# INTRUSION-DETECTION SYSTEM FOR MANETS: A SECURE EAACK

**Pratibha Wage[1], Channveer Patil[2]**

[1]*M.Tech Student, CSE Department, GNDEC, Karnataka, India*
[2]*Assistant Professor, CSE Department, GNDEC, Karnataka, India*

## Abstract

*The Mobile ad-hoc network does not have any fixed infrastructure so they rely on their neighbors to relay message. The mobile nodes can move around the network in free manner. Unlike wired networks, there is no fixed and dedicated link available between the nodes. So any node can access any link between any nodes. This nature of open medium of MANET they attracts malicious users. IDS techniques are used to detect malicious nodes. Here they propose new Intrusion detection method called EAACK .EAACK handles three weakness of watch dog they are:1) Receiver collision, 2) Limited transmission power, 3) False misbehavior. EAACK demonstrate higher malicious- behavior detection rates in certain circumstances while does not greatly affect the network performances .In proposed EAACK scheme they implemented both DSA and RSA.*

***Keywords:*** *Digital signature, DSA, EAACK, Mobile Ad hoc Network (MANET)*

----------***----------

## 1. INTRODUCTION

By definition, Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. MANET is used to exchange information from source to destination nodes. Nodes can communicate directly within their range otherwise indirectly rely on neighbours. Nodes act as routers to forward packets form each other.

MANET is popular among military applications, sensor networks, industrial application etc.

MANETs Vulnerable to malicious attackers because of open medium and wide distribution malicious attackers is easily attacked to improve security they develop IDS.

IDS detect and report the malicious activity in ad hoc networks. IDSs usually act as the second layer in MANETs.

## 2. EXISTING SYSTEM

- [7] MANET does not have any fixed topologies. So the mobile nodes can move freely around the network.
- The MANET can be divided into a SINGLE-HOP and MULTI-HOP networks [5].
- In single-hop networks the nodes are within communication range can communicate directly with each other.
- Whereas in Multi-hop networks, if the nodes are out of communicating range, the nodes must rely on intermediate nodes to forward the data packets to their destination.
- However, in both type of networks there is no dedicated link available like the links in wired networks.
- The absence of fixed and dedicated link among the nodes leads to severe security threats to the network.
- So an effective Intrusion Detection Scheme (IDS) is needed to safeguard the network from these threats.

There are several IDS techniques proposed to ensure the secure communication of data packets in the network. They are 1) watchdog 2) TWO ACK 3) AACK

### 2.1 Watchdog

Marti et al. [1] proposed two techniques (Watchdog and Pathrater) that improve the network throughput with the existence of selfish or misbehaving nodes. Consist of two techniques Watchdog and Pathrater. Watchdog serves as IDS and Pathrater cooperates with routing protocols.

It detects malicious nodes by overhearing next hop's transmission. A failure counter is occur if the next node fails to Forward the data packet. When it exceeds a predefined threshold the node said or marked it is malicious node. The drawback of watchdog are 1) ambiguous collisions, 2) receiver collisions 3) limited transmission power, 4) false misbehavior report, 5) collusion, and 6) partial dropping.

### 2.2 TWOACK

It solves the problem of receiver collision and power limitation of watchdog. In this scheme an acknowledgment of every data packets over every there nodes along transmission path. If

ACK is not received within predefined time, the other nodes are marked malicious. TWOACK works on routing protocols such as Dynamic Source Routing (DSR).

The disadvantages are 1) Limited battery power 2) Network overhead.

### 2.3 AACK

Itsolves the two problems of watchdog and improves the performance of TWOACK by reducing the routing overhead while maintaining better performance [2]. AACK is a combination of TACK and ACK. It reduces network overhead but fails to detect malicious nodes with false misbehavior report.

## 3. PROPOSED SYSTEM

Here we propose a strong new Intrusion detection mechanism called EAACK which requires less hardware cost. EAACK is an acknowledgement based IDS. This scheme uses the digital signature method to prevent the attacker from forging acknowledgment packets.

- EAACK is divided into three major parts called:
  - A) ACK
  - B) S-ACK
  - C) MRA
- ACK is an end-to-end acknowledgment scheme. EAACK, aiming to reduce low network overhead when no network misbehavior is detected. To preserve the lifecycle of battery and have low memory consumption.
- According to this ACK mode, if the receiver node does not send the ACK within predefined time interval, then ACK assumes malicious may present and switch to S-ACK mode to detect them.
- In S-ACK part, for every three consecutive nodes in the route, the third node sends an S-ACK acknowledgment packet to the first node.
- If malicious found, then MRA mode select alternate path to the destination.
- To initiate the MRA mode, the source nodes first searches its local knowledge base and take an alternative route to the destination node.
- If there is no other that exists, the source node starts a routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes.

