International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Clone Attack Detection in MWSN Using Neighbor Node Information

Ashe Kiran[1], Deepinder Dhaliwal[2]

Research Scholar, DBU, Mandi Gobindgarh, Pb., India

Assistant Professor, DBU, Mandi Gobindgarh, Pb., India

Abstract: ***Various types of attacks occurred in WSN network. Attack occur in WSN is clone attack which is also known as replica attack. In this attack the node copy the id of the other node and show its predictions at different locations. A clone node can create a black hole or wormhole attack include adversary can use them in different ways. This attack can transmit false information to all legitimate nodes. The clone attack is very suitable for adversary. For this attack adversary has not to be compromise for number of nodes. The adversary can do cloning of one node and can predict other nodes through this node. It falsifies its positions at different times at different locations. Main problem in this is to detect the node having clone attack, because each and every node has same id and locations at different position on same interval of time. This problem has also been arising in clusters in which clusters replicate and the main problem arises when cluster head replicate.***

Keywords: WSN, MWSN, Replication Attack, Leach, Clustering

1. Introduction

1.1 MWSN

Mobile wireless sensor networks (MWSNs) can be defined as a wireless sensor network (WSN) in which sensor nodes are mobile. MWSNs are an emerging field of research in contrast to their well-established predecessor. MWSNs are much more versatile than static sensor networks as they can be deployed in any scenario and cope with rapid topology changes. The advantages of mobile wireless sensor network over static wireless sensor networks include better energy efficiency, improved coverage, enhanced target tracking, and superior channel capacity. Commonly, the sensor nodes consist of a radio transceiver and a microcontroller powered by a battery, as well as some kinds of sensor for detecting light, heat, humidity, temperature, etc. Meanwhile, other mobile devices, like mobile phones, tablet, and laptop computers, can nowadays be seen as general-purpose mobile computing and sensing platforms.

1.2 Clustering

Clustering is the task of grouping a set of objects in such a way that objects in the same group (called a cluster) are more similar (in some sense or another) to each other than to those in other groups (clusters). It is a main task of exploratory data mining, and a common technique for statistical data analysis, used in many fields, including machine learning, pattern recognition, image analysis, information retrieval, and bioinformatics. Cluster analysis itself is not one specific algorithm, but the general task to be solved. It can be achieved by various algorithms that differ significantly in their notion of what constitutes a cluster and how to efficiently find them. Popular notions of clusters include groups with small distances among the cluster members, dense areas of the data space, intervals or particular statistical distributions. Clustering can therefore be formulated as a multi-objective optimization problem.

1.3 Advantages of Adding Mobility

Sensor network deployments are often determined by the application. Nodes can be placed in a grid, randomly, surrounding an object of interest, or in countless other arrangements. In many situations, an optimal deployment is unknown until the sensor nodes start collecting and processing data. For deployments in remote or wide areas, rearranging node positions is generally infeasible. However, when nodes are mobile, redeployment is possible. In fact, it has been shown that the integration of mobile entities into WSNs improves coverage, and hence, utility of the sensor network deployment. This enables more versatile sensing applications as well. When network sinks are stationary, nodes closer to the base station will die sooner, because they must forward more data messages than those nodes further away. By using mobile base stations, this problem is eliminated, and the lifetime of the network is extended. A MWSN that monitors wildfires as the fire spreads; the mobile sensors can track it, as well as stay out of its way. Mobility also enables greater channel capacity and maintains data integrity.

