Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.420 – 430

RESEARCH ARTICLE

Enhancing Security and Performance of Mobile Ad-Hoc Network (MANET) using Joint Authentication and Topology Control Scheme

Ms. Y.Gowsika[1], Dr. R.Pugazendi[2]

[1]Department of Computer Science, K.S.Rangasamy College of Arts and Science, Tiruchengode, TamilNadu, India
[2]Department of Computer Science, K.S.Rangasamy College of Arts and Science, Tiruchengode, TamilNadu, India

[1] gowsikayogaraj@gmail.com; [2] pugazendi_r@rediffmail.com

Abstract---- **The progress to wireless network beginning with wired network has been a universal development model in the past years. The capability to move one place to another and adopt the infinite number of nodes brought by wireless network prepared it feasible in many applications. Between all the modern wireless networks, MANET is one of the main significant and unique applications. On the different to traditional network design, MANET does not engage a predetermined network framework; each single node works as uniformly a transmitter and a receiver. Nodes communicate straight with each other when they are both within the related communication range or else, they depend on their neighbors to broadcast the messages. The self-configuring capability of nodes in the MANET through it admired between important mission applications related to military utilize and emergency recovery. They are generally formed in the conditions of emergency and non-permanent operations or basically if there are no resources to set up involved networks. The results for traditional networks are usually not sufficient to offer efficient Ad-hoc operations. Both the infrastructure less network and disseminated nature lead the Mobile ad hoc network defenseless to malicious attackers. In this situation it is important to build up efficient intrusion detection processes to preserve MANET from attacks. Different level of security problems are raised by the wireless environment of communication and requirement of any security infrastructure. In this paper a Joint Authentication and Topology Control (JATC) scheme is proposed to adaptively tune the network configurations to optimize the effective throughput and the efficiency of authentication protocols for MANET. The main goal of selective encryption is to reduce the amount of data to encrypt while achieving a required level of security. Finally SNMP specifies a standardized way of exposing management data (system configuration, performance measurements, etc.) by way of defining a set of objects on the managed devices.**

Key Words--- Mobile Ad hoc Network (MANET), JATC, Strengthened Selective Encryption- Improved AES, SNMP

I. INTRODUCTION

Mobile Ad hoc NETwork (MANET) is a group of mobile nodes capable of with mutually a wireless transmitter and a receiver that communicate through each other via bidirectional wireless associates moreover directly or indirectly. The configuration process of MANET could be differing. It depends upon its application whether it is small or large [4]. A static system is decided powerfully and it is totally controlled with the system which is large scale, mobile and highly active system. Every node is working with both transmitter and receiver. Nodes communicate straight with each other while they are both contained by the same communication range. Or else, they rely on their neighbors to communicate messages. Industrial remote access and control via wireless networks are suitable new and more admired these days. One of the most important of wireless networks is its capability to permit data communication among dissimilar parties and still keep up their mobility. Within the range of transmitters, this communication is slightly restricted. Two nodes cannot able to communicate with each other efficiently while the distance between two nodes is outside of the communication range. [5]

By allowing intermediate nodes MANET resolves this complexity. To hand there are two kinds of MANETs: closed and open. In a closed MANET, all mobile nodes assist through each other toward a general goal, such as emergency search and law enforcement operations. In an open MANET, various mobile nodes with dissimilar goals, share their resources in order to make sure global connectivity. Various resources are consumed rapidly as the nodes participate in the functions. Battery power is measured to be more significant in a mobile environment [6]. An individual node of a MANET comprises the benefits of other nodes but it refuses to share its own resources. Such nodes are called as misbehaving nodes or selfish nodes. A selfish node may decline to forward the data it received to save its own energy. MANET has two types of networks such as single-hop and multi-hop. All nodes communicate directly through each other which are surrounded by the same radio coverage area range. In a multi-hop network, if the destination node is out of their radio range an individual node should depend on other intermediate nodes to transmit. A self-configuring network of mobile nodes that are attached by wireless links is typically known as MANET. The nodes can easily move and arrange randomly [7]. The wireless topology of the network may be modified rapidly and impulsively. It may control in an unrelated fashion or associated to huge Internet resources. However the ability of open medium of MANET is defenseless to various types of attacks. Attackers can easily insert the malicious or incorporate nodes in the network to attain attacks. Several schemes and intrusion detection systems proposed to detect such nodes. Another important issue in MANET is topology control. Topologies in MANETs are changing over time as nodes are moving and adjusting their transmission and reception parameters all the time. The dynamic topology in MANETs has significant impact on the quality of service (QoS), especially for the end-to-end throughput in MANET. Security is the main concern and bottleneck for widely deployed wireless applications due to the fact that wireless channels are vulnerable to attacks and that wireless bandwidth is a constrained resource. In this sense, it is desirable to adaptively achieve security according to the available resource.

