# A Secure Intrusion-Detection System using Enhanced Adaptive Acknowledgement for MANET'S

**Mr. I. Jose Sahayam[1] Mr. G. Karpaga Kannan[2]**
[1]M. E. (Final year) [2] M. E. (Assistant Professor)
[1, 2] RatnaVel Subramaniam College of Engineering & Technology

*Abstract*---Mobile ad hoc Networks (shortly called as MANETs) are of increasing interest for various sets of applications. Instead of using any centralized infrastructure, nodes in MANET cooperate with one another to provide networking during their movements. Such capability is essential for some special scenarios like battlefield or emergency field work wherever preexisting or centralized communication infrastructures are not offered. MANET on the battlefield will offer various services to support different missions such as enemy situation, battlefield map, etc. Such applications place increasing demands on reliable transport and persistent sessions. EAACK is capable of detecting malicious nodes despite the existence of false scheme report and compared it against alternative widespread mechanisms in many situations through simulation. The results will demonstrate positive performances against Watchdog, TWOACK and AACK within the cases of receiver collision, restricted transmission power and false misbehavior report, packet delivery Ratio. IDDSA demonstrates higher malicious- behavior-detection rates in certain circumstances while does not greatly have an effect on the network performances.

**Keywords:** Mobile ad hoc Networks (MANETs), Internet Engineering Task Force (IETF), IDDSA & EAACK.

## I. INTRODUCTION

Reliable server pooling is an approach that provides the reliability of services by introducing redundancy in the number of servers available to a client. A group of servers can be viewed as a single transport endpoint. When a particular server becomes unavailable due to any of a number of possible reasons, the next available server in the pool takes its place without breaking the current session.

Similarly, if bandwidth to one particular server shrinks or the server is handling heavy loads, connections can be transferred over to other servers in the pool as a form of load balancing. The architecture and protocols for the operation and management of Server Pool are being developed by Internet Engineering Task Force (shortly IETF) to support highly reliability-demanding applications on Internet. The advantages of Server Pool, especially the fail-over merit, make it very attractive in tactical MANETs. However, the characteristics of MANETs indicate that the Server Pool protocols for Internet applications have to be tailored largely to fit MANET applications.

The unique features of tactical MANETs also bring the application of Server Pool serious challenges in security. Wireless links are susceptible to the attacks ranging from passive eavesdropping to active impersonating. Nodes roaming in the battlefield have non-negligible probability of being compromised. The adversary could launch Byzantine attacks through the compromised node. Trust relationships among nodes may change from time to time due to the change of network topology and membership. Furthermore, since MANET has no fixed infrastructure, a centralized Certificate Authority is unlikely to be available. Therefore, the security mechanisms which are popular on the Internet are not sufficient to guarantee security of MANET applications.

A significant amount of security research in MANET focuses on some basic goals of secure routing, key agreement and key distribution. In general, security against Byzantine adversaries becomes even harder to achieve because of the lack of complete connections between parties, the mobility of the parties, resulting in connection changes, or lack of availability of parties, and the absence of a centralized public-key infrastructure.

On the contrary to traditional network architecture, MANET does not need a fixed network infrastructure; each single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers.

During this case, it\'s crucial to develop efficient intrusion-detection mechanisms improvements MANET from attacks. With the enhancements of the technology and cut in hardware prices, we are witnessing a current trend of expanding MANETs into industrial applications. To regulate to such trend, we powerfully believe that it is very important to handle its potential security problems.

In this paper, we propose and implement a new intrusion-detection system named adaptive accommodative Acknowledgment (shortly EAACK) specially designed for MANETs. Compared to modern approaches, EAACK demonstrates higher malicious- behavior-detection rates in certain circumstances while doesn't\'t greatly affect the network performances.

## II. PROBLEM DECLARATION

In proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog mechanism, namely, false misbehavior, limited transmission power, and receiver collision. In this section, we discuss these three weaknesses thoroughly. Our proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog mechanism, namely, false misbehavior, limited transmission power, and receiver collision. In this section, we discuss these three weaknesses thoroughly.

