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

Detection and Avoidance of Clone Attack in WSN Using Neighbor Witness Node

Ghansham Dass[1], Rishideep Singh[2]

[1, 2]Department of Computer Science Engineering, NWIET, Dhudike, Punjab, India

Abstract: ***Wireless sensor nodes has been used for the sensing the information from harsh environment. 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. 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. In purposed work LEACH protocol will be used for clustering.***

Keywords: Wireless Sensor Network, LEACH, Clone Attack, Clustering, Replication Attack.

1. Introduction

1.1 Wireless Sensor Network

WSN networks compose possibly large number of wireless sensor nodes that are resource constrained in terms of energy, memory, computing capabilities and communication strange. A sensor node will be also referred to as just node or sensor in the sequel. There are various type of application of WSN are already present in health care, navigation, rescue, intelligent transportation, social networking, gaming application fields, and critical infrastructure protection. This network is of tenant attended and deployed in harsh environments. WSNs are hence subject to several threats because of their nature. In this, we focus on the security of the WSN. In particular, we cope with a fundamental, specific, and dreadful security attack mobile WSNs are subject to; the so-called clone attack. It consists in replicating and deploying the captured sensors to launch a variety of malicious activities. Replicating a node implies cloning the node ID and all the cryptographic material that is associated to that ID, as well as introducing further code to be executed this code supporting the adversary's goals. The code cloned by tamped red node in to a rogue replica enables this latter one to communicate with other nodes and being identified a
salegitimate one. Once cloned node sari deployed in the network, the adversary causes the min several malicious ways. For instance, a clone could create a black hole, initiate a wormhole.

1.2 Types of WSN:

1.2.1 Structured WSN: all or some of the sensor nodes are deployed in a pre-planned manner at fixed locations. The advantage of a structured WSN is that fewer devices can be deployed with lower network maintenance and management costs.

1.2.2 Unstructured WSN: contains a dense collection of sensor nodes, which are randomly placed into the field .An ad-hoc deployment is preferred over a pre-planned deployment when the network is composed of hundreds to thousands of nodes in order to cover a larger area or when the environment is not directly accessible by humans attempting to construct WSN

1.3Routing Protocols in WSN

We can reduce the energy consu7mption by using various techniques like data aggregation, clustering, data-centric methods, etc. The routing protocols can be classified as flat, hierarchical or location-based as follow:

1.3.1 Flat networks: In this network equal nodes are used. Hence each node plays the same role. This network has no logical hierarchy. It uses a flat addressing scheme. The example of flat network is Routing Information Protocol (RIP)

1.3.2 Hierarchical networks: The nodes are partitioned into a number of small groups called clusters. Each cluster has a cluster head (CH) which is the coordinator of other nodes. These CHs perform data aggregation so that energy inefficiency may be reduced. The cluster heads may change. The node which has the highest energy acts as the CH. Hierarchical routing is an efficient way to lower energy consumption within a cluster. It has major advantages of scalability, energy efficiency, efficient bandwidth utilization, reduces channel contention and packet collisions. Low Power Adaptive Clustering Hierarchy (LEACH), Hybrid, Energy-Efficient Distributed Clustering (HEED), etc. are examples of hierarchical networks [20].

1.3.3 Location-based networks: In location-based clustering, the location of the sensor nodes plays a important role. Base station is used to send data to a particular location. In these protocols, the awareness of position of the sensor nodes is very significant to transfer the data to destinations. The distance between neighboring nodes can be estimated on the basis of incoming signal strengths. On the basis of location based protocol, if there is no activity then

nodes should go to sleep to save energy. Location-Aided Routing (LAR) and the example of location based protocol Distance Routing Effect Algorithm for Mobility (DREAM).

1.4 Clustering Parameters

1.4.1 Number of clusters (cluster count): In most recent probabilistic and randomized clustering algorithms the CH election and formation process lead naturally to variable number of clusters. The set of CHs are predetermined and thus the number of clusters is preset. The number of clusters is usually a critical parameter with regard to the efficiency of the total routing protocol.

1.4.2 Intra-cluster communication: In some initial clustering approaches the communication between a sensor and its designated CH is assumed to be direct (one-hop communication). However, multi-hop intra-cluster communication is often required, i.e., when the communication range of the sensor nodes is limited or the number of sensor nodes is very large and the number of CHs is bounded.

1.4.3 Nodes and CH mobility: If we assume stationary sensor nodes and stationary CHs, we are normally led to stable clusters with facilitated intra-cluster and inter-cluster network management. On the contrary, if the CHs or the nodes themselves are assumed to be mobile, the cluster membership for each node should dynamically change; forcing clusters to evolve over time and probably need to be continuously maintained.