II. RELATED WORKS

Marti et.al proposed IDS called watchdog. It aims to improve the network throughput with the occurrence of malicious nodes in 2000. Watchdog consists of two parts specifically, watchdog and Pathrater. It is dependable to identify the malicious node misbehaviors in the network. Watchdog system has a failure counter. It is increased even as the next node fails to forward the packet. It is suggested that to calculate the threshold value to bring down the throughput in Ad-Hoc network. [1]

Ashish Kumar et al proposed a 2ACK scheme for the detection of routing misbehaviour in Mobile Ad-hoc Network (MANET) in 2010. The fundamental design of the 2ACK scheme is to throw two-hop acknowledgment packets in the reverse direction of the routing path. The 2ACK scheme also used to discover reliable data transmission, reliable route discovery, limited transmission power, and limited overhearing range. It is suggested that to utilize the 2ACK scheme to find the behavior of the link around the node. [2]

Kang et.al presents an intrusion detection scheme with a digital signature algorithm to provide secure transmission against the false misbehaviour report and partial dropping in 2010. This new IDS assumes the link between in the network is bidirectional. Malicious nodes also lie in the network. EAACK is based on both DSA and RSA algorithm. The three important parts of the EAACK approaches are ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). An acknowledgement based IDS are referred as EAACK. This approach is used the digital signature technique to avoid the attacker. Before the acknowledgement packets forward EAACK needs the entire acknowledgement packets are digitally signed and confirmed by its receiver until they are allowed. EAACK shows that high malicious behavior rates without decreasing the network performances. It is suggested that the hop ACK scheme is utilized to reduce the overhead ration of EAACK. [3]

Sanjith S et al proposed EAACK based Intrusion Detection and prevention system using Elliptic Curve Cryptography (ECC) approach specifically designed for MANET in 2013. The Intrusion Detection and Prevention System with ECC approach is used to provide security in packet delivery. The proposed system EAACK with ECC is used to tackle the weakness of Watchdog scheme such as limited transmission power, receiver collision, and false Misbehavior. It is suggested that to utilize the Key exchange mechanism to eliminate the necessity of pre-distributed keys. [8]

III. Joint Authentication and Topology Control Method

To jointly consider security and topology control, in this section, firstly present the system model for topology control and then introduce an authentication protocol that can be used in MANETs. The objective of topology control is achieved by adjusting some controllable parameters that affect link status, such as transmission power and transmission manners. This problem is addressed by routing protocols in mobile ad hoc networks which deal with finding and maintaining fresh paths to destinations with special focus on mobility and topology change.

An algorithm for link residual lifetime based topology control

Step 1: Initialize N number of nodes in the network
Step 2: Network topology can be described as a graph G (V, E)
Step 3: The topology control problem is modelled as,

$$\mathcal{G}_N^* = \arg\max f(\mathcal{G}_N) or \mathcal{G}_N^* = \arg\min f((\mathcal{G}_N)\ s.t\ connectivity\ to\ all\ the\ neighbors$$ //

