Performance Analysis of Modified AODV Protocol in Context of Denial of Service (Dos) Attack in Wireless Sensor Networks

Ms. Shagun Chaudhary¹, Mr. Prashant Thanvi²

¹Asst. Professor, Dept. of ECE, JIET School of Engg. And Technology for Girls
Jodhpur, Rajasthan, INDIA
shagun.chaudhary17@gmail.com, 9413421380

²Asso. Professor, Dept. of EEE, JIET School of Engg. And Technology for Girls
Jodhpur, Rajasthan, INDIA

Abstract — Security of wireless sensor networks is an important concern due to the open and unaided nature of wireless sensor networks. The absence of central monitoring unit makes it vulnerable to several attacks. Denial of service attack (Dos) is an active internal attack which results in performance degradation of the wireless sensor network. This attack can be localized or distributed in nature based on intent of attack. In this paper, I am using modified variant of Ad-hoc On Demand Distance Vector (AODV) protocol to analyze the effect of Dos attack on system performance and later apply the prevention scheme to analyze the change in network performance.

Keywords — WSN, AODV, Modified AODV, Dos, NS-2, Route disruption, Resource consumption

INTRODUCTION
Denial of service (Dos) attacks is one of the most common types of attack which is possible in WSNs [1] [7] [8] [9] [11] [13]. DoS attacks are most common in networks which are distributed in nature i.e. lack a central control and each node operates on individual as well as cooperative basis and therefore WSNs are easily targeted by such attacks [1] [2] [4] [14]. Also the shared nature of network resources like power management and available bandwidth makes the WSNs more vulnerable to Dos attacks [3] [4] [5] [10] [12] [14].

Denial-of-service (Dos) consists of three components: authorized users, a shared service, and a maximum waiting time. A DoS situation can occur due to any kind of incident that diminishes, eliminates, or hinders the normal activities of the network [6] [8] [11] [12]. DoS indicate to a particular condition in a network and is termed DoS attack only when the intentions are to disrupt the normal working of the WSN [10].

Dos attack may limit or eliminate the network functionality than the normal expected standards [6] [4]. Dos attack may occur at any layer of OSI Model [3] [10] [11]. Dos attack is dangerous as it penetrates the efficiency of targeted networks by affecting its associated protocols. Dos attacks may consume the resources, destruct or alter the infrastructure configuration and physically destroy the network components [3] [4] [7] [10].

PROPERTIES OF DOS ATTACK
As stated by Anthony D. Wood and John A. Stankovic [6], the Dos attack has following properties:

Malicious- This act is performed intentionally. Accidental failures are the domain of fault-tolerance and reliability engineering. Since such failures can potentially produce equally disruptive results as DOS attacks, these fields have important contributions to make to the robustness of WSNs. They are not considered DOS, however, due to the lack of malice.

Disruptive- A successful DOS attacks destroy few services in the WSN. If the effect is not measurable, we may still say that an attack has occurred, but DOS has not. It can be said that damaging the affected service may not be the only goal of the attacker.

Asymmetric- Usually the effect of an attack is much greater than the effort required to mount it. In Dos attack, the effort in making a malicious node and using it to create flood of unwanted data traffic is less compared to the effort required in delivering normal data traffic to the nodes in network. This creates asymmetry in the network which results in high vulnerability and easy attack scenarios.
Remote- In distributed systems; an attacker can carry out an attack in the network. Often this is done by unauthenticated or lightly authenticated users. The high profile of DOS attacks make physical presence uncomfortable for the attacker.

**METHODOLOGY OF Dos ATTACKS**

All Dos attacks work by either of the below mentioned parameters –

**Node Isolation** -

Here a malicious node or attacker establishes a route between the source and itself consuming all the data from the source node and isolating it from the overall network. Thus the sender node becomes isolated from the network.

**Route Disruption** -

The malicious node establishes itself between the sender and receiver nodes and disrupts the route of data packages by making false entries in routing tables. This is achieved by sending fake RREP packages in response to RREQ from the sender node.

**Resource Consumption** -

The malicious node consumes precious network resources as power and bandwidth by broadcasting large number of irrelevant packages and thus the nodes actually requiring those resources are denied of them.

**PROPOSED SIMULATION MODEL**

NS-2 was used to simulate a WSN with 80 nodes. The simulation parameters are as below:

<table>
<thead>
<tr>
<th>Simulator</th>
<th>NS2 (version 2.35)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Time</td>
<td>300 (s)</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>20, 30, ..., 80</td>
</tr>
<tr>
<td>Simulation Range</td>
<td>1000 × 1000 m</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Attack Type</td>
<td>Black-hole, Dos, Sybil</td>
</tr>
<tr>
<td>Traffic</td>
<td>CBR</td>
</tr>
<tr>
<td>Pause Time</td>
<td>10 (m/s)</td>
</tr>
<tr>
<td>Max Speed</td>
<td>20 (m/s)</td>
</tr>
</tbody>
</table>

Attack detection is progressed by comparison of sequence number of RREP packet when sender node receives a reply packet. Seven different traffic scenarios and seven different network topologies were made for simulation purpose. 60 simulations for normal AODV working, 60 for Dos attack and its prevention were carried out yielding results in trace and NAM files for further analysis.

![Fig. 1 Topology Scenario for 80 nodes](www.ijergs.org)
RESULTS AND ANALYSIS

The performance of the WSN under Dos attack and later under the effect of modified AODV for Dos attack prevention was analyzed on the basis of four parameters: End to end delay, throughput, packet delivery ratio and packet drop ratio.

Average End-to-End Delay -

The performance of WSN under normal working with unmodified AODV shows the smallest delays in the network. Under Dos attack the average End-to-End delay rises due to network congestion and route disruption. By using the new modified AODV protocol the performance of the network can be increased by reducing the delay in real time. As the number of nodes increases the effect of delay is less visible.

Throughput -

The throughput of a normal WSN with unmodified AODV is maximum as shown in the figure below. With introduction of Dos attack the throughput is reduced as compared to previous condition. To improve the network efficiency the modified AODV protocol is used which results in increase in throughput on every node as is clear from the figure below.
Packet delivery ratio -

Maximum number of packets is delivered in case of normal working of WSN with unmodified AODV. As Dos attack is introduced, the packet delivery ratio decreases due to more package loss. The modified AODV increase the net packet delivery efficiency.

Packet drop ratio -

The unmodified AODV results in lowest number of drops in the system as shown in the simulation result below. Introduction of Dos attack in the system results in more packet drop by rerouting the traffic through the malicious nodes. The modified AODV protocol compares the routing tables on sender and malicious and isolates the route to the malicious nodes resulting in fewer packet drops.
CONCLUSION AND FUTURE SCOPE

Dos attack results in overall degradation of the capabilities of a WSN by affecting different parameters like end to end delay, packet delivery ratio, throughput and number of dropped packets. For successful attack detection various methods have been proposed over time. The technique used by me based on comparison on RREP sequence number of packet received by the sender from its neighbors broadcasting the availability of fresher or shorter routes. In future applications the intrusion detection can be made more robust and universal rather than attack specific. Also the malicious node isolation result in lesser nodes available for communication and thus a robust algorithm which quarantines the affected nodes without removing them from the system is proposed. The currently proposed method can detect an isolated incidence of Dos attack and minimizes its adverse effects but the attack can also be distributed in nature and therefore the detection and prevention algorithm has the potential of further improvement.

REFERENCES:


