International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Robustness Strategy for Securing Data from Cyber Attacks

Tanay P. Vartak[1], Harshada V. Ankam[2], Komal K. Randive[3], Amrita A. Shirode[4]

[1,2,3]Student, Dept. of Computer Engineering, AISSMS Polytechnic, Maharashtra, India.
[4]Professor, Dept. of Computer Engineering, AISSMS Polytechnic, Maharashtra, India.

Abstract - *This paper first presents a new modeling strategy to generate scale-free network topologies, which considers the constraints in WSNs, such as the communication range and the threshold on the maximum node degree. ROSE, a robustness increasing algorithm for scale free wireless sensor network, is proposed. Given a scale-free topology, ROSE utilize the position and degree information of nodes to rearrange the edges to similar to an onion-like structure, which has been proven to be robust against malicious attacks. Meanwhile, ROSE does not change the degree of node such that the resulting topology remains scale-free. The extensive experimental results verify that our new modeling strategy indeed generates scale-free network topologies for WSNs, and ROSE can significantly improve the robustness of the network topologies generated by our modeling strategy.*

Key Words: **Wireless sensor networks (WSNs), Node, Layers, Degree, and Bandwidth**

1. INTRODUCTION

Wireless sensor networks (WSNs) are an important type of network for sensing the environment and collecting information. In order to sense environmental parameters, a large number of sensor nodes, such as sink nodes and sensor nodes, are deployed in distributed areas. These nodes form a multi-hop ad hoc network system and execute assigned tasks according to the application requirements. WSNs have been deployed in homes, buildings, forests, mountains, etc. The sensor network topology describes the wireless communications among the various sensor nodes in WSNs and is the basis for the design of various network communication protocols and routing protocols which play a vital role in network properties, such as network lifetime, energy consumption, reliability, and data latency. In random attacks, the attacker randomly chooses nodes in the network topology as the targets, whereas in malicious attacks, the attacker chooses the nodes with high node degrees as the targets. It is known that some types of network topologies are resistant to random attacks and some are resistant to malicious attacks. In this project, the proposed system ROSE can significantly improve the robustness of the network topologies generated by our modeling strategy. The scale-free topology belongs to the field of complex network theory which has broad applications in the real world, such as in global transportation networks cooperation networks of social networks and mobile networks. The main contribute in this paper malicious detected by using distributed network.

1.1 ROSE Overview

ROSE is designed to be processed in a centralized system. Before ROSE operates, each node sends its own coordinates and neighbor list to the centralized system through the multi-hop system. After we achieve the optimization results according to ROSE, the centralized system sends the new neighbor list to each node through the multi-hop system. To help explain ROSE, we first introduce the basic ideas of ROSE in this section. Then, we provide the details of ROSE in the following section. In general, the design of ROSE is based on the observation of Schneider et al. that graphs exhibiting an onion-like structure are robust to malicious attacks. Schneider et al. described the onion-like structure as a structure "consisting of a core of highly connected nodes hierarchically surrounded by rings of nodes with decreasing degrees." Note that Schneider et al. validated their observation only by extensive simulations. One year later, the theoretical analysis supporting this observation was provided by Tanizawaet al. Since the onion-like structure encompasses a family of network topologies, Tanizawa et al. analyzed one specific topology called the "interconnected random regular graphs" of this family, and proved its robustness against malicious attacks. Given that the above observation about the onion-like structure has been validated both experimentally and theoretically, the ROSE algorithm is aimed to transform network topologies to exhibit the onion-like structure. Specifically, ROSE involves two phases: a degree difference operation and angle sum operation.