Step 4: Probability distribution of link lifetime is computed as,

$$f_{link}^{v_1}(t) = dF_{link}^{v_1}(t)/dt$$

Step 5: PDF of the remaining link lifetime t condition on elapsed time $t_{elapsed}$ is given by,

$$f_{link}^{v_1}(t|t_{elapsed}) = \frac{1}{A}u(t)f_{link}^{v_1}(t|t_{elapsed})$$

Step 6: The expectation of the remaining link lifetime t given elapsed link lifetime $t_{elapsed}$ is,

$$E(t|t_{elapsed}) = \frac{1}{A}\int t\ f_{link}^{v_1}(t|t_{elapsed})dt$$

Step 7: The remaining link lifetime has the following distribution (P_R):

$$p_R(s) = \int_0^\infty p_R(s|t)dp(t) = \int_s^\infty \frac{1}{t}dp(t)$$

Step 8: Select the best path based on link lifetime.

Advantages

- ✓ By using the jointly consider security and topology control, the lifetime is computed and select the optimal path.
- ✓ Lifetime of the network is increased
- ✓ High network performance

IV. Strengthened Selective Encryption

AES cryptography algorithm is used for the selective encryption method. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

- ✓ Substitute bytes
- ✓ Shift rows
- ✓ Mix Columns
- ✓ Add Round Key

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

- ✓ Inverse Shift rows
- ✓ Inverse Substitute bytes
- ✓ Inverse Add Round Key
- ✓ Inverse Mix Columns

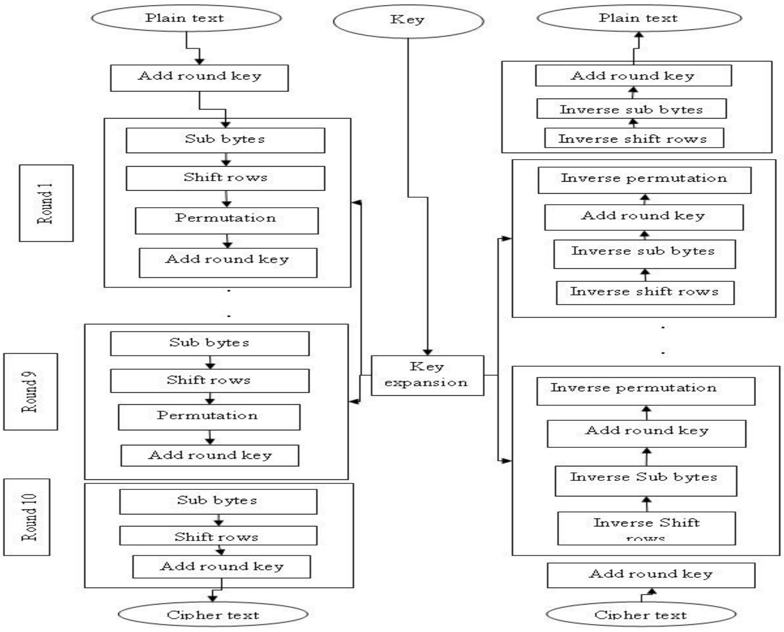


Fig 1: Improved AES

There are 10 rounds for full encryption. The four different stages that we use for Modified-AES Algorithm are:

- ✓ Substitution bytes
- ✓ Shift Rows
- ✓ Permutation
- ✓ Add Round Key

Substitution Bytes, Shift Rows and Add Round Key remain unaffected as it is in the AES. Here the important function is Permutation which is used instead of Mix column. These rounds are managed by the following the conversions shown in Fig 1. Permutation is widely used in cryptographic algorithms. Permutation operations are interesting and important from both cryptographic and architectural points of view. The inputs to the IP table consist of 64 bits. Improved AES algorithm takes 128 bits as input. The functions Substitution Bytes and Shift Rows are also interpreted as 128 bits whereas the Permutation function takes 64 bits. We divide the consequential bits of Shift Rows function into two parts of 64 bits and then take each part of 64 bits as input of permutation tables and shift bits one by one according to that table. We fetch one bit from the source, and put it into the correct position in the destination. Each bit of a block is subject to initial permutation, which can be represented by the following initial permutation (IP) table. In the permutation table each entry indicates a specific position of a numbered input bit consisting of 64 bits in the output. While reading the table from left to right and then from top to bottom it is observed that the 58th bit of the 64-bit block is in first position, the 50th is in second position and so forth.

