*(IJIRSE) International Journal of Innovative Research in Science & Engineering*
***ISSN (Online) 2347-3207***

# Misbehavior Report Authentication Intrusion Detection System in MANETs

**[1]M.Geetha [2]N.Senthilkumar**
[1]PG scholar, [2]Assistant Professor
ECE department
VivekanandhaCollege of Engineering For Women
Mail id: geethasharthi@gmail.com, senthilsuguna@gmail.com

***Abstract*** **- Mobile Ad hoc Network is a collection of wireless mobile nodes forming a network without using any existing infrastructure. MANET is a collection of mobile nodes prepared with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or not directly. A new intrusion detection system named Enhanced Adaptive Acknowledgement (EAACK) specially designed for MANETs. By the implementation of Misbehavior Report Authentication(MRA) scheme, EAACK is able of detecting malicious nodes despite the existence of false misbehavior report and compared it against other popular mechanisms in different scenarios during simulation. The results will demonstrate positive performances next to Watchdog, TWOACK and AACK in the cases of receiver collision, limited communication power and false misbehavior statement. EAACK demonstrates higher malicious behavior detection rates in certain circumstance while does not greatly affect the network performances.**

**Keywords – Mobile Ad hoc Network, Enhanced Adaptive Acknowledgement (EAACK), Misbehavior Report Authentication (MRA), TWO Acknowledgement (TWOACK), Adaptive Acknowledgement (AACK).**
.

## I. Introduction

Due to their natural mobility and scalability, wireless networks are always preferred since the rest day of their creation. Due to the improved technology and reduced costs, wireless networks have increase much more preferences over wired networks in the past a lot of decades.

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. Industrial remote access and control via wireless networks are becoming more and more popular these days. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multi hop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range.

In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [10], [12]. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflict, and medical emergency situations [9], [7].

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry [5]. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [5], attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

### Advantages of Mobile Ad Hoc Networks

Having discussed the general issues in MANETs, the reason behind their popularity and their benefits will now be discussed.

Low cost of deployment: As the name suggests, ad hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.

Fast deployment: When compared to WLANs, ad hoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.

Dynamic Configuration: Ad hoc network configuration can change dynamically with time. For the many scenarios such as data sharing in class-rooms, etc., this is a useful feature. When compared to configurability of LANs, it is very easy to change the network topology.

In the next section, mainly focus on discussing the background information required for understanding this research topic.

## II. Related Work

As discussed before, due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To address this problem, IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and they are a great complement to existing proactive approaches [8]. In this section, mainly describe three existing approaches, namely, Watchdog [4], TWOACK [5], and Adaptive Acknowledgment (AACK) [3].

1) Watchdog that aims to improve throughput of network with the presence of malicious nodes. In fact, the watchdog scheme is consisted of two parts, namely Watchdog and Pathrater. Watchdog serves as an intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listens to its next hop's transmission. If Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter.

Whenever a node's failure counter exceeds a pre-defined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following researches and implementations have proved that the Watchdog scheme to be efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. Watchdog scheme fails to detect malicious misbehaviors with the presence of Ambiguous collisions, Receiver collisions, Limited transmission power, False misbehavior report, Partial dropping.

2) TWOACK is neither an enhancement nor a Watch-dog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).The working process of TWOACK is demonstrated in Figure 1 node A first forwards packet 1 to node B, and then node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious.

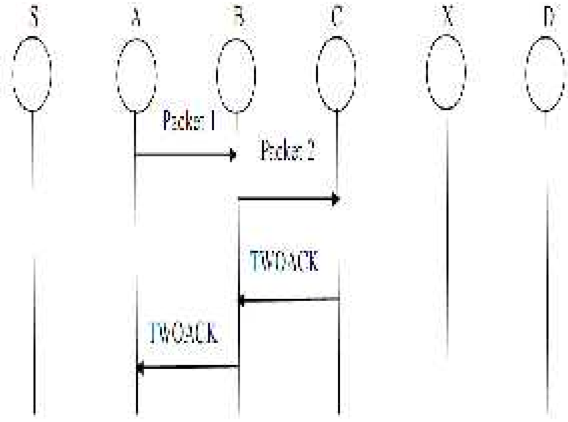

Figure 1.TWOACK

TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement process required in every packet transmission process added a significant amount of un-wanted network overhead. Due to the limited battery power nature of MANETs, Such redundant transmission process can easily degrade the life span of the entire network.