In Fig1 shows that both nodes B and X are trying to send Packet 1 and Packet 2, respectively, to node C at the same time.

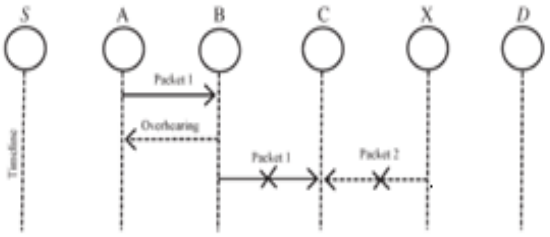



Fig. 1: Receiver collisions:

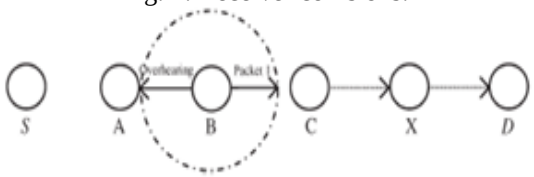



Fig. 2: Limited transmission power

In Fig.2 node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

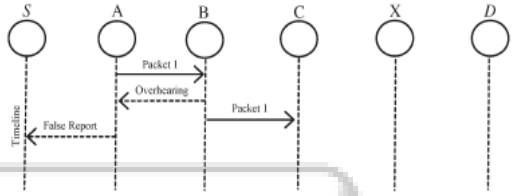



Fig 3: False misbehavior report

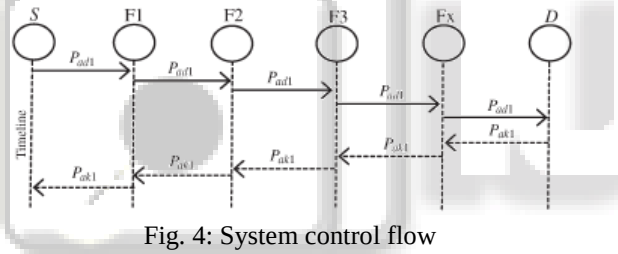



Fig. 4: System control flow

The above fig: 4 show the system flow of how the EAACK scheme works.

In a typical example of receiver collisions, shown in Fig. 1, once node a sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; in the meantime, node X is forwarding Packet a pair of two nodes C. In such case, node A overhears that node B has with success forwarded Packet one to node C however did not find that node C didn't receive this packet as a result of a collision between Packet one and Packet a pair of at node C. within the case of limited transmission power, in order to preserve its own battery resources, node B by choice limits its transmission power in order that it\'s strong enough to be overheard by node A however not catch enough to be received by node C. For false misbehavior report, though node A with success overheard that node B forwarded Packet one to node C, node A still reported node B as misbehaving.

A result of the open medium and remote distribution of typical MANETs, attackers will simply capture and compromise one or 2 nodes to realize this false misbehavior report attack. TWOACK and AACK solve two of those three weaknesses, namely, receiver collision and limited transmission power. However, each of them square measure vulnerable to the false misbehavior attack. During this analysis work, our goal is to propose new IDS specially designed for MANETs, that solves not only receiver collision and limited transmission power however additionally the false misbehavior problem.

Moreover, we extend our analysis to adopt a digital signature scheme during the packet transmission method. As in all acknowledgment-based IDSs, it is important to make sure the integrity and authenticity of all acknowledgment packets.

## III. SCHEMATIC APPROACH

### *A. Watchdog:*

It is very popular and highly efficient IDS for improving the throughput of network with the presence of malicious nodes. These IDS can be classified into two methods such as Watchdog and Path rater. It is responsible for discovering malicious node misbehaviors' in the network.

The Watchdog-IDS fails to discover malicious nodes in the following situations:

1) Ambiguous collisions;
2) Receiver collisions;
3) limited transmission power;
4) False misbehavior report;
5) Collusion; and
6) Partial dropping.

The main aim of this ID to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every 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 acknowledgment 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 TWOACK IDS effectively processes the receiver collision and limited transmission power problems indicated by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted 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. However, many research studies are working in energy harvesting to deal with this problem.

Each node is required to send back an acknowledgment packet to the node that is two hops away from it. The contrary too many other schemes, TWOACK is neither an enhancement nor a Watchdog-based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route required to send back an acknowledgment 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 shown in Fig. 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 that 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. The same process applies to every three consecutive nodes along the rest of the route.

*B. AACK:*

It is same *as* TWOACK IDS, AACK IDS is an acknowledgment-based network layer IDS. It can be treated as a combination of an ID called TACK (identical to TWOACK) and an end-to-end acknowledgment IDS called Acknowledge (ACK). Compared to TWOACK IDS, AACK IDS reduced network overhead.

The operation of DSR is divided into two activities: *Route Discovery* and *Route Maintenance*. In this section, we describe the basic form of Route Discovery and Route Maintenance in DSR. In DSR, when a node has a packet to send to some destination and does not currently have a route to that destination in its *Route Cache*, the node initiates Route Discovery to find a route; this node is known as the *initiator* of the Route Discovery, and the destination of the packet is known as the Discovery' *Target*, as illustrated in figure 1. The initiator (note *A*) transmits a ROUTE REQUEST packet as a local broadcast, specifying the target (node *D*) and a unique identifier from the initiator *A*. Each node receiving the ROUTE REQUEST, if it has recently seen this request identifier from the initiator or if its own address is already present in an address list in the REQUEST, discards the REQUEST. Otherwise, the appends its own node address to the address list in the REQUEST and rebroadcasts the REQUEST. When the ROUTE REQUEST reaches its target node, the target sends a ROUTE REPLY back to the initiator of the REQUEST, including a copy of the accumulated list of addresses from the REQUEST. When the REPLY reaches the initiator of the REQUEST, it caches the new route in its Route Cache. The DSR protocol also defines a number of optimizations to these mechanisms. Some of these optimizations, such as flow state, are relatively easy to secure whereas others, such as link-state caching, are more difficult (link-state caching requires some mechanism to authenticate links, but Ariadne only attempts to authenticate nodes). The use of these DSR optimizations is beyond the scope of this paper; we secure here only a basic version of DSR, with a limited path cache and without these optimizations.

It describe Ariadne primarily using the TESLA broadcast authentication protocol for authenticating routing messages, since TESLA is efficient and adds only a single message authentication code (MAC) to a message for broadcast authentication. Adding a MAC

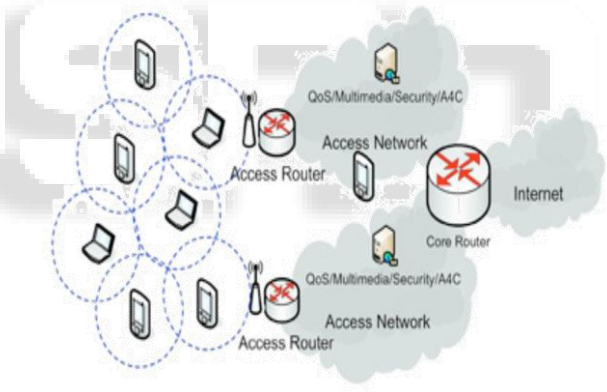
However, multiple receivers need to know the MAC key for verification, which would also allow any receiver to forge packets and impersonate the sender. Secure broadcast authentication thus requires an asymmetric primitive, such that the sender can generate valid authentication information, but the receivers can only verify the authentication information.