V. SIMPLE NETWORK MANAGEMENT PROTOCOL

In the SNMP method, the network is monitored by the trusted centre for all the nodes in the network. So, that the network performance is improved.

The parameters are:

- ✓ **Packet Sending / Receiving Rate (PSR/PRR):** Number of packets sent or received over a predefined period of time.
- ✓ **Packet Dropping Rate (PDR):** Packet dropping rate is the number of packets that were sent to a certain node but were not forwarded by that node.
- ✓ **Packet Forwarding Rate (PFR):** Packet forwarding rate of a certain node is the number of packets that the node received from its neighbors and consequently forwarded to its parent node during a predefined period of time.
- ✓ **Forward Delay Time (FDT):** Forward delay time is calculated as a difference between the reception time of the first packet and transmission time of the first packet.

These metrics are monitored by the trusted centre (TC). Attributes are: Packet Sending / Receiving Rate, Packet Dropping Rate, Packet Forwarding Rate and Forward Delay Time. Based on the attribute values, the reference patterns are generated for the normal and abnormal behaviour of the nodes. In order to monitor the network, these reference patterns are matched with the attribute values of the nodes and identify the normal and abnormal behaviour of the nodes in the network.

Algorithm: SNMP for Monitoring the Network (SNMP-MN)

Step 1: Initialize N number of nodes in the network
Step 2: TC monitors the network // Trusted centre
Step 3: While $i \leq N$

// Compute Packet Sending / Receiving Rate (PSR/PRR)

$$PSR/PRR_i = \frac{No\ of\ packets\ sent}{Prefined\ Time}$$

// Compute Packet Dropping Rate (PDR)

$$PDR_i = Packetds\ not\ forwarded\ to\ other\ node$$

// Packet Forwarding Rate (PFR)

$$PFR_i = \frac{No\ of\ packets\ received\ from\ its\ neighbours}{Predefined\ time}$$

// Forward Delay Time

$$FDT_i = \text{Reception time of the first packet} - \text{transmission time of the first packet}$$

Step 4: Compare with threshold value

$$If\left(\frac{PSR}{PRR}_i < Th1\right)||PDR_i > Th2||(PFR_i < Th3)||(FDT_i < Th4)$$

Step 5: Consider as abnormal nodes
Step 6: Else
Step 7: Normal nodes
Step 8: Compute the reference pattern by collecting the values for the attributes
Step 9: Find the abnormal nodes in the network by comparing the reference pattern

Advantages

- ✓ High accuracy of detecting the malicious nodes
- ✓ Highly secure

VI. EXPERIMENTAL RESULTS AND DISCUSSION

The performance metrics considered in this work to show the effectiveness of the proposed algorithms are throughput, routing overhead, packet delivery ratio and end-to-end delay.

Packet Delivery Ratio

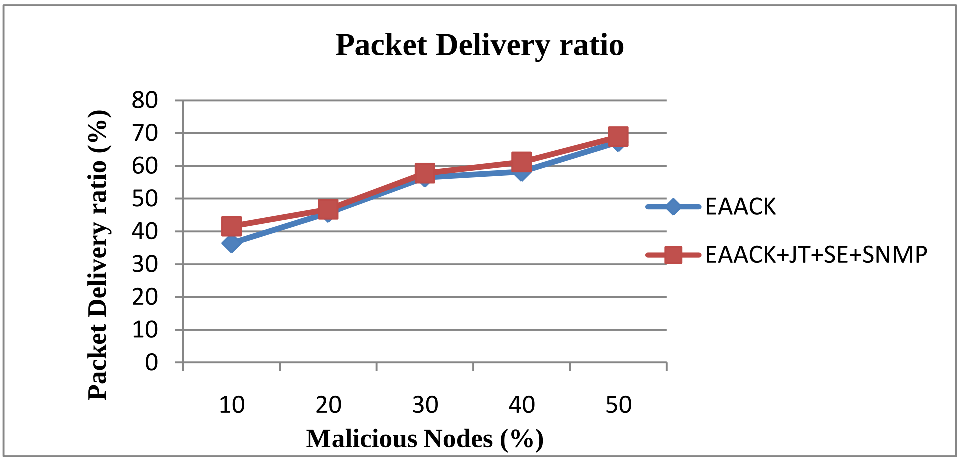
It is defined as the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

