Behavioral Malware Detection in Delay Tolerant Sensor Network

Maria Theresa Hoover¹ Mr. Manjunath C R²
¹,²Department of Computer Science & Engineering
¹,²Jain University

Abstract—Delay tolerant sensor networks (DTSNs) are a class of emerging networks that experience frequent and long-duration partitions and are kind of wireless mobile network which may lack continuous network connectivity. Multicast distributes the data to multiple users, a service is required for many DTSNs applications. There exist delay in the network due to link congestion and routing path length to overcome this problem the routing algorithm of minimizing maximum link congestion on grid networks is being used. There can be a possibility of malware occurrence to a node so depending upon the behavior of the node the malware detection is done. The proposed work aims at using threshold based filtering propagation algorithm to detect the malware in the network.

Key words: Delay Tolerant Sensor Networks (DTSNs), Multicasting, Grid Network, Threshold Based Filtering, Dijkstra Algorithm

I. INTRODUCTION

Delay tolerant sensor networks (DTSNs) are a class of emerging networks that experience frequent and long-duration partitions and are kind of wireless mobile network which may lack continuous network connectivity. Multicast distributes the data to multiple users, a service is required for many DTSN Applications [1][2]. There exist delay in the network due to link congestion and routing path length to overcome this problem the routing algorithm of minimizing maximum link congestion on grid networks is being used. [3]Malware is a piece of malicious code which disrupts the host node’s functionality and duplicates and propagates itself to other nodes via contact opportunities behavior malware detection in this network plays an important role where the malware is detected using threshold based filtering algorithm for propagation delay. Delay tolerant sensor network is used reduce the delay in the network and the best way is by using the grid link. Grid link mainly concentrates tolerating the delay in the networking and overcoming the link congestion and routing path length. Detection of the behavior of malware in the network plays an important role in the network and is detected by threshold based filtering propagation delay algorithm.

II. PROPOSED SYSTEM

Grid link formation of network is deployed where the delay, link congestion and routing path length are reduced using routing algorithm of minimizing maximum congestion on grid link networks algorithm and the nodes are randomly deployed in the grid link, it consists of multiple destinations. Behavior malware detection is checked using threshold based filtering propagation algorithm .the proposed work studied with parameters by simulations working of system is found marginally efficient.

III. SYSTEM ARCHITECTURE

The architecture of proposed work consists of a grid link network. The nodes are deployed inside the network, only the source is being placed outside the grid link network as shown in below figure.

A. Grid Link

Network is formed using the grid link where the node is being deployed inside the link only the source is being placed outside the link so that it is easy to send packets to multiple destinations.

B. Delay-Tolerant Networking

A Delay-Tolerant Network (DTN) is a general-purpose overlay network that operates on top of varying regional networks, including the Internet. DTNs allow regional networks with varying delay characteristics to interoperate by providing mechanisms to translate between their respective network parameters. Therefore, the underlying protocols and technologies for these regional networks may differ considerably, but the flexibility of the DTN architecture allows them to be connected to each other.

C. Malware Detection

In the network, the malware is detected based on the threshold value .If the node’s threshold value is lesser or greater than the given value it is detected as malware.

D. Routing

Routing is done using the dijikstra’s algorithm from single source to multiple destinations.

IV. OBJECTIVES

The objectives of the proposed work is shown below

- To establish an path between the nodes placed in grid network using dijikstra algorithm.
- To detect malware using threshold based filtering propagation algorithm.
- To compare the back pressure algorithm and grid link, dijkstras algorithm.

The assumptions for the proposed approach is considered as shown below

- The number of nodes assumed is 55, which are randomly deployed in the grid based network.
- Each grid consists of 8-10 nodes.
Delay value is assumed as 1000ms, 2000ms.

Threshold value assumed is 28ms

The proposed approach applied in two steps first: The data is sent form source to multiple destination using the dijkstras algorithm to find the shortest path, second is malware is detected based threshold value.

Algorithm of Dijisktras
While ([dict size $graph]]

Find unhandled node with least weight dict for {uu -} $graph

if [{Sd > [set dd [dict get $dist $uu]]} {set u $uu

set d $dd}

Nodes are deployed randomly in grid link. It consists of single source and multiple destinations and the packets are sent from source to destinations using the shortest path. the malware is detected based on the threshold value given. delay is calculated for nodes before and after getting affected.

V. ANALYSIS

The grid network consists of randomly deployed nodes where it consists of single source and multiple destinations. path is determined for delivering the data packets using dijkstras algorithm for multiple destinations.

The energy consumed to form grid link is 30joules and to deliver packets using dijkstras algorithm it consumes 30joules.

A. Observations

Working of the proposed approach, the considerations of 3 sets of delay for pre-defined multiple destinations and 1 destination per grid is chosen and the delay value is given as 1000ms for different destinations.

<table>
<thead>
<tr>
<th>Delay</th>
<th>Delay</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destinations</td>
<td>42.45</td>
<td>41.8</td>
</tr>
<tr>
<td>Threshold Value</td>
<td>30.651ms</td>
<td>28.48ms</td>
</tr>
<tr>
<td>Average End to End Delay</td>
<td>398.7ms</td>
<td>231.13ms</td>
</tr>
</tbody>
</table>

Table 6.1: Three sets of delay

The comparison of the proposed work is compared with back pressure algorithm, the results are shown below.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Generated Packets</th>
<th>Received Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back pressure algorithm</td>
<td>1526</td>
<td>15461</td>
</tr>
<tr>
<td>Dijisktras, grid link algorithm</td>
<td>4220</td>
<td>4198</td>
</tr>
</tbody>
</table>

Table 6.2: Comparison of back pressure algorithm and dijkstras, grid link algorithm

Back pressure algorithm and dijkstras algorithm are used to find the shortest path to reach multiple destinations. The above table compares the packets received to multiple destinations. The generated packets using back pressure algorithm is 1526 and the packets generated using dijkstras algorithm is 4220. Received packets of dijkstras algorithm is approximately equal to the generated packets and the packets received is 50 % more than the generated packets this shows the performance of delivering the packets using dijkstras algorithm is better compared to the back pressure algorithm.

VI. CONCLUSION

Here routing algorithm of minimizing maximum link congestion on grid links reduces the link congestion and path length in the grid link and dijkstras algorithm is used to build path from source to multiple destinations. malware in the grid network is detected using the threshold value.

Comparison with the back pressure algorithm shows the efficiency of proposed algorithm in delivery of packets. the future work is that many destinations can be built in a single grid.

REFERENCES


