & S-EA3ACK methods. Fig 15 and Table 5 picture the achieved simulation results. In all acknowledgment-based IDS, the proposed scheme S-EA3ACK surpasses EAACK performance by 8.4% when there are 10 and 100 nodes in the network. As the proposed algorithm finds minimum unbreakable maximum forward capacity nodes to increases no of connections it is possible to reduce the energy. S-EA3ACK is able to detect misbehaviors in the presence of receiver collision, limited transmission power, false misbehaviour report and partial dropping.

From all the above figures and tables, it is clear that the comparison of the S-EA3ACK illustrates that the proposed algorithm outperforms the EAACK (DSA) by providing the highest packet delivery ratio, the lowest end-to-end delay, and the average energy with the increase in the number of malicious nodes.

## 7. CONCLUSION

Malicious nodes and loss attack have always been a major threat to security in MANET. In this technical research paper, a novel IDS scheme named S-EA3ACK protocol specially designed for MANET is suggested in comparison with the other popular techniques through simulations. The results demonstrate the positive performance of the packet loss and quality of network S-EA3ACK when compared with that of EAACK (DSA) in the cases of receiver collision, limited transmission power, false misbehaviour report and collaborative attacks. This paper presents the performance of vary the number of nodes from 50 and 100 in a fixed topography of 1000m and 2000 meters with different set of malicious nodes in 10 and 20. S-EA3ACK Improve secure transmission packet delivery ratio with quality output and reduce delay ratio with maximum average energy compared to the existing EAACK (DSA) routing protocol. MARS4 cryptography schemes were implementing via network simulator 2. To increase the merits of this research work, there is a plan to investigate the following issues in our future research.

1. The same concept can be applied in satellite to increase delivery ratio and reduce delay in the route and also to save more energy.
2. The performance of S-EA3ACK can be tested in real time network environment.

## REFERENCES

[1] C.E. Perkins, et al. (2001) ‘Quality of Service in Ad-Hoc on-Demand Distance Vector Routing’, IETF Internet draft.

[2] Johnson, D, Maltz and J. Broch, (2002) “The dynamic source routing protocol for mobile ad-hoc networks”, IETF, Internet Draft.

[3] Jongoh Choi, et al, (2005) “Malicious Nodes Detection in AODV- Based Mobile Ad-Hoc Networks”, GESTS Trans. Comp. Science and Engr., vol.18, no.1, pp.49-55.

[4] Sheena Mathew and K.Paulose Jacob (2006) "A Novel Fast Hybrid Cryptographic System: MARS4", IEEE International Conference.

[5] K. Liu, et al. (2007) 'An acknowledgment-based approach for the detection of routing misbehaviour in MANETs,' IEEE Trans., Vol. 6, No. 5, pp.536–550.

[6] Aishwarya Sagar Anand Ukey, Meenu Chawla, (2010) Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI, Vol.7, No.4 (1).

[7] Celia Li, et al, (2011) "Secure Routing for Wireless Mesh Networks", International Journal of Network Security, vol.13, no.2, PP.109–120.

[8] K.Thamizhmaran, et al. (2012) 'Secure Routing Protocol in MANET – A Survey', International Journal of Advance Research in Technology', Vol. 3, No. 3, pp.9-14.

[9] Shakshuki, et al. (2013) 'EAACK - A Secure Intrusion Detection System for MANETs', IEEE Trans., Vol. 60, No. 3, pp.1089-1098.

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

[11] 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, Vol. 5, No. 3, pp.166–175.