$$\sum \text{Number of packet received} / \sum \text{Number of packet sends}$$

The statistical values for the packet delivery ratio are shown in table 6.1. If there are 50 % malicious nodes, the packet delivery ratio for EAACK is 67.3% and 68.9% for EAACK+JT+SE+SNMP method

Table I: Packet delivery ratio

Packet Delivery ratio (%)		
Malicious Nodes (%)	EAACK	EAACK+JT+SE+SNMP
10	36.4	41.6
20	45.7	46.8
30	56.5	57.8
40	58.2	61.2
50	67.3	68.9



Graph 1: Packet delivery ratio

The above graph clearly shows the Packet Delivery Ratio obtained by the Joint Authentication and Topology Control (JATC) scheme, Selective Encryption using Improved Advanced Encryption Standard algorithm (SE-IAES) and Simple Network Management Protocol (SNMP) that achieves higher Packet Delivery Ratio than the EAACK.

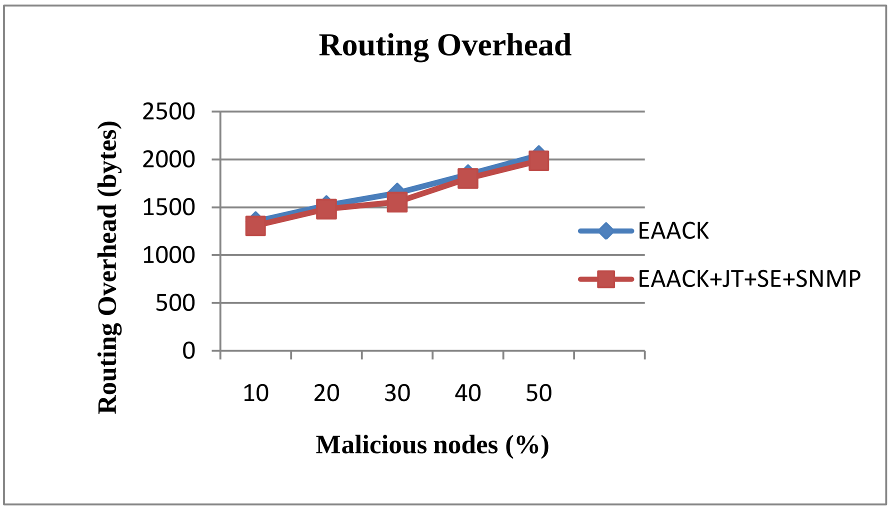
Routing Overhead

It is defined as the ratio of the total packet size of control packets (include RREQ, RREP, RERR, and Hello) to the total packet size of data packets delivered to the destinations.

The statistical values for the routing overhead are shown in table 6.2. If there are 50 % malicious nodes, the routing overhead for EAACK is 2044 bytes and 1987 bytes for EAACK+JT+SE+SNMP method.

Table II: Routing Overhead

Routing Overhead (bytes)		
Malicious Nodes (%)	EAACK	EAACK+JT+SE+SNMP
10	1352	1308
20	1520	1483
30	1651	1556
40	1844	1803
50	2044	1987



Graph 2: Routing Overhead

The above clearly shows the Routing Overhead obtained by the Joint Authentication and Topology Control (JATC) scheme, Selective Encryption using Improved Advanced Encryption Standard algorithm (SE-IAES) and Simple Network Management Protocol (SNMP) which decreases the Routing Overhead if the percentage of malicious node is increased compared to the Existing Method.

