International Journal of Engineering Research and General Science Volume 3, Issue 4, July-August, 2015
ISSN 2091-2730

A Secure Intrusion Detection System using EAACK in MANETs

Jidhesh R, Bhavya P, Fathimath Sinan K P, Rugma R, Lathesh K
Department of Information Technology
Government Engineering College Sreekrishnapuram
Kerala, India.
Email: rjidhesh@gmail.com
Contact No : +91 8907514898

Abstract— Nowadays wireless network became a trend than wired networks. Wireless networks provides various applications due to its mobility and scalability. Mobile Ad hoc NETwork (MANET) is one of the most important application. MANET does not require a fixed network infrastructure. But, MANET is vulnerable to malicious attackers. Thus, an efficient intrusion detection system is needed to protect from attacks. A new IDS named Enhanced Adaptive ACKnowledgment is proposed for MANETs which performs higher malicious behavior detection rates. It prevents attackers from initiating false misbehavior report and forge acknowledgment attacks.

Keywords— Ad-hoc On-demand Distance Vector (AODV), Digital signature, Enhanced Adaptive ACKnowledgment (EAACK), False misbehavior report, Forge acknowledgment packets, Misbehavior Report Authentication (MRA), Mobile Ad hoc NETwork (MANET), Packet Delivery Ratio(PDR), Rivest Shamir Adleman(RSA) Algorithm, Routing Overhead(RO).

INTRODUCTION

MANET (Mobile Ad hoc network) is an IEEE 802.11 framework which is a collection of mobile nodes equipped with both a wireless transmitter and receiver communicating via each other using bidirectional wireless links. This type of peer to peer system infers that each node or user in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. MANETs are self-forming, self-maintained and self-healing allowing for extreme network flexibility, which is often used in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances.

The open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. A new intrusion detection system named Enhanced Adaptive ACKnowledgment (EAACK) and Digital Signature is designed for MANETs to detect malicious nodes and to prevent advanced attacks. Many IDS are existing for MANET's and the three existing approaches are WATCHDOG, TWOACK and Adaptive ACKnowledgment (AACK). They suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report. Existing schemes are largely depend on the acknowledgment packets. Hence, the acknowledgment packets should be valid and authentic. Another drawback is the significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such overhead can easily degrade the life span of the entire network.

A new and efficient intrusion detection system named EAACK is proposed and implemented for MANETs. EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior report, limited transmission power and receiver collision. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances. To ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK) and misbehavior report authentication (MRA).

