Comparison of Variations in Performance of a WSN with Respect to Increasing Node Complexity under DOS Attack and Its Prevention

Shagun Chaudhary¹, Nitin Kumar²

¹Jodhpur Institute of Engineering and Technology – School of Engineering and Technology for Girls, Mogra, Jodhpur, Rajasthan, India

Abstract: In the recent years, the increase in number of nodes in a typical Wireless Sensor Network has led to specialized applications of these networks which were virtually not possible by the smaller and simpler networks. As the network becomes more complex, the behavior of individual node varies for parameter to parameter. Attacks on network also vary the different network parameters. Detailed analytical study should be employed to study the nature of Wireless Sensor Networks for large number of nodes with respect to different network topologies and different routing protocols along with various types of attacks.

Keywords: Performance parameters, Packet delivery ratio, Average end to end delay, Denial of service, Node density, Packet drop.

1. Introduction

The working of a Wireless Sensor Network is governed and restricted by the number of nodes that form the network. Each individual node has its own geographical range in which it can acquire process and transmit data. With increase in number of nodes the range of different nodes overlap resulting in a complex network. Network efficiency depends on various network parameters like number of packets delivered, number of packets dropped, network throughput and network overhead. Further these parameters are also affected by an attack on the network. The attack hampers the normal working of the network by diminishing available resources [1] [2] [3] [4] [5].

2. Denial of Service Attack & Prevention

A WSN in susceptible to various kinds of attacks ranging from passive eavesdropping to active node disruption and data re-routing [1] [2] [3]. Denial of service is the most common attack on a WSN resulting in diminished resources available for actual data transmission [9] [13] [14]. Dos attack can be isolated or distributed in nature. Also it can occur at every layer of network hierarchy [6][7][8][15]. There are different approaches to detect and prevent a DOS attack but most of them are ineffective mostly due to varied nature of attack as there is large number of possible attack scenarios simultaneously [10][11][12]. We have used the approach of RREQ sequence number detection. Detection and prevention stage is self sustaining and does not require external intervention. The performance of the network recovers effectively after using the prevention algorithm.

3. Simulation Model Parameters

The simulated network consists of 80 nodes and the simulated data is logged in the trace file. The data is further analyzed using awk scripts. The following modeling parameters where considered while network designing and simulation-

<table>
<thead>
<tr>
<th>Simulator</th>
<th>NS2 (version 2.35)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Time</td>
<td>200 (s)</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>20, 30, 40, 50, 60, 70, 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>Traffic</td>
<td>CBR</td>
</tr>
<tr>
<td>Pause Time</td>
<td>15 (ms)</td>
</tr>
<tr>
<td>Max Speed</td>
<td>30 (m/s)</td>
</tr>
<tr>
<td>Operating system</td>
<td>Ubuntu-12.04</td>
</tr>
</tbody>
</table>

4. Simulation Data Analysis

The simulated data is analyzed for four performance parameters defining the network efficiency under no attack condition, under DOS attack and under recovery phase.

4.1 Average Packet Delivery Ratio

Explanation – The average packet delivery ratio shows variations with respect to increasing node complexity as well as under no attack, attack and attack prevention stages. The packet delivery increases initially with increasing number of nodes as more number of alternate routes are available to data packets but as the network becomes complex, congestion takes toll and packet delivery drops for a network
a having large number of nodes. Under attack condition, the packet delivery is reduced for each corresponding node. Under the recovery phase the network tries to deliver maximum packets but the ratio is below the level of corresponding no attack condition.

4.2 End to End Delay

Explanation – Increasing node complexity results in more number of available routes thus shorter paths are always available between sender and receiver leading to corresponding decrease in end to end delays. Under attack the available resources becomes scarce and packet collisions ad network congestion results in increased delays. Under prevention phase, the network returns to its normal working with low delays with increasing number of nodes.

4.3 Packet drop

Explanation – packet drop is directly related to network congestion. As the number of nodes increases initially, alternate routes become available reducing congestion and reducing drop. After a while, network complexity increases to great extent leading to congestion and increased packet drop. Under attack, as the bandwidth and channels becomes restricted, drop increases. Under recovery, the malicious node is removed and network drop reduces.

5. Conclusion

Node complexity defines the range and capabilities of a wireless sensor network. A network having all the resources as bandwidth, memory, power can also become congested if node density is too large. Also DOS attack results in disrupting this resources making the congestion worse. Prevention or recovery schemes can increase the efficiency of the network but cannot restore 100 percent as compared to no attack condition. Thus I can be fairly concluded that the performance parameters fluctuate within a large range with increasing node density and network complexity.

References


Author Profile

**Shagun Chaudhary** did her B.tech in 2012 from RTU in Electronics and Communication Engineering. She is currently pursuing M.tech in digital communication from RTU. He is presently working as assistant professor in ECE department in JIET-SETG Jodhpur.

**Nitin Kumar** did his B.tech in 2011 from RTU in Electronics and Communication Engineering. He is currently pursuing M.tech in digital communication from JNU. He is presently working as assistant professor in ECE department in JIET-SETG Jodhpur.