## IV. ID BASED DIGITAL SIGNATURE ALGORITHM (IDDSA)

TESLA differs from traditional asymmetric protocols such as RSA in that TESLA achieves this asymmetry from clock synchronization and delayed key disclosure, rather than from computationally expensive one-way trapdoor functions. To use TESLA for authentication, each sender chooses a random initial key *KN* and generates a *one-way key chain* by repeatedly computing a one-way hash function *H* on this starting value:

*i)* $KN-1 = H[KN]$, $KN-2 = H[KN-1]$,
*ii)* In general, $Ki = H[Ki+1] = HN-i$
*iii)* $[KN]$ *Kj from* a key $Ki, j < i$,
*iv)* $Kj = Hi-j\ [Ki]$.

To authenticate any received value on the one-way chain, a node applies this equation to the received value to determine if the computed value matches a previous known authentic key on the chain. Coppersmith and Jacobson present efficient mechanisms for storing and generating values of hash chains. Each sender pre-determines schedules of the time at which it publishes (or discloses) each key of its one-way key chain, in the reverse order from generation; that is, a sender publishes its keys in the order *K*0*, K1, KN*. A simple key disclosure schedule, for example, would be to publish key *Ki* at time $T0+i \cdot I$, where *T*0 is the time at which *K*0 is published, and *I* is the key publication interval. TESLA relies on a receiver's ability to determine which keys a sender may have already published based on loose time synchronization between nodes.




*A. OLSR:*

OLSR protocol is an optimization for MANET of legacy link-state protocols. The key point of the optimization is the multipoint relay (MPR). Each node identifies (among its neighbors) its MPRs. By flooding a message to its MPRs, a node is guaranteed that the message, when retransmitted by the MPRs, will be received by all its two-hop neighbors. Furthermore, when exchanging link-state routing information, a node lists only the connections to those neighbors that have selected it as MPR, i.e., its Multipoint Relay Selector set. The protocol selects bi-directional links for routing, hence avoiding packet transfer over unidirectional links. Like OLSR, TBRPF is a link-state routing protocol that employs a different overhead reduction technique. Each node computes a shortest path tree to all other nodes, but to optimize bandwidth only part of the tree is propagated to the neighbors. The FSR protocol is also an optimization over link-state algorithms using fisheye technique. In essence, FSR propagates link state information to other nodes in the network based on how far away

(defined by scopes which are determined by number of hops) the nodes are. The protocol will propagate link state information more frequently to nodes that are in a closer scope, as opposed to ones that are further away.

## V. CONCLUSION

This approach uses the Packet-dropping attack has always been a significant threat to the security in MANETs. In this analysis paper, we have proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against alternative popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog mechanism, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report.

This paper concludes the following major points:

*i)* Identifies and eliminate the misbehaving nodes
*ii)* Avoid the collisions
*iii)* Transmission powers are extended
*iv)* Packet delivery ratios are extended.

## VI. FUTURE WORK

IDDSA is used to carry out three of the six weaknesses of Watchdog mechanism, false misbehavior, and receiver collision. Watchdog scheme solves the receiver collision and limited transmission power.

## REFERENCES

[1] Architecture for reliable server pooling www.ietf.org /ids.by.wg/rserpool.html
[2] M. Fecko, U. Kozat, S. Samtani, M. Uyar, and I. Hökelek, "Architecture and applications of dynamic survivable resource pooling in battlefield networks," in Proc. SPIE, vol. 5441, Bellingham, WA, 2004,
[3] Dhurandher, S.K., Obaidat, M.S., Verma, K., Gupta, P., Dhurandher, P., "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems", Systems Journal, IEEE 2011 (Volume:5 , Issue: 2 ),
[4] Mohammed, N., Otrok, H., Lingyu Wang, Debbabi, M., Bhattacharya, P., "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", Dependable and Secure Computing, IEEE Transactions on 2011, Page(s): 89 – 103.
[5] Burmester, M., de Medeiros, B., "On the Security of Route Discovery in MANETs", Mobile Computing, IEEE Transactions on (Volume: 8, Issue: 9) Page(s): 1180 – 1188.