ARCHITECTURE

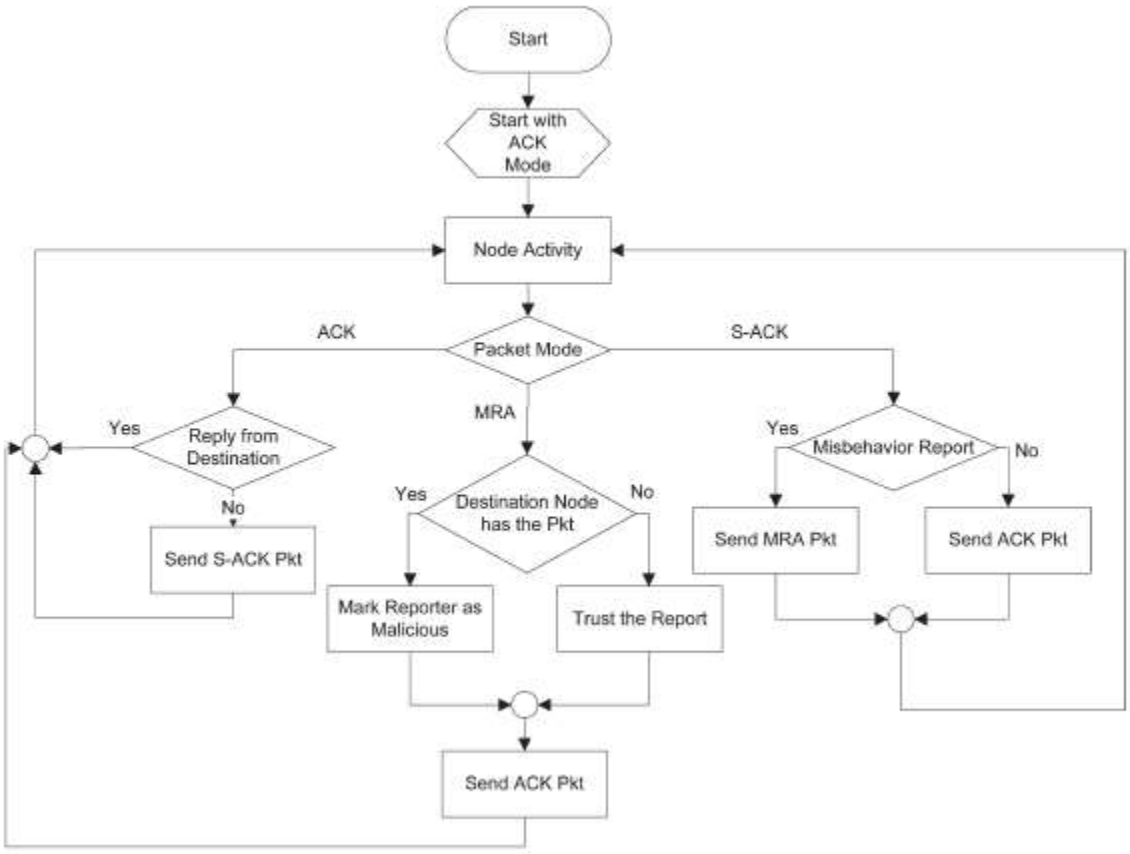

Figure.1 System Architecture

Following steps describes the functions of the system architecture:

1. Start sending packets in ACK mode.
2. If the reply from the destination is received to the source within a threshold time, then the packets are continued to be send in ACK mode.
3. Else, switch to S-ACK mode by sending out an S-ACK data packet.
4. In S-ACK mode, if there is misbehavior report then switch to MRA mode by sending an MRA packet. Otherwise, the ACK mode is continued.
5. In MRA mode, an alternative route to the destination is found and checks whether the destination node has received the reported packet or not.
6. If the destination node has the packet, then mark the reporter as malicious and avoid that node from further transmission. Then, switch back to ACK mode.
7. Else, the misbehavior report is trusted and accepted. Then switch back to ACK mode.

IMPLEMENTATION METHOD

Tools used

Our simulation is implemented in NS 2.34 environment with Ubuntu 10.04 platform. The system is running on a laptop with Intel processors with 4GB RAM and 500GB hard disk.

Languages used

1. TCL
2. C++

Algorithms used

Three different algorithms are used in this system. They are as follows:

- **EAACK**

1. Finding a route from the source node to the destination node using a routing protocol (AODV).
2. Start sending packets in ACK mode.
3. If the reply from the destination is received to the source within a threshold time, then the packets are continued to be send in ACK mode.
4. Else, switch to S-ACK mode by sending out an S-ACK data packet.
5. In S-ACK mode, if there is misbehavior report then switch to MRA mode by sending an MRA packet. Otherwise, the ACK mode is continued.
6. In MRA mode, an alternative route to the destination is found and checks whether the destination node has received the reported packet or not.
7. If the destination node has the packet, then mark the reporter as malicious and avoid that node from further transmission. Then, switch back to ACK mode.
8. **Else, the misbehavior report is trusted and accepted. Then switch back to ACK mode.**
9. Digital signature is implemented in order to tackle the forge acknowledgment packets.

- **AODV Routing Protocol**

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for MANETs which is a reactive routing protocol that uses some characteristics of proactive routing protocols. AODV routing protocol has two process, namely, Route Discovery and Route Maintenance. If a route to a destination is needed, it is established at the route discovery phase and is maintained at the route maintenance phase.

a) Route Discovery:

1. When a source node needs a route to a destination node, then source node broadcasts a route request packet (RREQ) to the destination node.
2. After receiving the route packet at each node, it creates or updates a reverse route to the source node in the routing table and it is not valid then resend RREQ.
3. If its valid each node send RREQ to its neighbor nodes.
4. When the RREQ from the source node arrives at the destination node, the destination node creates or updates the reverse route and it send a route reply packet (RREP) to the source.
5. When each node receives the RREP, it creates or updates a forward route to the destination node and it forwards the RREP to the reverse route.
6. When each node receives the RREQ that it has already processed, it discards the RREQ.
7. When the RREP arrives at the source node along with the reverse route, it creates or updates the forward route, and starts communications.

b) Route Maintenance:

Route maintenance protocol is used to provide feedback about the links of the route and to allow the route to be modified in case of any disruption due to movement of one or more nodes along the route.