### 3.1 Digital Signature

Digital Signature is used in EAACK to prevent the nodes from attacks. EAACK requires all acknowledgment packets to be digitally signed before sending out. We implement DSA and RSA digital signature Algorithm.

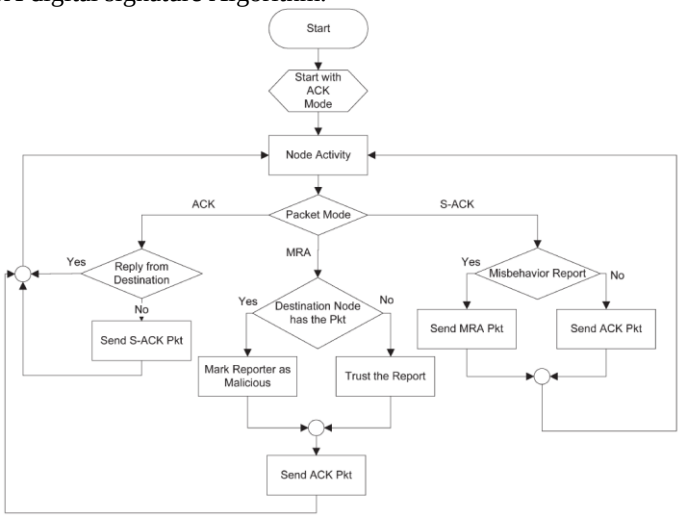


**Fig -1:**Flow chart for system architecture of EAACK

## 4. COMPARATIVE STUDY

Summarized comparison of above reviewed techniques is tabularized [8] as follows:

**Table1**.Comparison of various techniques

| S.NO | TITLE | EXTRACT OF THE PAPER | ROUTING OVERHEAD | DETECT FALSE MISBEHAVIOR REPORT | PREVENT ACKNOWLEDGEMENT FORGING | SOLVE RECEIVER COLLISIONS PROBLEM |
|---|---|---|---|---|---|---|
| 1 | TWOACK: preventing selfishness in mobile adhoc networks | TWOACK scheme to detectmisbehaving links by acknowledging every datapacket transmitted over eachthree consecutive nodes along the path from the source to | LARGE | NO | NO | YES |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | the destination. | | | | |
| 2 | An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs | The 2ACK scheme is to sendtwo-hop acknowledgmentpackets in the opposite direction of the routing path. In order to reduce additionalrouting overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme | LESSER THAN TWOACK | NO | YES | YES |
| 3 | AACK: Adaptive Acknowledgement Intrusion Detection for MANET with Detection Enhancement, | The AACK is a network layer acknowledgment based scheme, detects misbehaving node instead of misbehaving link and an end-to end acknowledgment scheme, to reduce the routing overhead of TWOACK. | LESSER THAN ABOVE TECHNIQUES | NO | NO | YES |
| 4 | Detecting misbehaving nodes in MANETs | Enhanced Adaptive ACKnowledgement (EAACK)scheme which consists of three parts (i) Acknowledge(ACK) (ii) Secure ACKnowledgement (S-ACK) (iii) Misbehavior Report Authentication (MRA). | SAME AS AACK | YES | NO | YES |
| 5 | Detecting Forged Acknowledgements in MANETs | Acknowledgement packets received in S-ACK phase of EAACK are digitally signed using Digital Signature Algorithm (DSA) to prevent the intermediate node from forging the S-ACK packet(EAACK2) | SAME AS AACK | YES | YES | YES |
| 6 | EAACK | The link between each node in the network is bi-directional, all acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its Receiver. | SAME AS AACK | YES | YES | YES |

## 5. MODULES

### 5.1 Network Creation and Routing

In this module, mobile ad-hoc network is created. Mobile nodes are configured with the properties like buffer, antenna..etc and randomly deployed in the network area. All the mobile nodes are connected with wireless links. The mobile can act as a data initiator or data forwarder which forwards the data from the other mobile nodes. A sample routing is performed to assess the connectivity of the network.

### 5.2 Implementation of WATCHDOG Method

In this module, a malicious node is randomly selected and configured. The malicious node continuously disturbs the network performance by doing unauthorized activities. The watchdog method is implemented across the network to identify the misbehaving nodes. The watchdog method constantly monitors the nodes activities and identifies the false nodes.

### 5.3 Performance Analysis

In this module, the performance of watchdog method is analyzed. Based on the analyzed results X-graphs are plotted. Throughput, delay, energy consumption are the basic

parameters are considered here and X-graphs are plotted for these parameters.