3) AACK is based on TWOACK Acknowledgement (AACK) similar to TWOACK,AACK is an acknowledgement-based network layer scheme which can be considered as a combination of a scheme call ACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining the same network throughput. Source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network over-head, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgement packets.

Both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets. In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such Detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic.

## III. Problem Definition

My proposed approach EAACK is designed to deal with three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. In this section discuss these three weaknesses in detail.

In the case of receiver collisions, demonstrated in Figure 2, after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding packet 2 to node C. In such case, node A overhears that node B has successfully, forwarded Packet 1 to node C, but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

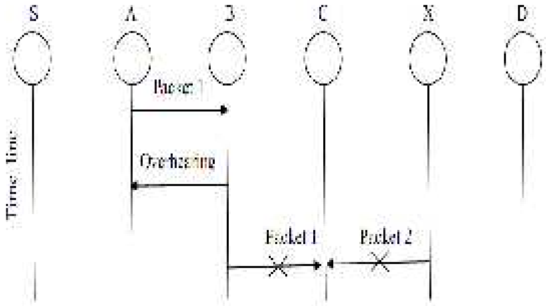

Figure 2.Receiver collision

In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C, as shown in Figure 3.

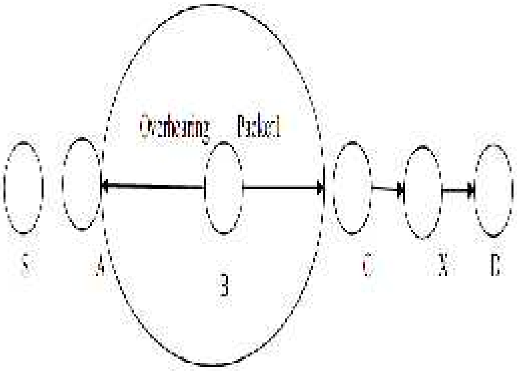

Figure 3.Limited Transmission power

For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, node a still reported node B as misbehaving as shown in Figure 4. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack.

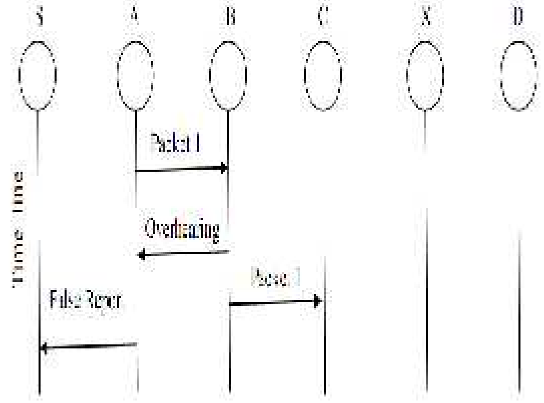

Figure 4.False misbehavior report

## IV. Scheme Description

In this section, describe my proposed EAACK scheme in detail. The approach described in this research paper is based on our previous work [12], where the backbone of EAACK was proposed and evaluated through implementation. In this paper, extend it with attacker from forging acknowledgment packets.

My proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

### 1. *A. ACK*

ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. In Figure 5 in ACK mode, node S first sends out an ACK data packet ad1 P to the destination node D.

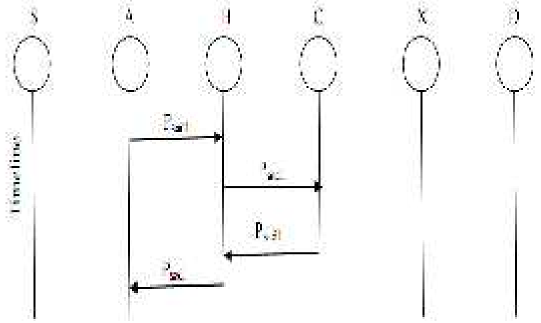

Figure 5.ACK

If all the intermediate nodes along the route between node S and node D are cooperative and node D successfully receives Pad1, node D is required to send back an ACK acknowledgement packet ak1 P along the same route but in a reverse order. Within a predefined time period, if node S receives ak1 P, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

### *2. B. S-ACK*

S-ACK scheme is an improved version of TWOACK scheme. The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgement packet to the first node. The intention of introduce

S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. As demonstrated in Figure 6 in S-ACK mode, the three consecutive nodes (i.e. F1, F2 and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet $P_{sad1}$ to node F2. Then node F2 forwards this packet to node F3.