1. Each node broadcasts a Hello packet periodically for local connectivity. It broadcasts the RREP with TTL=1 as the Hello packet.
2. When the node does not receive any packets from a neighbor during a few seconds, it assumes a link break to the neighbor.

3. When the node has the link break to the neighbor based on an acknowledgment of MAC layer, it detects a route break to the destination node that the next hop of the route is the neighbor.
4. When the node that detects the link break is close to the destination node, it requires a new route to the destination node, which is known as Local Repair.
5. During the local repair, arrival data packets received are buffered.
6. When the RREP is received and the local repair is successful, the node starts sending data packets in the buffer.

- **RSA Algorithm**

RSA is one of the first practicable public key cryptosystem and is widely used for secure data transmission. It consists of two key, one for encryption and other for decryption. The RSA algorithm involves three steps, Key generation, Encryption and Decryption.

a) Key Generation

RSA involves a public key and private key. The keys for the RSA algorithm are generated the following ways:

1. Choose two different large random prime numbers p and q.
2. Calculate n as product of p and q, i.e., n = pq, where n is the modulus for the public key and the private keys.
3. Calculate m as the product of (p-1) and (q-1) i.e., m = (p-1)(q-1).
4. Select any integer e<m such that it is co-prime to m, i.e., gcd(e,m) = 1.
5. Calculate d such that d mod m = 1, i.e, d =e^{-1}mod m.
6. The public key is (e,n).
7. The private key is (d,n).

b) Encryption

First converts the given plaintext p into a number smaller than n by using an agreed-upon reversible protocol known as a padding scheme. Then computes the cipher text c, corresponding to:
c = p^e mod n.

c) Decryption

We can convert the cipher text c into plaintext p, corresponding to:
p = c^d mod n.

ANALYSIS

In order to measure and compare the proposed EAACK scheme analysis is done on the basis of the following three metrics:

1. **Packet Delivery Ratio(PDR):**
   Packet Delivery Ratio defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

2. **Routing Overhead(RO):**
   Routing Overhead defines the ratio of the amount of routing-related transmissions [Route REQuest(RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

3. **Average End to End Delay:**

Average End-to-End Delay defines the time taken for a packet to be transmitted across a network from source node to destination node.

Analysis of the EAACK scheme is described in the following three comparison graphs:

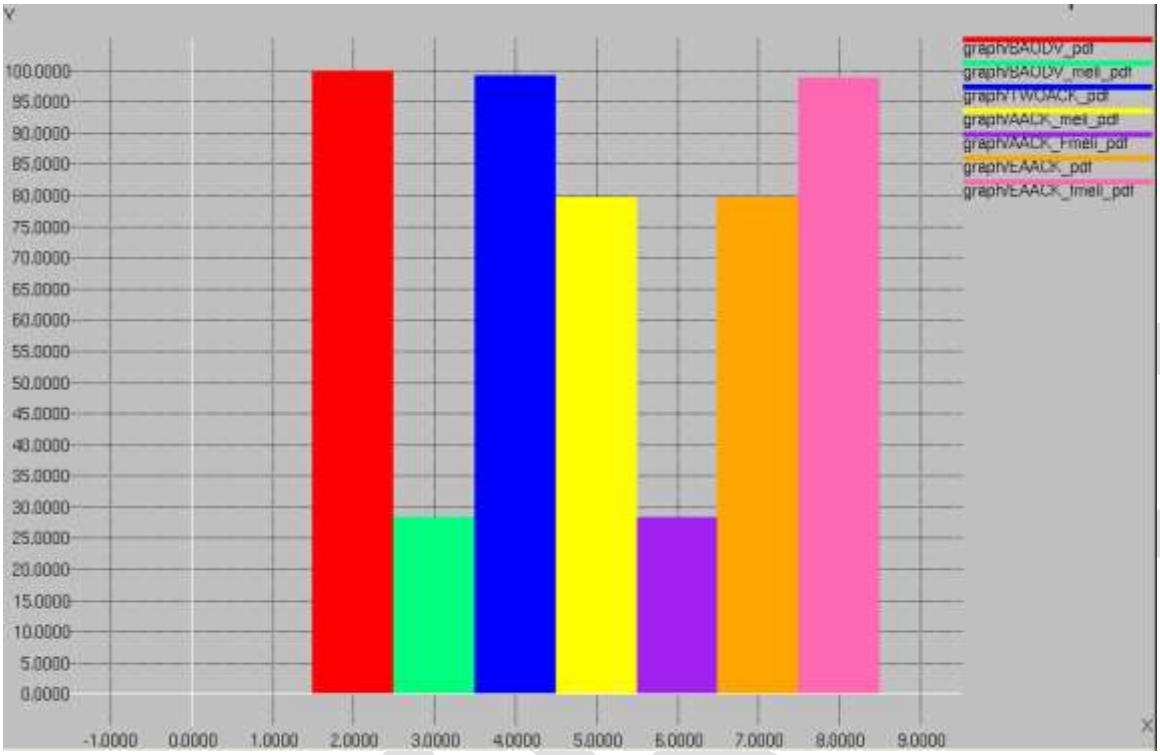

Figure.2 Packet Delivery Ratio graph

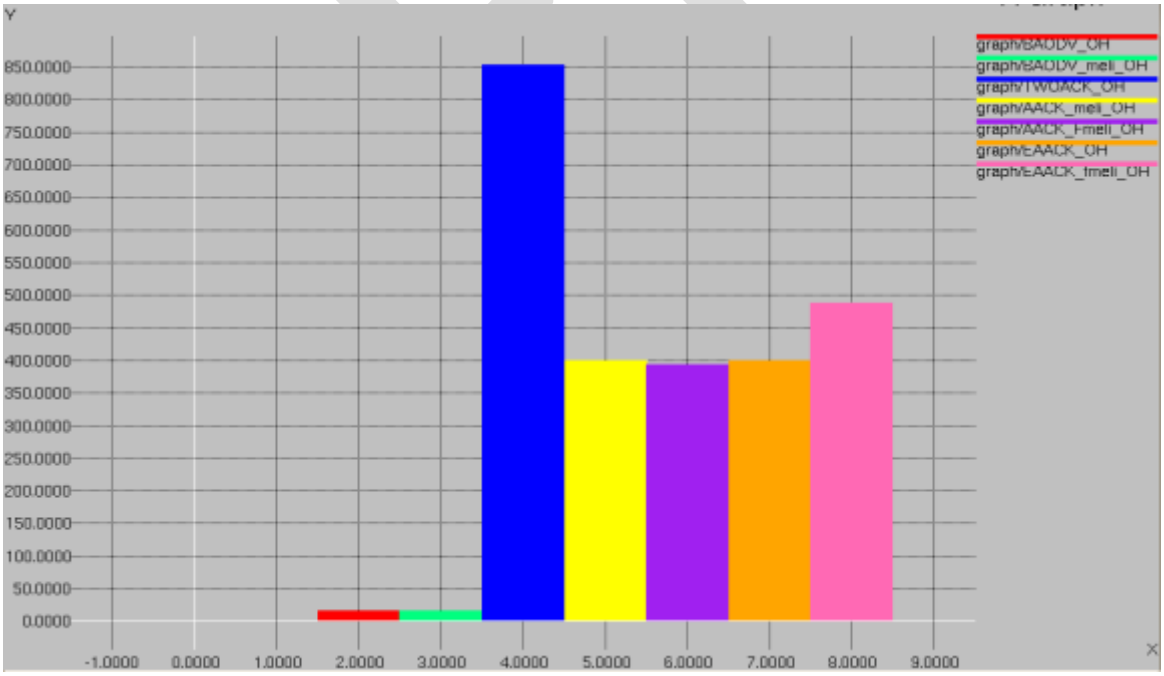

Figure.3 Routing Overhead graph

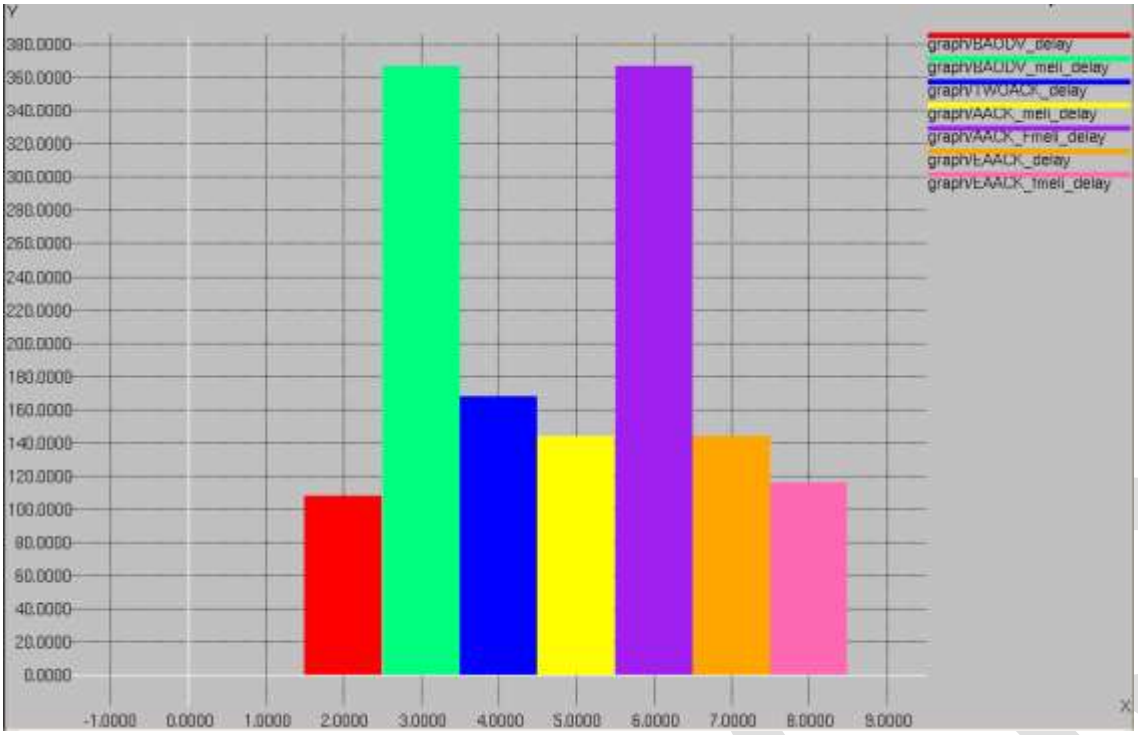

Figure.4 Average End to End Delay graph

All the above three xgraphs, analysis the comparison among the following seven conditions:

• Basic AODV routing condition.
• Basic AODV routing condition with malicious node in the network.
• TWOACK mode of transmission of packets, that is, two hops transmission of packets with in the network
• ACK mode of transmission of packets with malicious node in the network.
• ACK mode of transmission of packets with malicious node in the network and also this malicious node sends a forge acknowledgment packets to the source node.
• EAACK mode of transmission of packets with malicious node in the network.
• EAACK mode of transmission of packets with malicious node in the network and also this malicious node sends a forge acknowledgment packets to the source node.

PERFORMANCE EVALUATION

To better investigate the performance of EAACK under different types of attacks, two scenario settings to simulate different types of misbehavior or attacks are described.

Scenario 1:

Malicious node are set up to send out false misbehavior report to the source node whenever it is possible. This scenario is designed to test IDSs' performances against false misbehavior report.

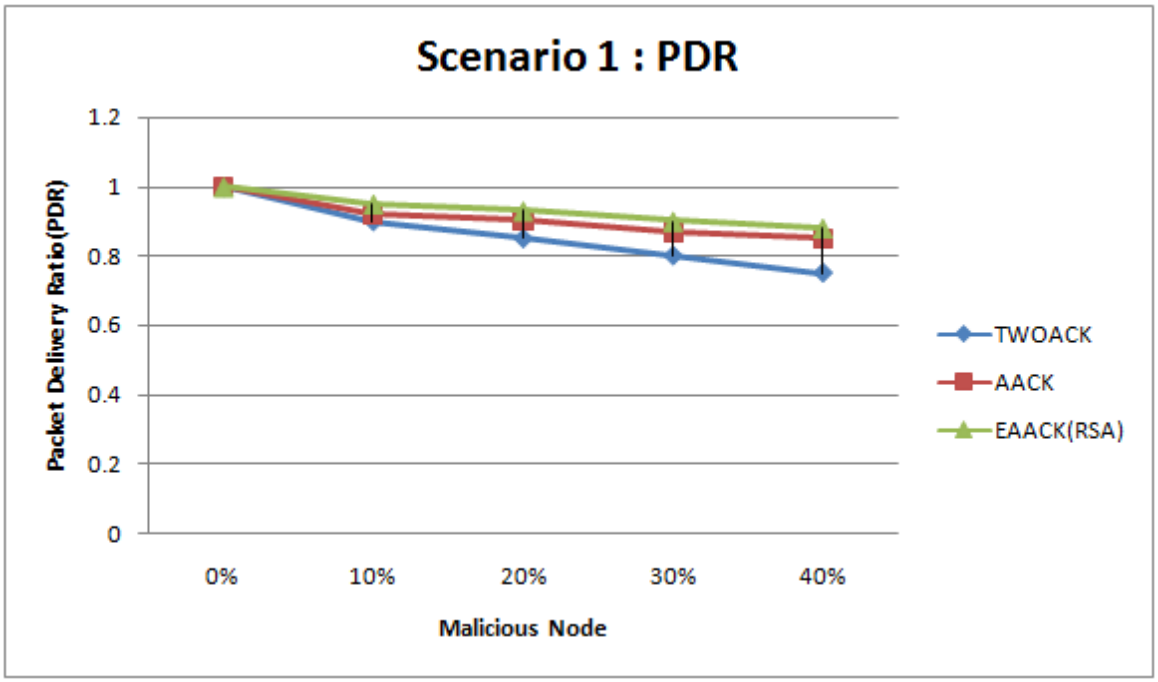

Figure.5 Scenario 1 : Packet Delivery Ratio

The above figure shows the simulation results based on PDR. When malicious nodes are 10 percent, EAACK performs 2 percent better than AACK and TWOACK. When the malicious nodes are at 20 percent and 30 percent, EAACK outperforms all the other schemes and maintains the PDR to over 90 percent. The introduction of MRA scheme mainly contributes to this performance. EAACK is the only scheme that is capable of detecting false misbehavior report.