2. Metrics of Robustness:

Under a local node failure or attacks, some nodes or edges of the topology are destroyed in WSNs, which leads in general to separation of the initial connected network. We assume the WSNs suffer random and malicious attacks. Random attacks comprise random selection and removal of nodes in a WSN to destroy the connectivity of the entire network. However, malicious attacks are aimed to destroy the most important node in a WSN and achieve the worst damage to the entire network topology. We determine the importance of nodes according to the degree. A node with a higher degree is more important than that with a lower degree. We determine a malicious attack scheme that is based on node degree to enhance the robustness of scale-free networks against malicious attacks. First, the degree of each node in the scale-free network is counted and the node with highest degree is removed. The edges connected to it

are removed at the same time. Then, we reorder the remaining nodes by their degree. The current highest degree node is removed. This process is repeated until all the nodes are isolated in the network. If more than one node has the highest degree, we randomly select a node to attack. This attack scheme is more hostile, and therefore, the metrics of robustness based on this attack scheme can reflect the robustness against malicious attacks "more obvious."

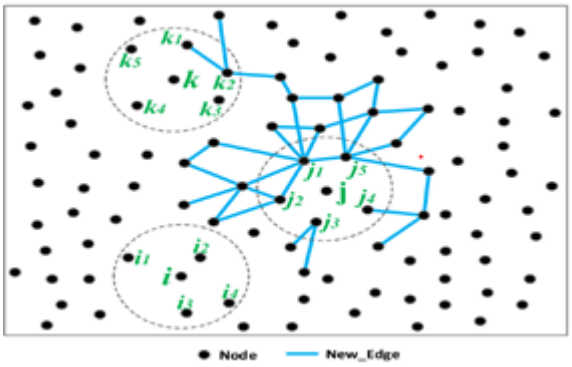

Fig -1: Scale free network

Ref: ROSE: Robustness Strategy for Scale-Free

Wireless Sensor Networks

In a recent paper, a new metric of robustness based on the percolation theory was proposed by Schneider et al. It considers the maximal connected sub graphs after the repeated removal of the highest degree node to measure the robustness of the network topology. We combined this metric with the malicious attacks scheme presented above, and describe network connectivity through calculating the proportion of maximal connected sub graphs of the entire network, and evaluate the extent of the damage. In a network with N nodes, the robustness metric R is defined as, R=1N+1∑n=0N−1MCSnN (3) in our topology construction strategy for WSNs, we restrict the order in which each node adds edges. For this reason, the nodes near the center of the network tend to have larger degrees than those near the boundary of the network. If the distance of two nodes from the coordinates of the centroid is the same, they have the greatest probability of having the same or similar degrees.

3. Methodology

Due to the recent proliferation of cyber-attacks, improving the robustness of wireless sensor networks (WSNs), so that they can withstand node failures has become a critical issue. Scale-free WSNs are important, because they tolerate random attacks very well; however, they are not protected from malicious attacks, which particularly target certain important nodes. In recent years, because of the rush in cyber-attacks increasing the robustness of the WSNs has become a critical issue. In existing a hill climbing algorithm introduced which is based on robustness metric R, which makes the network topologies resemble a stable distributed network structure through swapping edges. However, the multimodal phenomenon may prevent the algorithm from jumping out of the local optimum.

The proposed methodology ROSE enhances the robustness of scale-free networks against malicious attacks without changing the node degree distribution. ROSE consists of two phases: the degree difference and the angle sum operation. Both operations are aimed to transform the network topology toward the distributed network structure, which was shown in to be robust against the malicious attacks. The degree is assigned to each node to form the ROSE structure. The degree is just like weight or BW or capacity or range of node which is assigned by the system randomly at the time of registration or network topology creation.

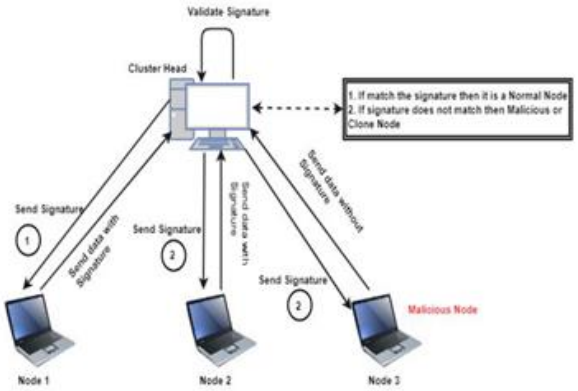

Fig -2: System Architecture

In this higher degree node is cover up by the lower degree nodes. In an distributed network structure, the nodes that have the same or similar degrees are connected with each other. All the neighbors of a high degree node have high degrees. The main contributions in this paper malicious are detected using distributed network.