Throughput

Throughput or network throughput is the rate of successful message delivery over a communication channel. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

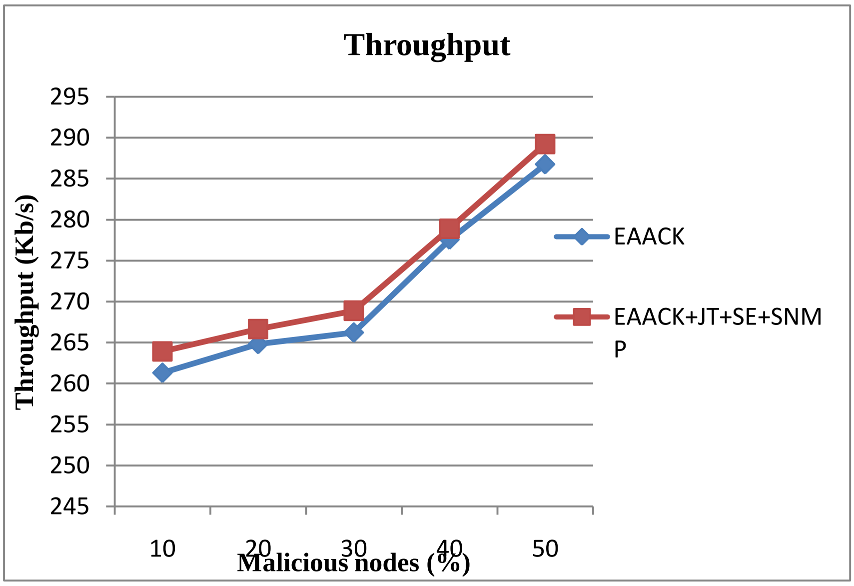
Transmission Time = File Size / Bandwidth (sec)

Throughput = File Size / Transmission Time (Kbps)

The statistical values for the throughput are shown in table 6.3. If there are 50 % malicious nodes, the throughput for EAACK is 286.76 and 289.24 Kb/sec for EAACK+JT+SE+SNMP method.

Table III: Throughput

Throughput (Kbytes/Sec)		
Malicious Nodes (%)	EAACK	EAACK+JT+SE+SNMP
10	261.32	263.92
20	264.82	266.65
30	266.23	268.89
40	277.56	278.89
50	286.76	289.24



Graph 3: Throughput

The above graph clearly shows the Throughput obtained by the Joint Authentication and Topology Control (JATC) scheme, Selective Encryption using Improved Advanced Encryption Standard algorithm (SE-IAES) and Simple Network Management Protocol (SNMP) which achieves the higher Throughput performance than the EAACK.

End-to-End delay

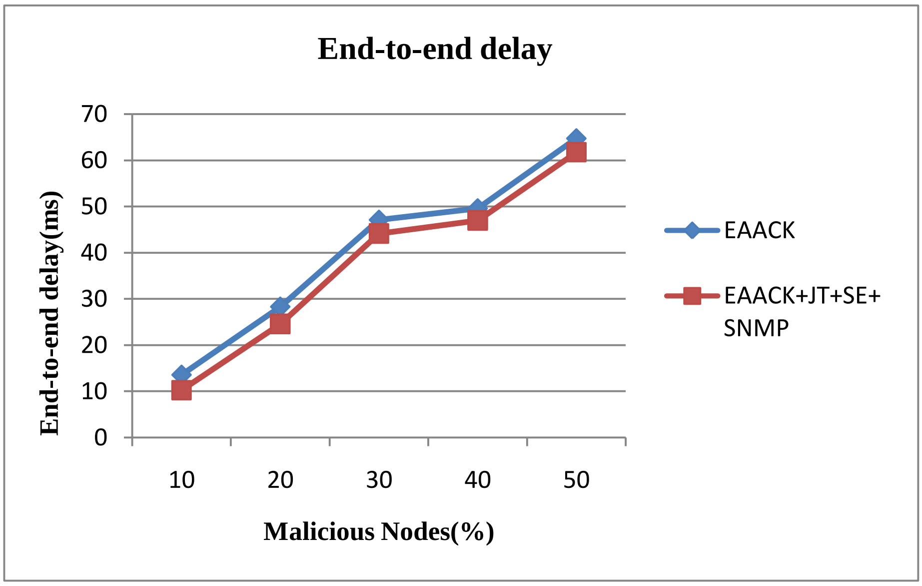
End-to-end delay is the time it takes a packet to travel across the network from source to destination. Delay jitter is the fluctuation of end-to-end delay from packet to the next packet.

