International Journal of Pure and Applied Mathematics
Volume 120 No. 8 2018, 187-195
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

A Predictive Based Localization Method for Wireless Sensor Network

Rajesh M*, Y Sahana and Rajiv Vincent
School of Computing Science Engineering
Vellore Institute of Technology, Chennai, India
rajesh.m@vit.ac.in

Abstract

The moto of location based key management system is to solve the issues that occur when sensor node tries to send the information from source to destination and to create a secure communication between the wireless sensor networks. The difficulties that occur in sensor node while passing the information from source to destination are Storage deficiency, Time delay in data exchange , packet drop, decrease in energy and some insider attacks. An insider attack is a malevolent attack that can be performed on a network by a human with authorized system access. Insiders that accomplish attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system procedures. This paper attempts to solve the problems that occur when a sensor node tries to send the collected information to the respected destination node.

Key Words: Insider attacks, Storage deficiency, Time delay, External attacks, Packet drop, Trustable nodes, Localization method, Wireless Sensor Network.

*Corresponding Author: Rajesh M

1 Introduction

Wireless sensor network comprises of a collection of spatially dispersed sensors that are used to detect or identify any environmental changes and arrange the collected data at a centralized location. The characteristics of wireless sensor networks are low cost, concurrency Processing, restricted energy resources and self-organization. The sensor node has three parts.

- Operating System which performs device-specific tasks.
- Sensor driver is a driver in which initializes the sensor hardware and performs the measurements in the sensor.
- Host middleware is the one which organizes the co-operation of distributed nodes in the network.

The main issues of the system are Energy efficiency, Increase in traffic so that it decreases the lifetime. The main advantages of wireless sensor networks are lot of wiring will be decreased and it can be accessed through a centralized monitor. The disadvantages of this system are it is too costly and gets distracted from various elements. Here individual nodes interact with distributed middleware layer to perform the functions dictated by the sensor network application.

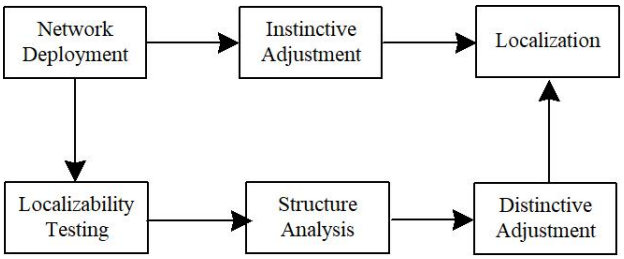

Figure 1: Architecture Diagram

Insider Threats: *False Positive:* In a WSN, the information or the packets are sent through a path of nodes where some of the intermediate nodes misbehave, manipulate the actual data and send to the right destination
False Negative: In the same way while transferring the packets,

some of the intermediate nodes misbehave and never send the information to the right destination

2 Literature Survey

In order to achieve security in wireless sensor networks one should follow encryption methods among sensor nodes in the network. The keys which we use for encryption purposes are to be authenticated by the other sensor nodes in the network. As we have resource constraints its important to get key agreement from sensor nodes [1].

According to Gartner et al.[5], nearly 26 billion devices will be connected through Internet of Things, which give a very high economic value. The main foundation of Internet of Things (IoT) is the wireless sensor network which is a reason for the actively pursuing technical research in it. Research is conducted on many fields for example Military, Medical, marine etc. [2]. So security always place a crucial role in the present running world.

Basically wireless sensor network can be affected in many ways physically, where the attack concentrates on affecting different layers, attacks related to privacy and authentication related attacks. Main type of attacks the wireless sensor networks do face are outsider attacks and insider attacks [11]. Outsider attacks are those attacks where an intruder comes into the network and do some malicious attack on the nodes the intruder wants to attack. Insider attacks occur where the trustable nodes does some malicious work within the network. As insider attacks occur through trustable devices, this has to be concentrated mainly because of the difficulty in finding out that trusted intruder [3].

In order to eradicate these kind of attacks localization algorithms are been used [4]. In this paper usage of these algorithms and the detailed explanation of how these algorithms play a major role to eradicate these attacks are done. An existing sensor network is with randomly scattered sensor nodes where nodes do not have a clear idea about their adjacent nodes and due to which nodes have to use their energy or power unnecessarily in order to get the adjacent node information.

