Enhancement of Intrusion-Detection System in MANETs

P. Rohini Vydehi, Srinivas Prasad, T.N. Shankar
M.Tech, Computer Sc. & Engg. GMR Institute of Technology
Faculty, Computer Sc. & Engg GMR IT, Rajam

Abstract—Most of the MANET IDs are referring watchdog scheme to thwart the malicious attacks, but this scheme fails to detect such type of destructive actions with the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior report, collusion and partial dropping. Enhanced adaptive acknowledgment EAACK is designed to handle three of the six weaknesses of the watchdog scheme namely false misbehavior, limited transmission power, and receiver collision by using the techniques ACK, 2-ACK, and misbehavior report identification MRI. Which is not fully efficient to resolve all the problems? This paper introduces digital signature with AOMDV to avoid forging acknowledgment packets from attackers. AOMDV throughput and routing overhead is better than and DSR protocols for the performance metrics like Packet Delivery Ratio and Routing Overhead.

Keywords: DSR, MANET, AOMDV, watchdog, ACK, 2-ACK, MRI.

I. INTRODUCTION

Mobile ad hoc network (MANET) and its security became very interesting topic in the research area of networking. MANET is a collection of mobile nodes which communicate via wireless radio links and without any central base station. Each node in the network acts as a router that forwards data packets for other nodes. At any instance a node may leave the network or rejoin, and free to move in any direction, because of the dynamic topology. It is difficult to route the packets towards the adjacent in the network for regular changes in topology. Flexibility and adaptability of MANETs make it more vulnerable to the malicious attacks. The routing protocol should design and chooses in such a way that it provides high reliability, security, power efficient, avoid overhead and provide best quality of service as well as should consider the unidirectional links also[1],[3]. Authentication and encryption would be used as the primary defense.

The security has a huge impact on the performance of any network. Intrusion Detection System (or IDS) generally detects any malicious threat to the systems. Less security in network facilitates the intruder to interrupt the transmission of data that leads towards data loss. Energy Consumption is more on the data transmission between the mobile nodes which effects on it.

Among the several kinds of attacks in MANETs, the attacks that are specific to the data transmission process are focused in this work. One of the main attacks against ad hoc networks affecting their routing protocols is named routing-disruption attacks.

II. BACK GROUND

Siddiq and Hymavathi have focused on real application of EAACK to overcome the Intruder attacks. Later Elhadi et al. have stressed on secure intrusion detection system for MANETS by using Enhanced adaptive acknowledgement EAACK technique as a novel contribution [1], [2].

How to defend the Intruders via Watchdog approach is published by Nidhi Lal [3].

Mahesh and Samir have discussed on AOMDV protocol which is an extension to AODV protocol for computing multiple loop-free and link disjoint paths [4].

A simulation and comparison of AODV, DSR and AOMDV routing protocols to prove the fastest process to detect the path are present in the paper by Chaddha et al. [5].

This paper is developed after a comprehensive study work on above articles.

A. Ad Hoc on-demand Multipath Distance Vector(AOMDV)

AODV routing protocol is based on route discovery procedure that is needed in case of link failure occurs in between source and destination. High overhead and latency increase at mobile nodes due to it. So this issue can be overcome by AOMDV which is available with the multiple paths. AOMDV protocol is specially designed to calculate multiple paths at the time of route discovery process in highly dynamic ad hoc networks in case of link breakage occurs for frequently moving nodes. Route discovery procedure is happened in case of overall paths to source or destination fails. The
routing information which is used by AOMDV routing protocol can be available in the AODV protocol is able to find a loop free paths.

Each copy of the route request packet received by a node introduces an alternate path back to the source. Using all such copies to establish routes may be chance to form routing loops. To overcome such type of problems, a similar invariant should be maintained as it is defined in single path case. However, the major inequality is the multiple next-hop routes obtained by multiple route advertisement are accepted and maintained as long as the invariant is complied. A possible drawback is that various routes to the same destination may have different hop-counts [3]. Therefore, route identification is required to determine which of these hop-counts is advertised to others due to impossibility of advertising different hop-count to different neighbors with the same destination sequence number.

According to the source and destination nodes, the advertised hop-count is defined as the maximum hop-count of the multiple paths for destination available at source. By using the maximum hop-count, the advertised hop count cannot be changed for the same sequence number. The alternate routes to the destination with lower hop-counts could only be accepted by applying this protocol which should be loop-free paths. Like this AOMDV will find multiple paths.

### Table I

<table>
<thead>
<tr>
<th>AODV</th>
<th>AOMDV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination</td>
</tr>
<tr>
<td>Sequence number</td>
<td>Sequence number</td>
</tr>
<tr>
<td>Hop-count</td>
<td>Advertised Hop-count</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Route-list {{nexthop1, hop-count1}, {nexthop2, hop-count2}…}</td>
</tr>
<tr>
<td>Expiration-timeout</td>
<td>Expiration-timeout</td>
</tr>
</tbody>
</table>

### B. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a routing protocol, which is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. DSR protocol uses source routing instead of using routing table at each intermediate device, and the routing information is maintained (continually updated) at mobile nodes. Determining source routes requires each node appends own identifier when forwarding RREQ during route discovery. The appended path information is caught by nodes processing the route discovery packets. The routed packet contains the address of each device to minimize the overhead cost to traverse a long distance. DSR optionally defines a flow id option that allows packets to forward on a hop-by-hop basis to avoid the source routing.

Route discovery and route maintenance are the two major phases of DSR protocol. Route reply would only be generated as soon as the message reaching at destination node. The destination node should return the route reply. The route would be used if the route is in the destination node’s route cache, else the node reverse the route based on the route record in the route reply message header. The route maintenance phase is initiated with the route error packets are generated at a node. The error generated hop should be removed from the node’s route cache and all routes containing the hop are truncated at that point. Again, the route discovery phase should be initiated.

### III. Digital Signature

Digital signature is a mechanism that is used to protect the information. Digital signature is an integral part of cryptography. Cryptography is a technique for secure communication in the presence of the third parties. Digital signature can be generalized as a data string, which associates a message (in digital form).[1], [3] In general, cryptography is a mathematical technique which related to aspects of information security such as confidentiality, data integrity, authentication, and data origin authentication. A digital signature scheme is mainly divided into two categories

1. **Digital Signature:** In this algorithm the original message is required to verify the signature. 
   Example: Digital Signature Algorithm (DSA).

2. **Digital Signature with Message Recovery:** 
   In this type of scheme there is no requirement of other information, signature itself is enough to verify.

![Fig.1. Communication with digital signature](image_url)

Anil
Balaji

Page 76
This paper implements both Digital Signature Algorithm DSA and RSA. The main purpose of this implementation is to compare the performances of both algorithms in MANETs. For every message m, a pre agreed hash function H is applied.

**Hashing (message) = message digest**  
In the Second step, the sender Anil needs to apply its own private key Private key-Anil on the computed message digest d. The result is a signature SigAnil. This signature is attached to message m and Anil’s secret private key.

**SecretPrivateKey−Anil (d) = SigAnil**  
The sender Anil should keep her private key Private Key−Anil as a secret without revealing to anyone else, to ensure the validity of the digital signature. Otherwise, if any attacker gets the secret private key of Anils, she/he can intercept the message and easily forge malicious messages with Anil’s signature and send them to Babu. As these malicious messages are digitally signed by Anil, Babu will see them as authentic messages from Anil. Thus, Eve can readily achieve malicious attacks to Babu or even the entire network.

After that Anil can send a message ‘m’ along with the signature SigAnil to Babu via an unsecured channel. Then Babu will compute the received message m against the pre-agreed hash function H to get the message digest d. This process can be generalized as

**Hashing (message’) = d’**

Babu can verify the signature by applying Anil’s public key Pk-Anil on SigAnil, by using

**SecretPrivateKey−Anil (SigAnil) = d**

If both the message digests are equal (i.e. d == d’) then it is safe to claim that the message m transmitted through an unsecured channel is indeed sent from Anil and the message itself is intact.

**IDS systems:** The researches had provided number of collaborative IDS systems namely

1. Watch dog  
2. ACK  
3. 2-ACK

**Watchdog**

Watchdog IDS works by listening the transmission to its next hop to detect malicious behavior. It increases its failure counter with a overhear of the next node fails to forward the packet within a certain period of time. The watchdog node reports a misbehaving when failure counter of a node exceeds a predefined threshold.

**IV. PROBLEM DEFINITION**

Three of the six weaknesses of Watchdog scheme: False misbehavior, limited transmission power, and receiver collision are handled by the proposed system. This section is stressed on these three weaknesses in detail.

---

**Fig 2. Receiver collision**

As shown in Fig 2 both nodes A and D are trying to send packets to node B at the same time node B is unable to receive the both the data.

**Fig 3 Limited transmission power**

In Fig 3 node A limits its transmission power so that the packet transmission can be overheard by node S, but it too weak to reach node B.

**Fig.4. False misbehavior report**
In Fig 4 Node A sends back a misbehavior report even though node B forwarded the packet to node D.

2-ACK and ACK solves receiver collision and limited transmission power was discussed. However, these two are vulnerable to the false misbehavior attack. This technique adopts the digital signature scheme during the packet transmission process to provide more security and overcome the problem of false misbehavior within the process finding acknowledgment-based IDSs.

A. ACK

The ACK is an end-to-end acknowledgment scheme. In the ACK scheme, the intermediate nodes simply forward the packet which sends out by the source node S. As soon as destination node D receives the Packet 1, it requires sending back an ACK acknowledgment packet to the source node S in a reverse order of the same route within a predefined period of time. Otherwise it must be switched to 2-ACK scheme.

B. 2-ACK

Misbehaving links can be identified by acknowledging every data packet transmitted over every three consecutive nodes along with the path from the source to the destination. First of all Node A forwards Packet 1 to node B, then node B forwards Packet 1 to node C. Now Node C is two hops away from node A and it is ready to generate a 2-ACK packet after receiving the Packet1. Whenever the node C sends a 2-ACK packet back to A then it is a successful transmission of Packet 1 from node A to node C. If 2-ACK packet is not received in a predefined time period, both node B and node C are reported as malicious. The same process applies to every three consecutive nodes along with the rest of the route. The misbehavior report is generated by node A and sends to the source node S. This technique requires the source node to switch in MRI mode to confirm this misbehavior report. This is a critical step to detect false misbehavior report.

C. MRI

The misbehavior report identification (MRI) is designed to identify the misbehavior report in the presence of false misbehavior report. This resolves the weakness of Watchdog when it fails to detect misbehaving nodes. In general the false report can be generated by malicious attackers to report the innocent nodes as malicious nodes. This type of attacks will cause great harm or destruct the network. The attack is dangerous when the attackers break down more number of nodes that cause a network division. The main aim of MRI scheme is to authenticate the destination node whether it is received the missing packet through different paths or not. To initiate the MRI mode, the source node first searches an alternative route to the destination node by using its local knowledge. If there is no alternative path then, the source node starts an AOMDV routing request to find another route.

The misbehavior reporter node can be stopped by adopting an alternative route to the destination node. The destination node searches its local knowledge base and compares if the reported packet was received or not as soon as receiving an MRI packet. Whoever generated this report is marked as malicious, if it is already received after that safe to conclude as a false misbehavior report. Or else, the misbehavior report is trusted and accepted.

V. SCHEME DESCRIPTION

Intrusion detection system on mobile ad hoc networks (MANETs) with the collaboration of three intrusion detection system (IDS): ACK, secure 2-ACK, and misbehavior report identification (MRI) are focused in this work. Digital signature is introduced to avoid forging acknowledgment packets from attackers. In proposed system a comparison of AOMDV and DSR protocol is present with performance metrics like packet delivery ratio and routing overhead. In a network the source and destination nodes are assumed as trusted nodes, and they act as both sender and receiver. All acknowledgment packets in a network system should be digitally signed at source node and verified by destination node.

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Packet Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Data</td>
<td>00</td>
</tr>
<tr>
<td>ACK</td>
<td>01</td>
</tr>
<tr>
<td>2-ACK</td>
<td>10</td>
</tr>
<tr>
<td>MRI</td>
<td>11</td>
</tr>
</tbody>
</table>

The Table-1 is showing distinguish the different packet types (ACK, 2-ACK and MRI) 2-bit packet header should be added.

IV PERFORMANCE EVALUATION

This section is focused on, simulation environment and methodology as well as comparing performances through simulation result comparison with AOMDV and DSR.
A. Simulation Methodologies

To measure the performance of proposed system under different types of attacks, three states have been proposed to simulate different types of misbehaviors or attacks.

State 1: In this state, a basic packet dropping attack is simulated. Malicious nodes simply drop all the packets that they receive. The purpose of this state is to test the performance of IDSs against two weaknesses of Watchdog, namely, receiver collision and limited transmission power.

State 2: This state is exclusively designed to test IDSs’ performances against false misbehavior report. Malicious nodes always drop the packets that they receive and send ack a false is behavior report whenever it is possible in case of it.

State 3: This state is intended to test the IDSs’ performances when the attackers are smart enough to tamper acknowledgment packets to claim positive result while, actually, it is negative. As Watchdog is not an acknowledgment-based scheme, it is not eligible for this state setting.