3.1 Degree Difference operation

The degree is assigned to each node to form the ROSE structure (distributed network –like structure). The degree is just like weight or BW or capacity or range of node which is assigned by the system randomly at the time of registration or network topology creation. In this higher degree node is cover up by the lower degree nodes. In a distributed network -like structure, the nodes that have the same or similar degrees are connected with each other. All the neighbors of a high degree node have high degrees. When the node fails, its neighbors can replace its original function and ensure the connectivity of the residual network. Thus, the destruction of malicious attacks is weakened to a great extent in WSNs. At the same time, the distributed

network -like structure retains the property of the scale-free network. The majority of nodes have low degrees. The admin will send the signature or witness message to each node at time of registration.

Depends on this signature or witness messages the malicious nodes are detected which are affected by malicious or random attacks. When attacker attacks the node the signature / witness message will automatically changes. These signatures are stored at admin side in form of digest by using MD5 algorithm.

3.2 Distributed Network

The admin will send request to all nodes for witness message to detect the malicious node in the network. Upon receiving the request from the admin the node will send the signature to admin. (The victim i.e. the infected node doesn't know about the attack). Once admin receives the signature the system generates the digest of that message and validation of digest message which is available at admin and received digest is done. If doesn't matches the system will gives the alert for malicious node in the network.

4. CONCLUSION

A newly proposed algorithm called ROSE was designed for enhancing the robustness of scale-free networks against malicious attacks. The combination of a degree difference operation and an angle sum operation in the algorithm makes scale-free network topologies rapidly approach an onion-like structure without changing the original power-law distribution. Finally, the performance of ROSE was evaluated on scale-free network topologies having different sizes and edge densities. The simulation results show that ROSE significantly improves robustness against malicious attacks and retains the original scale-free property in WSNs at the same time. ROSE shows better robustness enhancement results and consumes less computation time.

REFERENCES

[1] F. M. Al-Turjman, H. S. Hassanein, and M. Ibnkahla, "Towards prolonged lifetime for deployed WSNs in outdoor environment monitoring," Ad Hoc Netw., vol. 24, pp. 172–185, Jan. 2015.

[2] S. Ji, R. Beyah, and Z. Cai, "Snapshot and continuous data collection in probabilistic wireless sensor networks," IEEE Trans. Mobile Comput., vol. 13, no. 3, pp. 626–637, Mar. 2014.

[3] J. Long, A. Liu, M. Dong, and Z. Li, "An energy-efficient and sinklocation privacy enhanced scheme for WSNs through ring based routing," J. Parallel Distrib. Comput., vols. 81–82, pp. 47–65, Jul. 2015.

[4] A. Munir, A. Gordon-Ross, and S. Ranka, "Multi-core embedded wireless sensor networks: Architecture and applications," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 6, pp. 1553–1562, Jun. 2014.

[5] P. Eugster, V. Sundaram, and X. Zhang, "Debugging the Internet of Things: The case of wireless sensor networks," IEEE Softw., vol. 32, no. 1, pp. 38–49, Jan. 2015.

[6] T. Qiu, R. Qiao, and D. Wu, "EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things," IEEE Trans. Mobile Comput., to be published,doi: 10.1109/TMC.2017.2702670.

[7] Z. Li and H. Shen, "A QoS-oriented distributed routing protocol for hybrid wireless networks," IEEE Trans. Mobile Comput., vol. 13, no. 3, pp. 693–708, Mar. 2014.