An Sensor node finds the adjacent node, it senses, collects the data, and transfers the collected data through the nodes and give the data to the cluster head. An anchor node transfers various nonces to sensor nodes depending on the energy level[8]. The sensor node creates/generates a key depending on the received nonces from the nodes. Not considering the communications between cluster heads or the cluster heads and the base stations, we are going to focus only on the key management and the insider threats [6]. A variety of Outsider and Insider threats are considered. Rather than the outsider attack insider attack is more critical as it sends authorized and authenticated messages and can even drop critical packets[9].

There are many kinds of Insider attacks, where some of them are listed here like eavesdropping, modification, mis-routing and packet drops[10]. We propose a methodology where we solve some of the problems that occur through insider threats.

3 Proposed System

Our system initially deals with the network architecture where the sensor nodes are placed in a selective architecture chosen through various network topologies. As we create this network, all the nodes in the network know about their adjacent node's identity and their energy levels. Basically a group of 5 nodes are formed and each node senses and sends data to other four nodes, and if any of the nodes responds and gives first four correct acknowledgments will be chosen as cluster head.

All the sensor nodes contact their cluster heads and all the cluster heads contact a particular sink. If a sensor node wants to send data to another sensor node of another group, then the source sensor node sends the data to its cluster head and the cluster head transfers information to the sink, now the sink identifies corresponding head of destination sensor, after identifying sink sends the information to the cluster head and the cluster head contacts the particular destination sensor node.

A randomly dispersed sensor network is taken and a scenario of multiple source and multiple destination is assumed,now while sending information from a source to destination the network chooses

an optimal path, the data is transmitted through that path where we can see some droppers in between because nodes cannot link with each other as the distance between them is more and storage can also be a reason for any packet loss. So we move to our proposed work where the randomly distributed nodes are grouped together based on their location and a trustable node is selected among them. If a node wants to send information within the group to multiple destinations then a forward node which is chosen based on trustworthiness and the information is transferred through this node to the destination nodes, where this forward node saves time and drops no packets as these nodes are within the location. This follows

- Spatial priority and
- Partial Buffer sharing

Partial buffer sharing comes when the network fails. So if the network fails, we allot some backup sensors which take responsibility if the other nodes in the network do not work. These backup sensors choose the trustable nodes in between this network and transfers the data to the destination. In that sense if we are using backup nodes we are following a path where we chose a very selective trustable nodes and sending the information through the forward nodes. As we observe this we can understand that we need not use this localization concept for our networks but we can even manage the network when it is randomly dispersed. The thing to be done for the randomly distributed network is that we have to choose trustable nodes and some forward nodes in order to send data without any data loss.

The above architecture diagram represents our proposed system. After identifying the real time sensors location and the network topology we firstly deploy the network in a simulation tool for example ns2. After network deployment localizability testing is done so that sensor nodes can form a group and chose their cluster head. Structure analysis after localizability testing is done in order to analyze the structure of the formed network with group of nodes with cluster heads. After this analysis if the network needs to undergo any changes, then the changes are to be done accordingly. This is known as distinctive analysis. Finally the Network has to

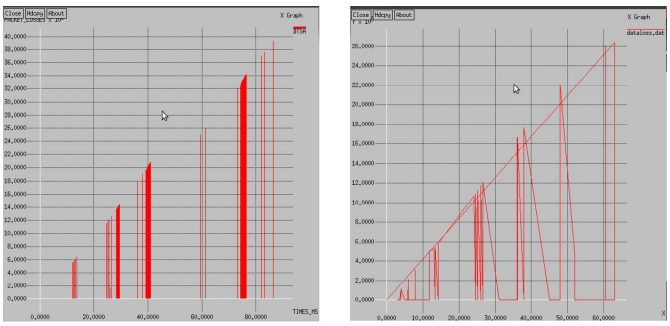

Figure 2: (a) Packet loss of Existing system and (b) Proposed system

undergo localization. Whereas our traditional localization do not follow the above steps but only undergoes indistinctive adjustment before the step of localization. Here we are choosing mesh topology for our network construction. This topology resolves collision attacks.

