Behavioral Malware Detection in Delay Tolerant Sensor Network

Maria Theresa Hoover[1] Mr. Manjunath C R[2]
[1,2]Department of Computer Science & Engineering
[1,2]Jain 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, Dijikstra 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.

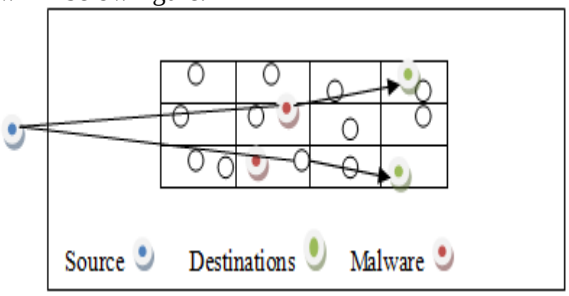

Fig. 1: System Architecture

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, dijikstras 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 dijikstras algorithm to find the shortest path , second is malware is detected based threshold value .

Algorithm of Dijikstras

```
While {[dict size $graph]} {
 Find unhandled node with least weight
dict for {uu -} $graph {
 if {$d > [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 dijikstras algorithm for multiple destinations.

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

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.

	Delay 1	**Delay 2**	**Delay 3**
Destinations	42,45	41,8	31,45
Threshold Value	30.651ms	28.48ms	26.451ms
Average End to End Delay	398.7ms	231.13ms	200.08ms

Table 6.1: Three sets of delay

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

	Generated Packets	Received Packets
Back pressure algorithm	1526	15461
Dijikstras, grid link algorithm	4220	4198

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

Back pressure algorithm and dijikstras 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 dijikstras algorithm is 4220. Received packets of dijikstras 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 dijikstras algorithm is better compared to the back pressure algorithm

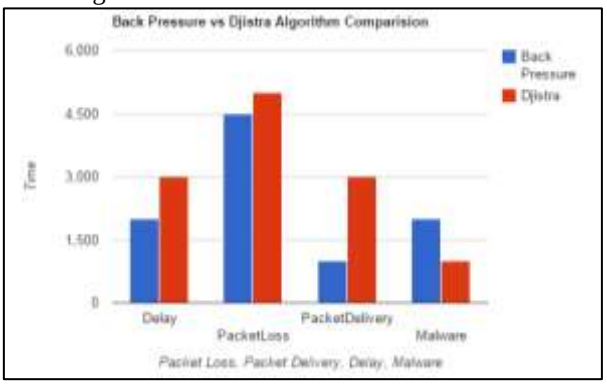

Fig. 2: Graph

The above graph shows that using dijikstras, gridlink network has better performance under packet delivery ratio, delay and detection of malware

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 dijikstras 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

[1] Muhammad Abdulla, "A simulation analysis of multicasting in delay tolerant networks", Department of Computer Science George Mason University Fairfax, VA 22030, U.S.A.IEEE 2006.
[2] Yunsheng Wang, "multicasting in delay tolerant networks: delegation forwarding", Department of Computer and Information Sciences Temple University Philadelphia, PA 19122, USA.
[3] Vinod P.," Survey on Malware Detection Methods", Department of Computer Engineering, Malaviya National Institute of Technology, Jaipur, Rajasthan.
[4] Wei Sun,"On Delay-Tolerant Networking and Its Application" International Conference on Computer Science and Information Technology.IEEE 2011.
[5] Pubudu N. Pathirana," Node Localization Using Mobile Robots in Delay-Tolerant Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING 2005.
[6] Silvio Cesare, Member, Yang Xiang, and Wanlei Zhou "Control Flow-Based Malware Variant Detection"IEEE 2014.
[7] Wei Peng, Feng Li, Xukai Zou, Jie Wu "Behavioral Detection and Containment of Proximity Malware in Delay Tolerant Networks**"** 2011 Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems.
[8] Feng Li,Yinying Yang Jie WuCPMC" An Efficient Proximity Malware Coping Scheme in Smartphone-based Mobile Networks" IEEE 2010.

[9] Mihai Christodorescu and Somesh Jha ," Testing Malware Detectors", in Proc. ISSTA'04, July 11 - 14, 2004.
[10] Bailey, m., Oberheide, J., Andersen, J., Mao, Jahanian, f., and Nazario, j. Automated Classification and Analysis of Internet Malware. In Symposium on Recent Advances in Intrusion Detection (RAID) (2007).