When node F3 receives $P_{sad1}$, as it is the third node in this three node group, node F3 is required to send back an S-ACK acknowledgement packet $P_{sak1}$ to node F2. Node F2 forwards $P_{sak1}$ back to node F1. If node F1 does not receive this acknowledgement packet within a predefined time period, both nodes F2 and F3 are reported as malicious.

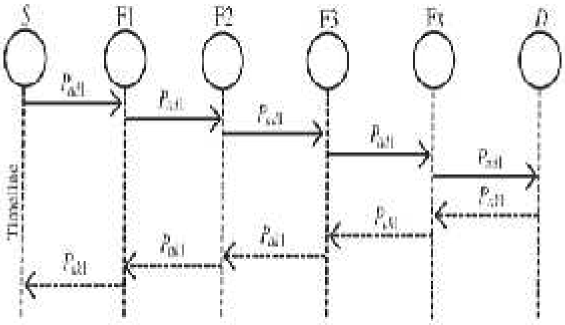

Figure 6.S-ACK

Moreover, a misbehavior report will be generated by node F1 and sent to the source node S. Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

### *3. C.MRA*

The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. False misbehavior report can be generated by malicious attackers to falsely report that innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node.

If there is none other exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehavior report and whoever generated this report is marked as malicious.

Otherwise, the misbehavior report is trusted and accepted. By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

## V. Conclusion

Packet dropping attack has always been a major threat to the security in MANETs. In this work a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulation. The results described positive performances against Watchdog, TWOACK and AACK in the cases of receiver collision and limited Transmission power and false misbehavior report.

Furthermore, in an effort to prevent the attackers from initiating a forged acknowledgement attacks, extended to incorporate digital signature in proposed scheme. Although it generates more routing overhead in some cases, as demonstrated in experiment, it can vastly improve the networks packet delivery ratio when the attackers are smart enough to forget acknowledgement packets. This trade-off is worthwhile when network security is of top priority. In order to seek the optimal digital signature algorithms in MANETs, implemented both DSA and RSA scheme in our simulation.

## REFERENCE

[1] R. H. Akbani, S. Patel, and D. C. Jinwala, “DoS attacks in mobile ad hoc Networks: A survey,” in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[2] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B Viollet, “Which wireless technology for industrial wireless sensor networks? The development of OCARI technol,” IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[3] T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[4] Ashish Kumar, Vidya Kadam, Subodh Kumar, Shital Pawar, “An Acknowledgement – Based Approach for the Detection of Routing Misbehavior in MANETS” International Journal of advances in Embedded Systems, vol.1, Issue.1, 2011.

[5] V. C. Gungor and G. P. Hancke, “Industrial wireless sensor networks: Challenges, design principles, and technical approach,” IEEE Trans. Ind.Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[6] Jun Yao, Salil S. Kanhere,, “Improving QoS in High-Speed Mobility Using Bandwidth Maps,”ieee transaction On mobile computing, vol. 11, no. 4, April 2008.

[7] N. Kang, E. Shakshuki, and T. Sheltami, “Detecting misbehaving nodes In MANETs,” in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10,2010, pp. 216–222.

[8] Liqun Hou and Neil W. Bergmann, “Novel Industrial Wireless Sensor Networks for Machine Condition Monitoring and Fault Diagnosis,” IEEE Trans. Ind. Electron., vol. 61, no. 10, pp. 4266–4278, Oct. 2012.

[9] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros-Mendez, “Energy harvesting from piezoelectric materials fully integrated in footwear,” *IEEE* Trans. Ind. Electron. vol. 57, no. 3, pp. 813–819,Mar. 2010.

[10]T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video Transmission enhancement in presence of misbehaving nodes in MANETs,"Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[11] A. Singh, M. Maheshwari and N. Kumar. "Security and Trust Management in MANET", in Communications in Computer and Information Science, vol. 147, part 3, pp. 384-387. Springer, 2011.