2. Approaches Used

LEACH protocol: Low Energy Adaptive Clustering Hierarchy ("LEACH") is a TDMA-based MAC protocol which is integrated with clustering and a simple routing protocol in wireless sensor networks (WSNs). The goal of LEACH is to lower the energy consumption required to create and maintain clusters in order to improve the life time of a wireless sensor network. LEACH is a hierarchical protocol in which most nodes transmit to cluster heads, and the cluster heads aggregate and compress the data and forward it to the base station (sink). The cluster head then creates a schedule for each node in its cluster to transmit its data. All nodes that are not cluster heads only communicate with the cluster head in a TDMA fashion, according to the schedule created by the cluster head. They do so using the minimum energy needed to reach the cluster head, and only need to keep their radios on during their time slot. LEACH

also uses CDMA so that each cluster uses a different set of CDMA codes, to minimize interference between clusters. LEACH is based on a hierarchical clustering structure model and energy efficient cluster-based routing protocols for sensor networks. In this routing protocol, nodes self-organize themselves into several local clusters, each of which has one node serving as the cluster-head. In order to prolong the overall lifetime of the sensor networks, LEACH changes cluster heads periodically. LEACH has two main steps: the set-up phase and the steady-state phase.

In the set-up phase, there are two parts, the cluster-head electing part and the cluster constructing part. After the cluster-heads have been decided on, sensor nodes (which are chosen as cluster-heads) broadcast an advertisement message that includes their node ID as the cluster-head ID to inform non-cluster sensor nodes that the chosen sensor nodes are new cluster-heads in the sensor networks.

They use the carrier-sense multiple access (CSMA) medium access control (MAC) protocol to transmit this information. The non-cluster sensor nodes that receive it choose the most suitable cluster-head according to the signal strength of the advertisement message, and send a join request message to register on the chosen cluster-head. After receiving the join message, the cluster-heads make a time division multiple-access (TDMA) schedule for data exchange with non-cluster sensor nodes. Then, the cluster head informs the sensor nodes of its own cluster and the sensor nodes then start sending their data to the base station via their cluster-head during the steady-state phase. However, the balance of energy consumption between all nodes in this manner does not ensure that the sensing coverage is preserved sufficiently.

3. Related Work

M. Conti, R.DiPietrob, A. Spognard et al [1] "Clone wars: Distributed detection of clone attacks in mobile WSNs" Among security challenges raised by mobile Wireless Sensor Networks, clone attack is particularly dreadful since it makes an adversary able to subvert the behavior of a network just leveraging a few replicas of some previously compromised sensors. In this work, we provide several contributions: first, we introduce two novel realistic adversary models, the *vanishing* and the *persistent* adversary, characterized by different compromising capability. We then propose two distributed, efficient, and cooperative protocols to detect replicas: History Information- exchange Protocol (HIP) and its optimized version (HOP). Both HIP and HOP leverage just local (*one-hop*) communications and node mobility, and differ for the amount of computation required.

Muhammad Arshad1 et al [2] "Efficient Cluster Head Selection Scheme in Mobile Data Collector Based Routing Protocol" describes Mobile Wireless Sensor Network (MWSN) is one of the rising and emerging technologies for various application of NWGN. The enormous concerns of these networks are energy efficiency and data aggregation within the network. The aim of data aggregation is that eliminates redundant data transmission and enhances the lifetime of energy in MWSN. In this paper, Author propose, analyze and validate efficient cluster head selection scheme in Mobile Data Collector based routing protocol for data aggregation, which is based on multi-hop routing strategy. Moreover, our approach is better than traditional LEACH in terms of energy consumption of sensor nodes and enhances the network lifetime due to less energy consumption during data transmission.

Akyildiz, I.F et al [3] "A survey on sensor networks" describes advancement in wireless communications and electronics has enabled the development of low-cost sensor networks. The sensor networks can be used for various application areas (e.g., health, military, home). For different application areas, there are different technical issues that researchers are currently resolving. The current state of the art of sensor networks is captured in this article, where solutions are discussed under their related protocol stack layer sections. This article also points out the open research issues and intends to spark new interests and developments in this field.