1.4.4 Nodes types and roles: In heterogeneous environments, the CHs are assumed to be equipped with significantly more computation and communication resources than others. In homogeneous environments, all nodes have the same capabilities and just a subset of the deployed sensors is designated as CHs.

1.4.5 Cluster formation methodology: In most recent approaches, when CHs are just regular sensors nodes and time efficiency is a primary design criterion, clustering is being performed in a distributed manner without coordination. In few earlier approaches a centralized (or hybrid) approach is followed; one or more coordinator nodes are used to partition the whole network off-line and control the cluster membership.

1.4.6 Cluster-head selection: The leader nodes of the clusters (CHs) in some proposed algorithms (mainly for heterogeneous environments) can be pre-assigned. In most cases however (i.e., in homogeneous environments), the CHs are picked from the deployed set of nodes either in a probabilistic or completely random way or based on other more specific criteria (residual energy, connectivity etc.).

1.4.7 Algorithm complexity: In most recent algorithms the fast termination of the executed protocol is one of the primary design goals. Thus, the time complexity or convergence rate of most cluster formation procedures proposed nowadays is constant (or just dependent on the number of CHs or the number of hops). In some earlier protocols, however, the complexity time has been allowed to depend on the total number of sensors in the network.

1.4.8 Multiple levels: In several published approaches the concept of a multi-level cluster hierarchy is introduced to achieve even better energy distribution and total energy consumption (instead of using only one cluster level). The improvements offered by multi-level clustering are to be further studied, especially when we have very large networks and inter-CH communication efficiency is of high importance.

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). Each node uses a stochastic algorithm at each round to determine whether it will become a cluster head in this round. LEACH assumes that each node has a radio powerful enough to directly reach the base station or the nearest cluster head, but that using this radio at full power all the time would waste energy. Nodes that have been cluster heads cannot become cluster heads again for P rounds, where P is the desired percentage of cluster heads. Thereafter, each node has a 1/P probability of becoming a cluster head in each round. At the end of each round, each node that is not a cluster head selects the closest cluster head and joins that cluster. The cluster head then creates a schedule for each node in its cluster to transmit its data.

3. Related Survey

Muhammad Arshad1 et al [1] "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 [2] "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 [3] "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-cluster routing strategy from cluster head to base station. Moreover, the performance of multi hop routing is calculated and compared with single hop LEACH routing strategy. The simulation results reveal that multi hop routing strategy is to increase the sensor nodes throughput and network lifetime but not efficient approach for delay sensitive and data reliable applications.

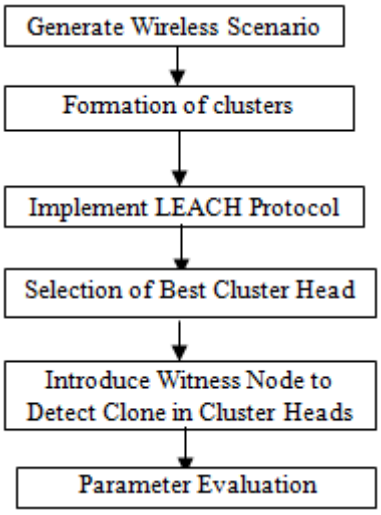
Qin Wang; Hempstead et al [4] "A Realistic Power Consumption Model for Wireless Sensor Network Devices" describes realistic power consumption model of wireless communication subsystems typically used in many sensor network node devices is presented. Simple power consumption models for major components 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 [5] "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. Therefore, alternative navigation techniques are required. In this paper Author present Trip Nav, a localization and navigation system that is implemented entirely on resource-constrained wireless sensor nodes.

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 t5he 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

Sharing of tables is use for the detection of nodes from the replication.

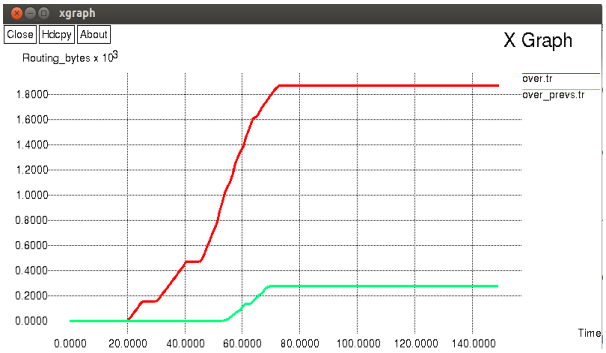


Figure 6.5: Overloading

This graph is use to represent the overloading of message.