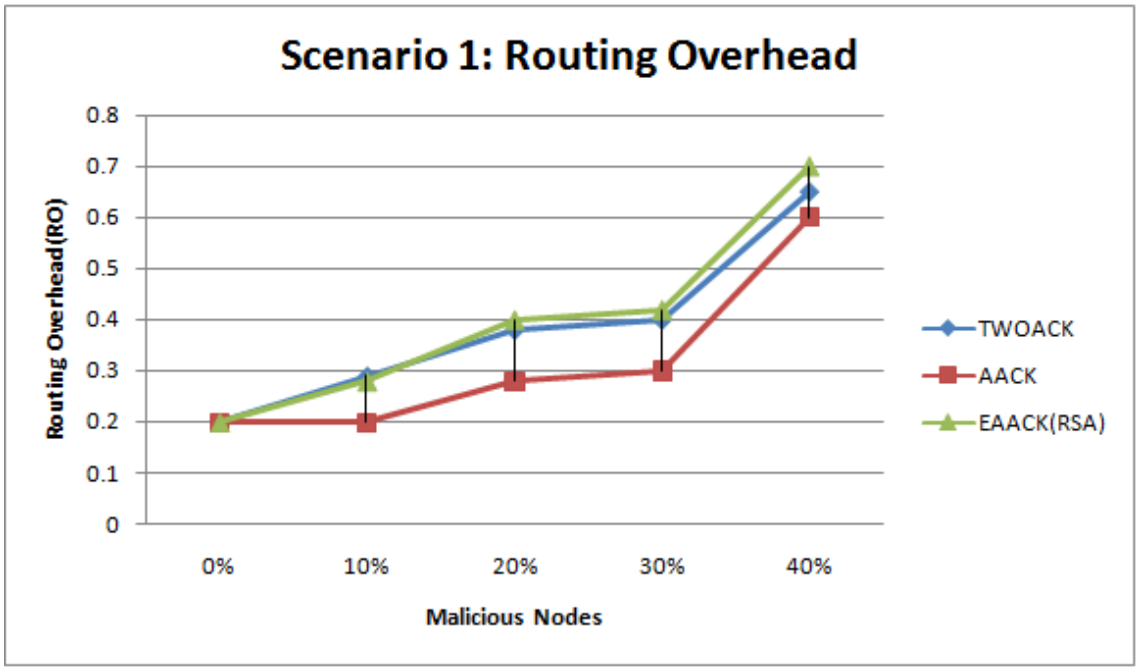

Figure.6 Scenario 1 : Routing Overhead

In terms of RO, EAACK maintains a lower network overhead compared to TWOACK in most cases, RO rises rapidly with the increase of malicious nodes. It is due to the fact that more malicious nodes require a lot more acknowledgment packets and digital signatures.

Scenario 2:

This scenario is used to test the IDSs' performances when the attackers are smart enough to forge acknowledgment packets. Malicious nodes simply drop all the packets that they receive and send back forged positive acknowledgment packets to its previous node whenever necessary.

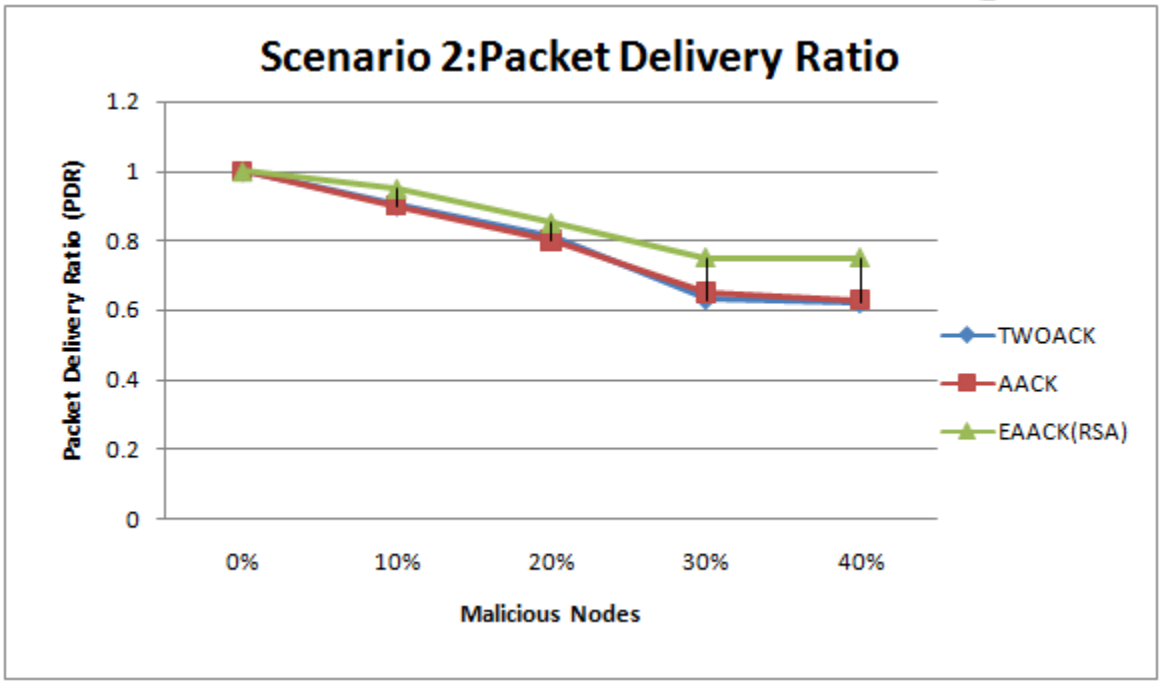

Figure.7 Scenario 2 : Packet Delivery Ratio

The PDR performance comparison in scenario 2 is shown in the above figure. It was observed that the proposed scheme EAACK outperforms TWOACK and AACK in all test scenarios. It is believed that this is because EAACK is the only scheme which is capable of detecting forged acknowledgment packets.