Arshad, M et al [4] "Routing strategies in hierarchical cluster based mobile wireless sensor networks" Ubiquitous communication networks is a keystone for New Generation Network (NWGN). Mobile Wireless Communication Networks (MWSN) is a viable solution to accomplish the requirements of NWGN. Due to mobility of sensor nodes, the data reliability and end-to-end delay with energy efficiency in the network is an enormous concern. Various real-time and delay sensitive applications enforced to use both environments mobile and fixed sensor nodes, whereas the others claims an entire mobile sensors environments in network. Packet loss ratio and end-to-end delay happened because of the nodes mobility which is directly impact to degrade the quality of service, network lifetime and energy consumption. This paper enlightens a comprehensive comparison between single and multi hop inter-clusterrouting strategy from cluster head to base station. Moreover, the performance of multi hop routing is calculated and compared with single hop LEACH routing strategy.

Qin Wang; Hempstead et al [5] "A Realistic Power Consumption Model for Wireless Sensor Network Devices" describes realistic power consumption model of wireless communication subsystems typically used in many sensor network node devices is presented. Simple power consumption models for major components are individually identified, and the effective transmission range of a sensor node is modeled by the output power of the transmitting power amplifier, sensitivity of the receiving low noise amplifier, and RF environment. Using this basic model, conditions for minimum sensor network power consumption are derived for communication of sensor data from a source device to a destination node. Power consumption model parameters are extracted for two types of wireless sensor nodes that are widely used and commercially available. For typical hardware configurations and RF environments, it is shown that whenever single hop routing is possible it is almost always more power efficient than multi-hop routing.

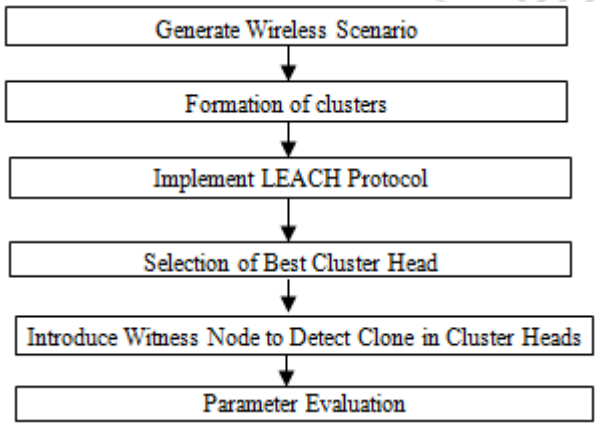
Amundson, I et al [6] "Mobile sensor localization and navigation using RF Doppler shifts" over the past decade,

wireless sensor networks have advanced in terms of hardware design, communication protocols, resource efficiency, and other aspects. Recently, there has been growing interest in mobile wireless sensor networks, and several small-profile sensing devices that are able to control their own movement have already been developed. Unfortunately, resource constraints inhibit the use of traditional navigation methods, because these typically require bulky, expensive, and sophisticated sensors, substantial memory and processor allocation, and a generous power supply.

4. Problem Formulation

In the wireless sensor networks the network nodes are used for the sensing the information from the various types of non-reachable areas. Wireless sensor nodes has been used for the sensing the information from harsh environment. In these nodes sensors of different types has been used for collecting information. Wireless sensor networks are of main two types, which are static wireless sensor nodes and mobility wireless sensor networks. In MWSNs the main threat in the network is security. Various types of attacks occurred in these networks. Attack occur in WSN is clone attack which is also known as replica attack. In this attack the node copy the id of the other node and show its predictions at different locations. A clone node can create a black hole or wormhole attack include adversary can use them in different ways. This attack can transmit false information to all legitimate nodes. The clone attack is very suitable for adversary. For this attack adversary has not to be compromise for number of nodes. The adversary can do cloning of one node and can predict other nodes through this node. It falsifies its positions at different times at different locations. Main problem in this is to detect the node having clone attack, because each and every node has same id and locations at different position on same interval of time. This problem has also been arising in clusters in which clusters replicate and the main problem arises when cluster head replicate.