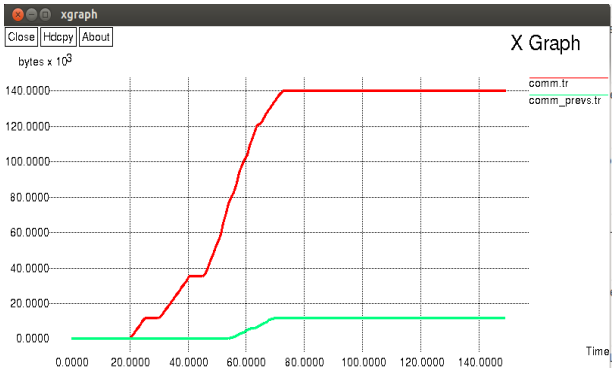


Figure 6.6: Communication

This graph is use to represent the transfer of messages between the nodes, which is called communication between the nodes

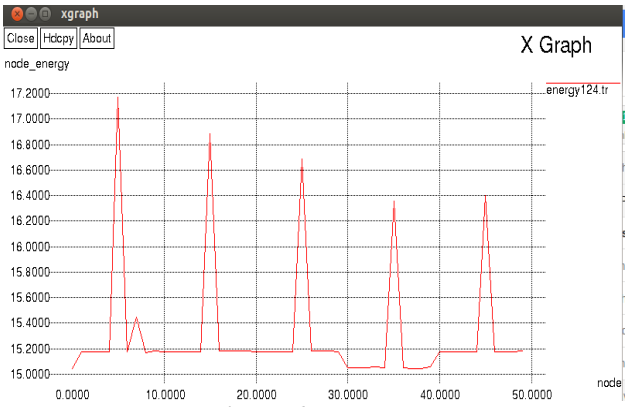


Figure 6.7: Energy

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

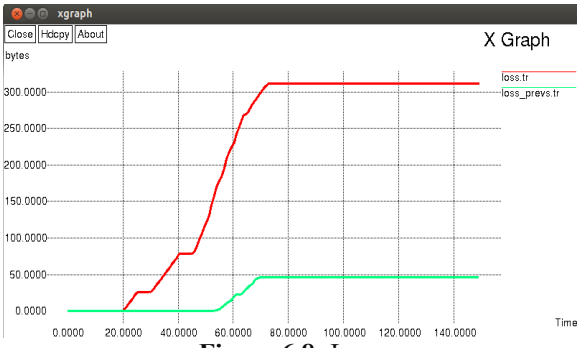


Figure 6.8: Loss

This graph is use to represent the packet loss in the network.

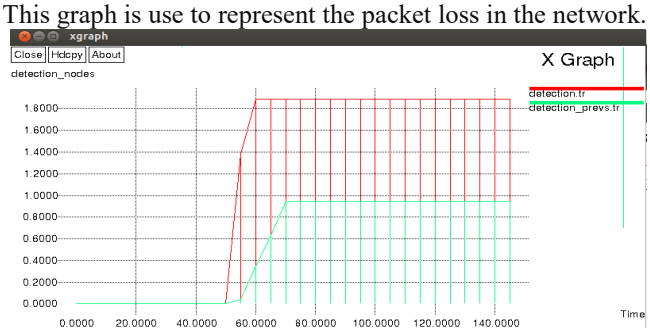


Figure 6.9: Detection

This graph is use to represent the detection of nodes from replication.

7. Conclusion

WSN networks compose possibly large number of wireless sensor nodes that are resource constrained in terms of energy, memory, computing capabilities and communication strange. A sensor node will be also referred to as just node or sensor in the sequel. Wireless sensor networks are of main two types, which are static wireless sensor nodes and mobility wireless sensor 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. 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. We got various types of parameters & on the basis of these parameters we concluded that our system gives us better results.

References

[1] Muhammad Arshad1 “Efficient Cluster Head Selection Scheme in Mobile Data Collector Based Routing Protocol”, ISSN 978-1-4577-1967-7, IEEE, 2011.
[2] Akyildiz, I.F “A survey on sensor networks”, ISSN 0163-6804, pp 102 – 114, IEEE, 2002.
[3] 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.

[4] 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.

[5] 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)

[6] Md Azharuddin "A Distributed Fault-tolerant Clustering Algorithm for Wireless Sensor Networks", ISSN 978-1-4673-6217-7, IEEE, 2013.

[7] 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.

[8] 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.

[9] Yuling Lei, "The Research of Coverage Problems in Wireless Sensor Network", ISSN 978-0-7695-3901-0, pp 31 – 34, IEEE, 2009.

[10] Mittal, R. "Wireless sensor networks for monitoring the environmental activities" 978-1-4244-5965-0, pp. 1 – 5, IEEE, 2010.

[11] M.Contia "Clone wars: Distributed detection of clone attacks in mobile WSNs", 4321 6754, 123-543, IEEE, 2013.

[12] Md Azharuddin "A Distributed Fault-tolerant Clustering Algorithm for Wireless Sensor Networks", 978-1-4673-6217-7, IEEE, 2013.