4 Results and Future Work

For our implementation purpose we chose ns2 simulator for implementing existing system as well as our proposed system. We deployed both the networks in the simulator and on the comparison of both the deployed networks we got 2 packet loss graphs comparing the existing and the proposed system.

In Figure 2:(a), the graph represents the packet loss of the randomly distributed nodes when they pass information to a particular destination. X axis in the graph represents the time and Y axis represents the number of packets. So as we observe that the packet loss exists for a period of time as the distance from the nodes is more and insufficient storage can also be a reason for the packet loss.

As we observe that in Figure 2:(b), the packet loss is much less compared to the previous existing system. Even though the loss is there, it is very much less compared to the above loss. This is because we have followed localization concept where the network

follows grouping of nodes and a forward node is chosen to send the data to destination. A forward node is chosen because the distance between the source and destination is high and forward node helps to save time in case of multiple destinations. Even if the network fails we are with some backup sensors which help in passing the information to the right destination. The issue is not only regarding the packet loss but also the throughput, delay in transmission, number of drop nodes, channel, protocol efficiency, source frequency, DES frequency. Overall we can show the efficiency of our proposed work in the above graphs. Graphs are generated by creating our network and the existing network in a simulator called ns2. Ns2 gives us a platform to represent our network and find the issues with it.

5 Conclusion

Minimization in localization error has been carried out by finding the optimum signal strength (range) of anchor nodes. The RSS information between sensor nodes and its neighbor anchor nodes is used to estimate the positions without any complicated hardware. First of all, the edge weight of each anchor node which is adjacent and within the range the sensor node, is applied to estimate the sensor node position, then the edge weights are calculated and the localization of node is carried out by weighted centroid theorem.

References

[1] Wenliang Du, Jing Deng, Y.S. Han, *A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge*, INFOCOM, Proceedings IEEE INFOCOM, The 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, Hong Kong, China,(2004).

[2] L. D. Xu, W. He, and S. Li, *Internet of things in industries: A survey*,IEEE Transaction Industrial Informatics, vol. 10, no. 4, pp. 2233-2243 (2014).

[3] L. Sujihelen , C. Jayakumar , C. Senthil Singh, *Detecting Node Replication Attacks in Wireless Sensor Networks: Survey*, Indian Journal of Science and Technology, vol.18, issue 16, (2015).

[4] Chun-I Fan, Shi-Yuan Huang and Yih-Loong Lai, *Privacy-Enhanced Data Aggregation Scheme Against Internal Attackers in Smart Grid*, IEEE Trans. Industrial Informatics, vol. 10, no. 1, pp. 666-675 (2014).

[5] Laurent Eschenauer and Virgil D. Gligor, *A key-management scheme for distributed sensor networks*, Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA, pp. 41-47 (2002).

[6] Farooq Anjum, *Location dependent key management in sensor networks without using deployment knowledge*, Wireless Networks, vol. 16, no. 6, pp. 1587-1600, (2010).

[7] Wu Yafeng, Stankovic John A, He Tian and Lin Shan, *Realistic and efficient multichannel communications in wireless sensor networks*, In proceedings of INFOCOM 2008-The 27th Conference on Computer Communications, IEEE, 1867-1875, (2008).

[8] Kwon Taekyoung, Lee JongHyup and Song JooSeok, *Location-based pairwise key predistribution for wireless sensor networks*, IEEE transactions on wireless communications, vol. 8, no. 11, pp. 5436-5442, (2009).

[9] Ding Wei, Yu Yingbing and Yenduri Sumanth, *Distributed first stage detection for node capture*, in Proceedings-GLOBECOM Workshops IEEE, pp. 1566-1570, (2010).

[10] Choi Jaewoo, Bang Jihyun, Kim LeeHyung and Ahn Mirim and Kwon Taekyoung, *Location-based key management strong against insider threats in wireless sensor networks*, IEEE Systems Journal, vol. 11, no.2, pp. 494–502, (2017).