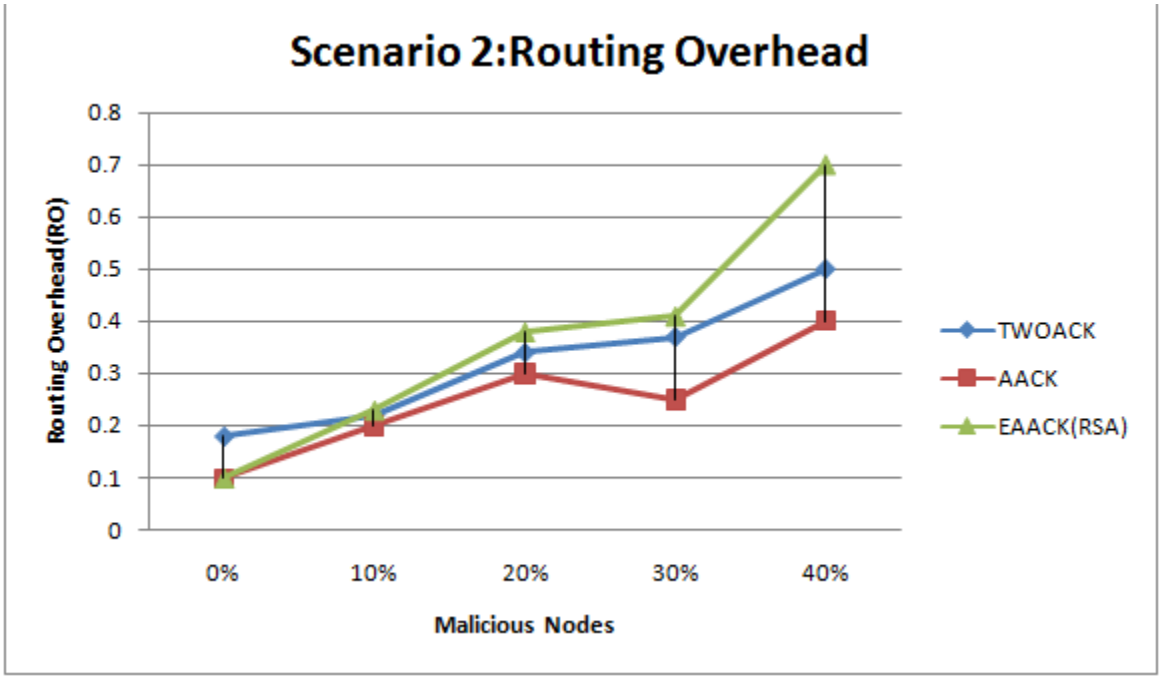

Figure.8 Scenario 2 : Routing Overhead

The above figure shows the achieved RO performance results for each IDS in scenario 2. Regardless of digital signature scheme adopted in EAACK, it produces more network overhead than AACK and TWOACK when malicious nodes are more than 10 percent. Digital signature scheme brings in more overhead than the other two schemes.

CONCLUSION

A new IDS named EAACK protocol is designed for MANETs and is compared against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Also, to prevent the attackers from initiating forged acknowledgment attacks, it is extended to incorporate digital signature also. For this purpose, RSA scheme is introduced in the simulation.

The future works includes the adaption of hybrid cryptography techniques to further reduce the network overhead caused by digital signature. The performance of EAACK can be tested in real network environment instead of software simulation.

REFERENCES:

[1] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," *in Wireless/Mobile Security*, 2008.
[2] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, pp. 255–265, 2000.
[3] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.
[4] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," *in Mobile Computing*, ch. 5, pp. 153–181, 1996.
[5] Ashok M. Kanthe, Dina Simunic and Ramjee Prasad, "Comparison of AODV and DSR On-Demand Routing Protocols in Mobile Ad hoc Networks," *in Emerging Technology Trends in Electronics, Communication and Networking*, 2012.
[6] P.Priyanka, S.Swetha, "Detection of misbehavior nodes in MANETS using EIDS," 2014.
[7] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.
[8] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582, 2007.

[9] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
[10] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in Proc. IEEE Int. Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.
[11] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf. Pervasive Comput. Commun., 2005, pp. 191–199.
[12] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. ACM Workshop Wireless Secur.*, 2002, pp. 1–10.
[13] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS)