World Conference on Information Technology

Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol

Ahmed M. Abdalla\textsuperscript{a}, Imane A. Saroit\textsuperscript{b}, Amira Kotb\textsuperscript{b}, Ali H. Afsari\textsuperscript{c} \textsuperscript{a*}

\textsuperscript{a} College of Technological, PAAET, Kuwait, Kuwait
\textsuperscript{b} College of Computer and Information, IT Department, Cairo University, Cairo, Egypt
\textsuperscript{c} College of Engineering, Kuwait University, Kuwait, Kuwait

Abstract

Intrusion Detection Systems (IDS) in Mobile Ad hoc Networks (MANETs) are required to develop a strong security scheme it is therefore necessary to understand how malicious nodes can attack the MANETs. Focusing on the Optimized Link State Routing (OLSR) protocol, an IDS mechanism to accurately detect and isolate misbehavior node(s) in OLSR protocol based on End-to-End (E2E) communication between the source and the destination is proposed. The collaboration of a group of neighbor nodes is used to make accurate decisions. Creating and broadcasting attackers list to neighbor nodes enables other node to isolate misbehavior nodes by eliminating them from the routing table. Eliminating misbehavior node allows the source to select another trusted path to its destination. The simulation results show that the proposed mechanism is able to detect any number of attackers while keeping a reasonably low overhead in terms of network traffic.

Keywords: - IDS; OLSR; Security; Ad hoc; MANETs.

1. Introduction

The Optimized Link State Routing (OLSR) protocol offers promising performance in terms of bandwidth, required overhead, and delivered traffic. In this paper, we present an intrusion detection system to accurately detect and isolate misbehavior node(s) in OLSR protocol based on End-to-End (E2E) communication between the source and the destination. The proposed mechanism is able to detect and isolate different attack types that could occur along the source-destination path by utilizing special messages. Our proposed IDS used the collaboration of a group of nodes to make accurate decisions. Although analysis is focused on OLSR protocol, the proposed solution is applicable to other routing protocols for MANETs.

The rest of this paper is organized as follows. Section 2 presented the background review for the OLSR protocol. Section 3 presents the IDS overview and related works that are important for the understanding of the material to follow. Sections 4 and 5 present the proposed contribution. The simulation results and discussion presented in section 6. Finally, conclusions drawn from the paper and future work are given in section 7.

2. The Optimized Link State Routing (OLSR) Protocol

OLSR is the table driven, proactive routing protocol designed for mobile ad-hoc networks. It exchanges routing information periodically and has route immediately available when needed. The OLSR protocol achieves optimization by determining for each node of the network a minimal subset of neighbors, called Multi Point Relays (MPR) which are able to reach all 2-hop neighbors of the node. Generally two types of routing messages are used a HELLO message and a Topology Control (TC) message [1-2].

1) HELLO message is periodically broadcasted by each node and contains the sender's identity and three lists:

\* Corresponding author. Tel.: +96599200578.
E-mail address: am.mahmoud@paaet.edu.kw, amamsaad@hotmail.com.
Ahmed M. Abdalla, Imane A. Saroit, Amira Kotb, Ali H. Afsari / Procedia Computer Science 00 (2010) 000–000

The OLSR operation can be summarized as follows:

1. **Neighbor sensing**: To achieve that each node broadcasts to its 1-hop neighbors HELLO messages periodically.

2. **MPR selection**: There are two types of sets
   - **MPR set**: This set of selected neighbor nodes for each node from its 1-hop neighbors. When a node sends a routing message, only the nodes that are in its MPR set forward this message.
   - **MPR selector set**: Each node also maintains information about the set of neighbors that selected it as MPR which is called MPR selector set.

3. **Topology Diffusion**: Nodes that were selected as MPR must send TC messages to construct routing table. TC messages are flooded in the network and only MPRs are allowed to forward TC messages. Each node in OLSR protocol has two tasks:
   - Correctly generate the routing protocol control traffic
   - Correctly relay the routing protocol control traffic on behalf of other nodes.