$$\sum \text{(arrive time – send time)} / \sum \text{Number of connections}$$

The statistical values for the end-to-end delay are shown in Table 6.4. If there are 50 % malicious nodes, the end-to-end delay for EAACK is 64.7647ms and 61.7541 ms for EAACK+JT+SE+SNMP method.

Table IV: End-to-End delay

End-to-End delay (ms)		
Malicious Nodes (%)	EAACK	EAACK+JT+SE+SNMP
10	13.5714	10.2793
20	28.3179	24.6012
30	47.1279	44.1647
40	49.6012	47.0046
50	64.7647	61.7541



Graph 4: End-to-End delay

The above graph clearly shows the End-to-End Delay is obtained by the Joint Authentication and Topology Control (JATC) scheme, Selective Encryption using Improved Advanced Encryption Standard algorithm (SE-IAES) and Simple Network Management Protocol (SNMP) which decreases the delay than the EAACK.

VII. CONCLUSION AND FUTURE CONSIDERATIONS

Packet-dropping attack has always been a major threat to the security in MANETs. In this existing system, novel IDS named EAACK protocol is specially designed for MANET 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. But the disadvantage is Security is the main concern and bottleneck for widely deployed wireless applications due to the fact that wireless channels are vulnerable to attacks and that wireless bandwidth is a constrained resource. So, in the proposed system a joint authentication and topology control (JATC) scheme is proposed to improve the throughput. Next for security a strengthened selective encryption is proposed. Selective encryption is a new trend in image and video content protection. It consists of encrypting only a subset of the data. The aim of selective encryption is to reduce the amount of data to encrypt while preserving a sufficient level of security. For future work, considers the different attacks in the mobile adhoc networks.

REFERENCES

[1]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annual International Conference on Mobile Computing Netw. Boston, MA, ISBN: 1-58113-197-6, 2000, pp. 255–265.

[2]. Ashish Kumar," An Acknowledgement-Based Approach for the Detection of Routing Misbehaviour in MANETS", International Journal of Advances in Embedded Systems, Vol.1, 2010, pp. 04-06.

[3]. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, from Nov. 8 to Nov. 10, 2010.

[4]. Mokit Kumar," An Overview of MANET: History, Challenges and Applications", International Journal of Computer Science and Engineering, ISSN: 0976-5166, Vol.3, 2012.

[5]. Aarti, Dr.S.S.Tyagi, "Study of MANET: Characteristics, Challenges, Applications and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 5, 2013.

[6]. R. Bharathi, Saranya. A.V," High Throughput Analysis Using Topological Control & Authentication Scheme in MANET", International Journal of Emerging Technology and Advanced Engineering, Vol. 3, No. 3, 2013.

[7]. Elhadi M. Shakshuki, " EAACK—A Secure Intrusion Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol.60, No.3, 2013.

[8]. Sanjith S, "EAACK – Based Intrusion Detection and Prevention for MANETs using ECC Approach", International Journal of Emerging Trends & Technology in Computer Science, Vol 2, Issue 4, ISSN 2278-6856, 2013, pp.424-431.

AUTHOR'S BIOGRAPHY

Ms.Y.Gowsika received her MCA (Master of Computer Applications) degree from SNS College of Technology, Affiliated to Anna University, Chennai in 2013. She is pursuing M.Phil (Computer Science) degree Under the Supervision of Dr. R. Pugazendi. Her Area of interest is Networking.

Dr. R. Pugazendi is working as an Associate professor and Head in Department of Computer Science. He obtained his Ph.D in Computer Science from Periyar University and published numerous research Papers in International Journals and also presented papers in various National and International Conferences. His Area of interest is Computer Networking.