Algorithm:
Step 1: Start acknowledgement mode
Step 2: Check the node activity in packet mode
Step 3: If packet mode is ACK, then check whether reply is from destination or not.
Step 4: Else switch to 2-ACK mode.
Step 5: Go to step 2.
Step 6: If the packet mode is 2-ACK then check node misbehavior if yes send the MRI
Step 7: Else send ACK.

B. Simulation Configurations

The simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform. The system is running on a system with i3 processor and 4GB RAM. The Simulating parameters are shown in below Table 2.

<table>
<thead>
<tr>
<th>S.NO</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Simulator</td>
<td>NS-2</td>
</tr>
<tr>
<td>2</td>
<td>Channel type</td>
<td>Channel/Wireless Channel</td>
</tr>
<tr>
<td>3</td>
<td>Radio Propagation Model</td>
<td>Propagation/TwoRay Ground</td>
</tr>
<tr>
<td>4</td>
<td>Network interface Type</td>
<td>Phy/WirelessPhy</td>
</tr>
<tr>
<td>5</td>
<td>MAC Type</td>
<td>Mac /802_11</td>
</tr>
<tr>
<td>6</td>
<td>InterfaceQueue Type</td>
<td>Queue/DropTail/ PriQueue</td>
</tr>
<tr>
<td>7</td>
<td>Routing Protocol</td>
<td>DSR,AOMDV</td>
</tr>
<tr>
<td>8</td>
<td>Antenna</td>
<td>Antenna / Omni Antenna</td>
</tr>
<tr>
<td>9</td>
<td>Type of traffic</td>
<td>CBR</td>
</tr>
<tr>
<td>10</td>
<td>Area (M*M)</td>
<td>1216 *743</td>
</tr>
<tr>
<td>11</td>
<td>Simulation Time</td>
<td>50 sec</td>
</tr>
<tr>
<td>12</td>
<td>No of nodes</td>
<td>18</td>
</tr>
</tbody>
</table>

Table-II
SIMULATION PARAMETERS

To compare performances between DSA and RSA schemes, we generated a 1024-b DSA key and a 1024-b RSA key for every node in the network. We assumed that both a public key and a private key are generated for each node and they were all distributed in advance. The typical sizes of public- and private-key files are 654 and 509 B with a 1024-b DSA key, respectively.

1) Packet delivery ratio (PDR): PDR is the ratio of the number of delivered packets to the destinations divided by the total number of packets actually sent. The greater the value of the packet delivery ratio, the better is the performance of the protocol.

2) Routing overhead (RO): The additional costs incurred during the data packet delivery process. It contains routing-related transmissions (Route request (RREQ), Route reply (RREP), Route error (RERR), ACK, 2-ACK, and MRI).

3) Throughput (t): throughput is defined as the rate of successful message delivery over a communication channel.

Observations
In Fig 5 red color indicates the routing overhead in AOMDV routing protocol and the green color indicates the routing overhead in DSR routing protocol. When node moving frequently the routing overhead in AOMDV performance is less compare to DSR.

![Image](https://via.placeholder.com/150)

**Table 3 Comparison of Throughput and Energy**

<table>
<thead>
<tr>
<th>Results</th>
<th>AOMDV</th>
<th>DSR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of packets sent</td>
<td>14450</td>
<td>6153</td>
</tr>
<tr>
<td>Number of packets received</td>
<td>6772</td>
<td>4927</td>
</tr>
<tr>
<td>Throughput</td>
<td>213.379</td>
<td>124.88</td>
</tr>
<tr>
<td>Total energy required for nodes communicating</td>
<td>791</td>
<td>1695</td>
</tr>
<tr>
<td>Average energy required by each node</td>
<td>7.98</td>
<td>17.12</td>
</tr>
</tbody>
</table>

On observing the above results it concludes that the throughput is high in proactive routing protocol compared to the reactive routing protocol and nodes energy consumption is less in AOMDV than DSR.

**CONCLUSION AND FUTURE WORK**

In this paper the AOMDV protocol with digital signature has been proposed to achieve the enhanced security. Of course the overall performance of AOMDV is better than DSR. If the nodes mobility is high in the network then it is clear that reactive routing protocols are less preferable than proactive routing protocols in terms of overhead cost and speed. Only fixed numbers of nodes have been considered yet, no emphasis on mobility with neglected pause time. Find out the factors which are responsible for these simulation results, as well as better performance of AOMDV in various situations as compared to DSR are under the development. Further simulation needs to be carried out for the performance evaluation with not only increased number of nodes but also varying other related parameters like Pause Time, Network load, Speed.

**REFERENCES**