3. **IDS Overview And Related Works**

Intrusion detection is defined as the method to identify “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource”.

For Mobile Ad hoc Networks, the general function of IDS is to detect misbehaviors by observing the networks traffic in a Mobile Ad hoc [3].

Intrusion detection systems on wired network based have generally employed two models: signature based and anomaly based approaches. A signature-based IDS[4-5] monitors activities on the networks and compares them with known attacks. However, a weakness of this approach is that new unknown threats cannot be detected.

In anomaly-based detection [6], profiles of normal behavior of systems, usually established through automated training, are compared with the actual activity of the system to flag any significant deviation. A training phase in anomaly-based intrusion detection determines characteristics of normal activity; in operation, unknown activity, which is usually statistically and significantly different from what was determined to be normal, is flagged as suspicious. Anomaly detection can detect unknown attacks, but the issue is that anomaly based approaches yield high false positives for a wired network. If we apply these statistical approaches to MANETs, the false positive problem will be worse because of the unpredictable topology changes due to node mobility in MANETs.

The specification based approach, is recently presented and is ideal for new environments, such as MANETs.

In specification-based detection [7-9], the correct behaviors of critical objects are abstracted and crafted as security specifications, which are compared to the actual behavior of the objects. Intrusions, which usually cause an object to behave in an incorrect manner, can be detected without exact knowledge about the nature of the Intrusions. Currently, specification-based detection has been applied to privileged programs, applications, and several network protocols.

Most of recent researches focused on providing preventive schemes to secure routing in MANETs [10-14]. Key distribution and establishes a line of defense defined in [10], [11] is based on mechanism for in which nodes are either trusted or not and if trusted they are not compromised. Also contribution in [12], [14] considers the compromise of trusted nodes. It is assumed that a public key infrastructure (PKI) and timestamp algorithm are in place. However, the above approaches cannot prevent attacks from node who own a legitimate key.

It is necessary to understand how malicious nodes can attack the MANETs. A model to address the Black Hole Search problem algorithm and the number of agents that are necessary to locate the black hole without the knowledge of incoming link developed in [15]. Watchdog and path-rater discussed in [16] but it is noticed that it increases the percentage of overhead significantly with the percentage increase of misbehavior nodes. Ex-watchdog [17] suggests modifying the previous system to decrease of percentage of overhead.

[18] Introduces IDS which formulate the problem of distributed collaborative defense against coordinated attacks as a dynamic game problem. The same group extends their work in [19] by proposing detection schemes that are suitable to detect in-band wormhole attacks. The first detection scheme uses the Sequential Probability Ratio Test (SPRT) [20]. The SPRT has been proven to be an optimal detection test when the probability distributions of both normal and abnormal behaviors are given.
A feedback mechanism to secure OLSR against the link spoofing attacks was provided in [21], [22] the solution assesses the integrity of control messages by correlating local routing data with additional feedback messages called CPM sent by the receivers of the control messages.

Another formal approach to harden the MPR selection and thwart the attacks against OLSR suggested in [23]. This approach validates the routing table and the topology information using trust based reasoning. Hence, each node can verify the validity of the received HELLO and TC messages simply by correlating the information provided by these messages. A technique to detect the attack by discussing a collusion attack model against the OLSR protocol was presented in [24].

4. Mechanism For Detecting Misbehavior Nodes

The IDS we propose belongs to specification-based detection with distributed cooperative nodes that are suitable for MANETs. The misbehavior node detection process that we propose validates the communication path then detects and isolates misbehavior nodes in the invalid paths. The proposed IDS uses the collaboration of a group of nodes to make accurate decisions. The successfully detected misbehavior node is added to a black-list which is broadcast to all 1-Neighbors and so on to all network nodes. Then all neighbor nodes receive this list and it makes another confirmation by sending a PVM message to the attacker to be certain this node is actually an attacker. After confirmation it resends the black-list to its neighbors with a higher rating. When the neighbor receives this black-list it excludes the attacker from the routing table to ignore attacking attempts.

OLSR security vulnerabilities can be summarized as [19]:

- Identity spoofing
- Link spoofing
- Traffic relay/generation refusal.
- Replay attacks
- Wormholes

In this study, we are focusing only on traffic relay/generation refusal where the malicious node acts as a black-hole and drops packets. We introduced two types of attackers. The type-1 attacker drops all the received packets. The type-2 attacker is smarter and drops only data packets and exchanges control packets normally.

We extended the security of OLSR in two parts. The first part validates the communication path by sending periodic messages. The second part is concerned with finding malicious nodes in the invalid path. The process starts by sending Path Validation Messages (PVM) periodically to the destination at a specified interval, as shown in fig. 1.

The destination node is required to acknowledge back to the source with a reply-PVM to verify the validity of the path along which the data packets are transmitted. If the PVM fails to reach back to the source node before sending the next PVM, as shown in fig. 2, then the source node increases the number of failed PVMs. N failed PVMs mean there is a problem in the path and the source node triggers the attacker search process. The process starts by sending an Attacker Finder Message AFM to each node in the path to destination. Each intermediate node that receives the AFM is required to:

- Reply back to the source node with a message (AFM_b) that contains information about the hop count and the next-node-to-destination (NNTD)
- Send AFM to the destination through NNTD
The source node waits for acknowledgment from the intermediate nodes for a certain time. It updates the potential attacker information with the NNTD information received from each AFM received within the waiting time. Once the wait passes the last NNTD stored at the source is considered the attacker. This process is illustrated in fig. 3.

![Fig. 3 AFM process with type-1 attacker](image)

If all the nodes along the path reply back to the source with AFM, then the source starts the second process of the attacker search. This time the source sends a PVM to each node in the path and waits for a period of time. If the intermediate node replies back before the waiting interval, the source sends a PVM to the next intermediate node in the path. This process is repeated until it reaches its destination. If a node fails to reply within the waiting time then it is considered the attacker and is added to the black-list.

This attacker is considered of type-2 where it was dropping the data packets (PVM) but not the control packets (AFM). An extra step is added to ensure the type-1 attacker is correctly detected. A PVM is sent to the attacker and if it replies back to the source then it is considered a false detection is consequently and removed from the black-list.

![Fig. 4 (a) AFM process with type-2 attacker (b) AFM Algorithm](image)

5. Mechanism For Isolating Misbehavior Nodes

The detector node needs to share the information about the detected attacker with other nodes in the network. This is accomplished by flooding the network with Attacker Information Messages (AIMs). As we noticed from our previous work [25], nodes can be incorrectly detected as attackers due to network malfunction during a certain period. Such nodes would be wrongly isolated for the lifetime of the whole network. We added a verification step that would ensure nodes are correctly detected and isolated. The verification process relies on neighbors and attacker ratings to verify the attacker before they forward the AIMs.
The process illustrated in fig. 5 starts with the detector node sending AIMs to its first tier (N1) of neighbors. AIMs are initially sent with an attacker rating equal to one. The neighbor sends a PVM to the attacker node and waits for a specified period of time. If a reply to the PVM is received from the attacker before the period expires then it means that it was a false detection and the neighbor sends an AIM with rating equals to (-1) to other nodes. If the period expires then it means it is an attacker and the N1 neighbor increases the attacker rating and sends AIM to N2 neighbors.

The neighbors will maintain the verification process until a certain attacker rating value is reached after which the receiving neighboring nodes just forward the AIM without verification first. Each node receiving an AIM will add a record about the attacker to its blacklist table. To avoid having an infinite loop, it checks first for the (detector, attacker) pair in the table before adding. If a record is found, a packet is dropped. Otherwise the attacker verification and information sharing process will continue normally. Once the attacker information is shared among all network nodes, the attacker will no longer be able to participate in any communication with its neighbors. For every message received, nodes will check in their blacklist table for the sender to ensure it is not the attacker before processing the message.