### 5.4 Implementation of EAACK

In this module, the EAACK method is configured in the network. The mobile nodes need to send the ACK to the sender node to acknowledge the packet delivery. EAACK method takes advantage of the ACK method. EAACK identifies the malicious nodes by non-receiving of ACK packets using different modes.

## 6. PERFORMANCE EVALUATION

In order to measure and compare the performance of our proposed scheme, we adopt the following performance metrics:

**1) Packet Delivery Ratio**: Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources.

**2) Delay**: Network delay is an important design and performance characteristic. The delay of a network specifies how long ittakes for a bit of data to travel across the network from one node or endpoint to another.

**3) Routing Overhead**: Routing overhead refers to the ratio of routing related transmissions.

## 7. PERFORMANCE ANALYSIS AND RESULT CONCLUSION

In this module, the performance of the proposed EAACK is analyzed. Based on the analyzed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters considered here and X-graphs are plotted for these parameters.
Finally, the results obtained from this module is compared with third module results and comparison X-graphs are plotted. Form the comparison result, final RESULT is concluded.

## 8. EXPECTED RESULTS ANALYSIS

The simulation results were conducted with the help of the Network Simulator. The simulation results and makes it easier to compare the results. The moving speed of mobile node is up to 30 m/s and a pause time of 1000 seconds. User Datagram Protocol with constant bit rate is implemented with a 512 B packet size of. To measure and compare the performance of proposed scheme, consider the following two parameters.Packet delivery ratio (PDR) and Routing overhead (RO). The comparison graph has been plotted between the malicious nodes and Packet Delivery Ratio.

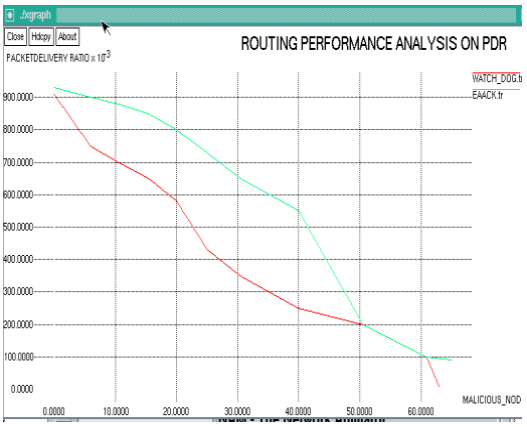


**Fig 2:** Performance analysis on PDR

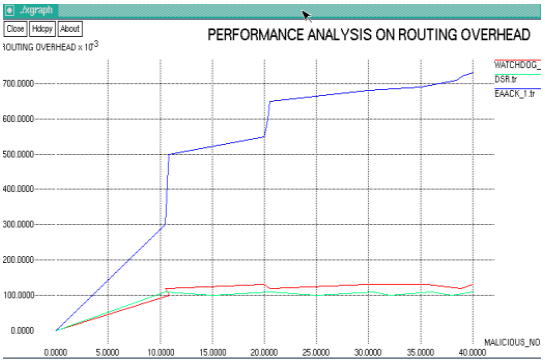


**Fig 3:** Performance analysis on RO

## 9. CONCLUSIONS

EAACK makes MANETs more secure .The major threats like false misbehavior report and forge acknowledgement can be detected by using this scheme. EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations.

- Results demonstrate positive performance against existing scheme such as watchdog, TWOACK.
- Digital signatures were incorporated which caused more ROs but vastly improves PDR when attackers are smart to entre forge acknowledgement packet. In proposed system we implemented both DSA and RSA but DSA scheme is more suitable.

## REFERENCES

[1]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routingmisbe- haviour in mobile ad hoc networks,” in Proc. 6th Annu. Int.Conf. Mobile Comput.Netw., Boston, MA, 2000, pp. 255–265.
[2]. Sheltami, T., Al-Roubaiey, A., Shakshuki, E. and Mahmoud, A. 2009. Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs
[3]. ElhadiM.Shakshuki, Senior Member, IEEE, Nan Kang, and TarekR.Sheltami, Member, IEEE TRANSACTIONS ON

INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.
[4]. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in MobileAd Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.
[5]. J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detectionand response for mobile ad hoc networks," in Proc. IEEE Int. Conf.Perform., Comput.,Commun., 2004, pp. 747–752.
[6]. A. Patcha and A. Mishra, "Collaborative security architecture for blackhole attack prevention in mobile ad hoc networks," in Proc. Radio WirelessConf., 2003, pp. 75–78.
[7]. A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Securerouting and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf.Pervasive Comput. Commun., 2005, pp. 191–199.
[8]. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digitalsignatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2,pp. 120–126, Feb. 1983.