5. Methodology



6. Results and Discussions

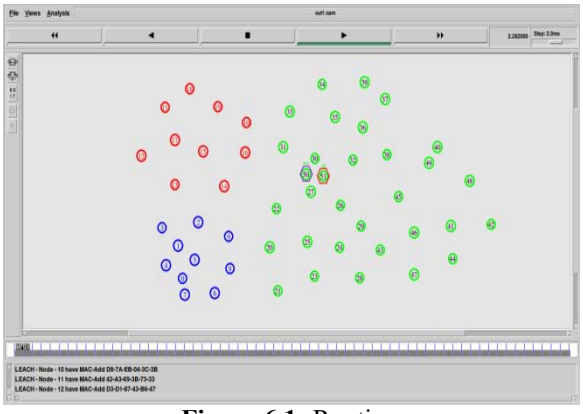


Figure 6.1: Routing

This figure is use to represent the communication between the nodes. Routing is the process of selecting best paths in a network. In the past, the term routing also meant forwarding network traffic among networks. However, that latter function is better described as forwarding.

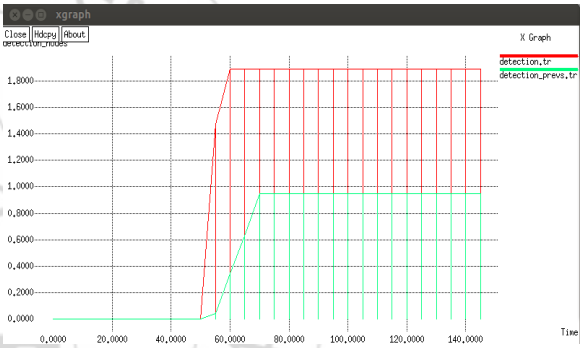


Figure 6.2: Detection of clone attack

This graph is use to represent the detection of clone attack. In this attack the node copy the id of the other node and show its predictions at different locations. A clone node can create a black hole or wormhole attack include adversary can use them in different ways. This attack can transmit false information to all legitimate nodes.

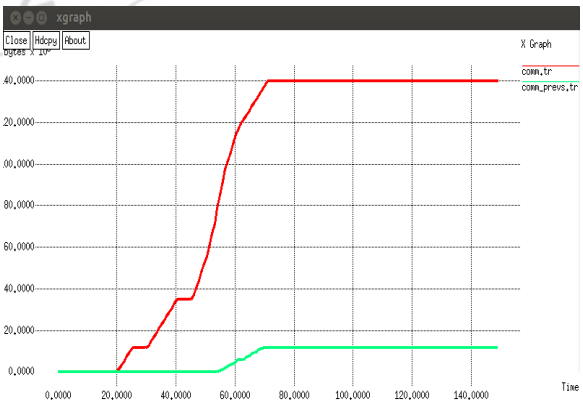


Figure 6.3: Communication between nodes

This graph is use to represent the communication between the nodes.

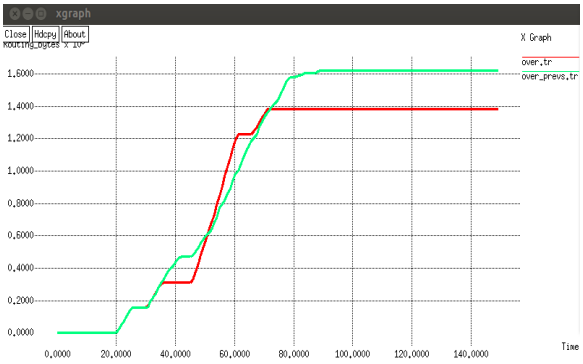


Figure 6.4: Network Overhead

This figure is use to represent the network overhead.