### Fig. 5 (a) Flooding of AI messages (b) AI Algorithm

1. Source Send AIM to all neighbor nodes
2. Each Neighbor receive AI message check on (detector, attacker) pair in its black list table.
3. If pair found then
   4. Drop message
   5. Else
      6. Add to black list table
      7. If attacker rating > max. neighbor level to verify then
         8. Forward AI message to neighbor nodes
      9. Else
         10. Send PVM to malicious node (for verification) and Set PVM timer
      11. If PVM reply received before timer expired then
           12. Delete malicious node from black list table
           13. Send AIM to neighbors with attacker rating =-1
      14. Else
           15. Attacker rating ++ and send AIM to neighbors
      16. End if
     17. End if
    18. End if

### 6. Simulation Results And Discussions

The simulation results presented in this paper were performed using the network simulator ns2 version 2.31[26] with a modified version of the UM-OLSR [27] and an implementation version 0.8.8 of OLSR. The OLSR protocol implementation follows RFC 3626. The simulation scenarios consisted of 30 wireless nodes over an area 1500mX300m for duration of 900 seconds. We selected a rectangular shaped area to have good node scattering and collaboration.

The PVM messages were sent at a rate of 5% of the total data messages. We started with no attacker then increased it to 1, 2 and 3 attackers with each simulation. The main objective was to successfully detect and isolate the attackers.

Fig. 6 (a) shows the overhead of our proposed algorithm with respect to the total OLSR control packets. The figure above shows that when there is no attacker on the network the percentage of overhead is nearly 12% which is due to the fact that PVM packets are not dropped. Once an attacker is introduced in the network the percentage of overhead is reduced linearly with the increased number of attackers. Also the figure shows that smart attackers (attacker Type-2) produce an overhead that is slightly larger than a normal attacker (attacker Type-1) which can be contributed to the extra processing done by the type-2 process to send AFM and PVM packets.

Fig. 6 (b) shows the relation between percentages of dropped packets versus number of attackers. We can conclude from this figure that the percentage of the dropped data packets is small with no attacker as packets are not dropped intentionally. As the attackers are introduced into the network the number of dropped packet increases proportionally with the increase in the number of attackers. The figure above also shows that a smart attacker (attacker Type-2) drops less packets compared to type-1 because a smart attacker drops only PVM packets and forwards AFM packets normally.
Table 1 shows a sample of black-list table created at each node.

<table>
<thead>
<tr>
<th>Time</th>
<th>Detector</th>
<th>Attacker</th>
<th>Attacker rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>165.76738</td>
<td>25</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>165.8394</td>
<td>7</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>220.2</td>
<td>28</td>
<td>21</td>
<td>1</td>
</tr>
<tr>
<td>340.73298</td>
<td>23</td>
<td>21</td>
<td>3</td>
</tr>
<tr>
<td>341.66071</td>
<td>5</td>
<td>12</td>
<td>3</td>
</tr>
<tr>
<td>585.87079</td>
<td>22</td>
<td>24</td>
<td>-1</td>
</tr>
<tr>
<td>710.200</td>
<td>13</td>
<td>14</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 1 shows a sample of black-list table containing the attacker detector node and attacker node and time of detecting attacker. The last column indicates the attacker rating, this may take a positive value, which means that it is a certain attacker and as long as the positive value increases the degree of certainty this node is an attacker also increases. Then the node is eliminated from the routing table. The value of attacker rating = (-1) when the node detects that there is a false detection.

7. Conclusions and future works

We have presented an IDS mechanism based on End-to-End connection for securing the OLSR protocol. Our mechanism can detect and isolate many types of misbehavior node(s) through the path between the source and the destination then a blacklist of misbehavior nodes is created and broadcasting to 1-Neighbors.

The collaboration of a group of neighbor nodes is used to make accurate decisions. Eliminating misbehavior node(s) enables the source to select another trusted path to its destination.

We achieved better performance results when action was taken to isolate misbehavior nodes by utilizing the blacklist created and broadcasting to other nodes in the network. The simulation results showed that our mechanism is able to detect and then isolate any number of attackers, while keeping a reasonably low overhead in terms of network traffic.

Our future work will be focused on how to apply the proposed IDS on other MANET routing protocols methods.

References