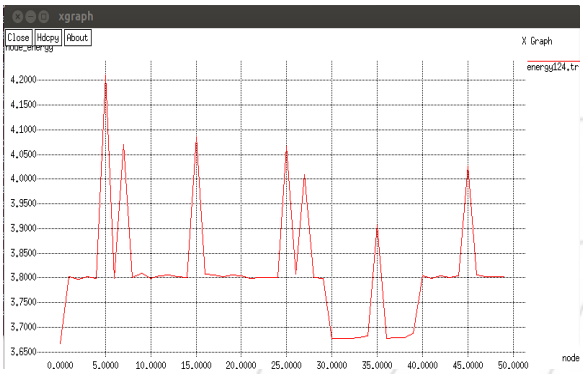


Figure 6.5: Energy

This graph is use to represent energy. Energy is a property of objects which can be transferred to other objects or converted into different forms, but cannot be created or destroyed.

7. Conclusion

Wireless sensor nodes has been used for the sensing the information from harsh environment. In these nodes sensors of different types has been used for collecting information. Attack occur in WSN is clone attack which is also known as replication attack. In this attack the node copy the id of the other node and show its predictions at different locations. A clone node can create a black hole or wormhole attack include adversary can use them in different ways. This attack can transmit false information to all legitimate nodes. Main problem in this is to detect the node having clone attack, because each and every node has same id and locations at different position on same interval of time. This problem has also been arising in clusters in which clusters replicate and the main problem arises when cluster head replicate. In this we used leach protocol for clustering. Then introduce witness node in network to check clone in cluster heads. Then compare the node entry table of cluster head with other cluster heads to check duplicity. In last we got various types of parameters & on the basis of these parameters we conclude that our system gives us better results.

References

[1] M.Conti, "Clone wars: Distributed detection of clone attacks in mobile WSNs", Journal of Computer and System Sciences, 2013.
[2] Muhammad Arshad1"Efficient Cluster Head Selection Scheme in Mobile Data Collector Based Routing Protocol", ISSN 978-1-4577-1967-7, IEEE, 2011.
[3] Akyildiz, I.F "A survey on sensor networks", ISSN 0163-6804, pp 102 – 114, IEEE, 2002.
[4] Arshad, M. "Routing strategies in hierarchical cluster based mobile wireless sensor networks," International Conference on Electrical, Control and Computer Engineering (INECCE), 2011, vol., no., pp.65-69, 21-22 June 2011.
[5] Qin Wang; Hempstead, M.; Yang, W.; "A Realistic Power Consumption Model for Wireless Sensor Network Devices," Sensor and Ad Hoc Communications and Networks, 3rd Annual IEEE Communications Society on, vol.1, no., pp.286-295, 28-28 Sept. 2006.
[6] Amundson, I., Koutsoukos, X., Sallai, J. "Mobile sensor localization and navigation using RF doppler shifts," In: 1st ACM International Workshop on Mobile Entity Localization and Tracking in GPS-less Environments, MELT (2008)
[7] MdAzharuddin "A Distributed Fault-tolerant Clustering Algorithm for Wireless Sensor Networks", ISSN 978-1-4673-6217-7, IEEE, 2013.
[8] Xuhui Chen, "Research on hierarchical mobile wireless sensor network architecture with mobile sensor nodes", ISSN 978-1-4244-6495-1, pp 2863 – 2867, IEEE, 2010.
[9] Yong-Sik Choi "A study on sensor nodes attestation protocol in a Wireless Sensor Network", ISSN 978-1-4244-5427-3, pp 1738-9445, IEEE, 2010.
[10] Yuling Lei, "The Research of Coverage Problems in Wireless Sensor Network", ISSN 978-0-7695-3901-0, pp 31 – 34, IEEE, 2009.
[11] Mittal, R. "Wireless sensor networks for monitoring the environmental activities" 978-1-4244-5965-0, pp. 1 – 5, IEEE, 2010.
[12] M.Contia "Clone wars: Distributed detection of clone attacks in mobile WSNs", 4321 6754, 123-543, IEEE, 2013.