Detection of Clone Attack in Mobile Wireless Sensor Network

Benu
M.Tech Scholar
Department of ECE
SBSSTC, Ferozepur, Punjab

Chakshu Goyal
Assistant Professor
Department of ECE
SBSSTC, Ferozepur, Punjab

ABSTRACT
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. 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. 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. We can remove this clone attack by using witness approach algorithm. In the presented paper, four parameters are generated i.e Packet Loss, Packet Delay, Packet Delivery Ratio, Throughput and on the basis of these parameters we conclude that our system gives us better performance.

Keywords
Leach, HEED, WSN, MWSN

1. INTRODUCTION
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 [1].

This network is of tenant attended and deployed in harsh environments. WSNs are hence subject to several threats because of their nature. Basically in this paper we focus on the security of the WSN. Specifically, we adapt to a key, particular, and terrifying security attack mobile WSNs are liable to; called as clone attack. [3–5].It comprises in replicating and sending the captured sensors to dispatch a variety of malicious exercises. Copying a node means cloning the node ID and all the cryptographic material that is linked 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 sale gitimate one. Once cloned node sari deployed in the network, the adversary causes the min several malicious ways [6, 7].For instance, a clone could create a black hole, initiate a wormhole.

Both the energy management and packet loss have been the focus of discussion. For removing this problem lot of solution is designed like Low-Energy Adaptive Clustering Hierarchy (LEACH), Threshold Sensitive Energy Efficient Sensor Network (TEEN),Geographic and Energy Aware Routing (GEAR) Protocol, , Geographic Adaptive Fidelity (GAF),Hybrid Energy-Efficient Distributed Clustering (HEED), , and Simple Least-Time Energy Routing Protocol with One-Level Data Aggregation (One-LEO). All these above protocols is used to decrease or remove energy consumption and distribute traffic. If the number of nodes is increased, packets processed by each node significantly increase. There is no guarantee that nodes with large flow do not exhaust all energy or have traffic congestion due to overloading, leading to packet loss or node failure. The solution of this problem is to change the transmission path when the traffic of packet cross their limits, which trades off the transmission efficiency for the benefit of traffic dispersion. But it works only in some cases but .The WSN will fail when the traffic of all other routes exceeds loading limits in the same time. In that point, we add a new node for proper working with the existing node. In the authors were by use of dividing the single line in every node into multiple weighted sub-lines logically and forward packets in each sub-queue based on its weight, such that proposed a multi-queue-LIFO approach to improve delay and fairness in congested WSNs. By means of migration the data traffic to non-congestion region, the authors in provided a so-called on-demand node placement algorithm. Where the buffer in each node is adjusted we introduced an algorithm according to the transmitting downstream nodes in order to minimize packet drop while as to avoid packet drops due to congestion [1].

1.1 Parts of WSN
1.1.1 Sensor Node
This is a core component of WSN. This node does a multiple tasks in WSN, such as simple sensing; data storage; routing; and data processing.

1.1.2 Clusters
Clusters are the organizational unit for WSNs. The crowded nature of these systems requirement for them to be separated into clusters to make the tasks simple such as communication.

1.1.3 Cluster heads
Cluster heads are the managing the cluster head. They often are needed to managing task in the cluster. These tasks include but are not restricted to data-aggregation and organizing the communication timetable of a cluster[11].

1.1.4 Base Station
The base station is at the upper level of the hierarchical WSN. It provides the communication link between the sensor network and the end-user.

1.1.5 End User
The data in a sensor network can be used for a wide-range of

applications. Therefore, a particular application may be used for the network data over the internet, using a PDA, or even a desktop computer.

The sensors must be placed in exact locations, since there are a limited number of nodes extracting information from the environment. Furthermore, deployment of these nodes and cables is costly and awkward, requiring helicopters to transport the system and bulldozers to ensure the sensors can be placed in exact positions. There would be large economic and environmental gains if these large, bulky, expensive macro-sensor nodes could be replaced with hundreds of cheap micro-sensor nodes that can be easily deployed. This would save significant expenses in the nodes themselves and in the organization of these nodes. These micro-sensor networks would be fault-tolerant, as their sheer number of nodes can guarantee that there is sufficient redundancy in data acquisition that not all nodes need to be functional. Using wireless communication between the nodes would eliminate the need for a fixed infrastructure.

1.2 Sensor Nodes

Wireless sensor networks (WSNs) comprised of a large number of small, cheap, computational, and energy-constrained sensor nodes that are organized in network service area and since it's nature is wireless , it is easy to add more sensor nodes or move deployed/mounted nodes for better coverage and reach . In a Wireless Sensor Network, the sensor nodes perform two main functions: sensing and relaying data. The sensing component is responsible for testing their environment to track a stimuli/target. The collected (sensed) data are then relayed to the gateway(s). Nodes that are more than one jump away from the gateway send their data through sending nodes[5]. Fig 1.1 describes the architecture of a sensor node.

A typical sensor node consists of 4 main parts.

- Sensing unit
- Processing unit
- Power unit
- Transceiver unit

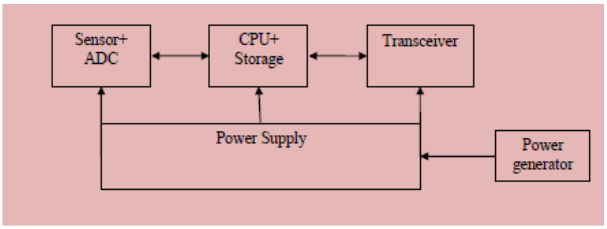


Figure 1: The architecture of a sensor node.

1.2.1 Sensing unit

The sensing unit collects the data (analog signal) and its analog to digital converter (ADC) converts the data to digital then sends it to the processing unit.

1.2.2 Processing unit

The processing unit deals with the task list and systems to collaborate with other sensor nodes. The processor can perform simple task on the received digital signal, and can store it into its memory.

1.2.3 Power unit

The power unit handles and sometimes generates the power using solar cells if available. The power supply is to power the node. The sensor circuitry can transform physical quantities into an electric signal.

1.2.4 Transceiver

The transceiver unit sends and receives the data from neighboring sensors [5].

The Sensor networks are used to sense environmental factors like temperature or pressure. These can be deployed in factories in order to monitor toxic or hazardous materials. They are also used to measure the weakness in building structures, or in vehicles and airplanes.

1.3 Types of WSN

1.3.1 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 organized with lower network maintenance and management costs.

1.3.2 Unstructured WSN

This type of WSN contains a dense collection of sensor nodes, which are randomly placed into the field .An ad-hoc organization is preferred over a pre-arranged deployment when the network is composed of number of nodes in order to cover a larger region or when the environment is not directly available by humans attempting to construct WSN, e.g. Polar Regions, disaster areas such as a nuclear accident area or deep sea.

2. PROBLEM IN EXISTING PROBLEM

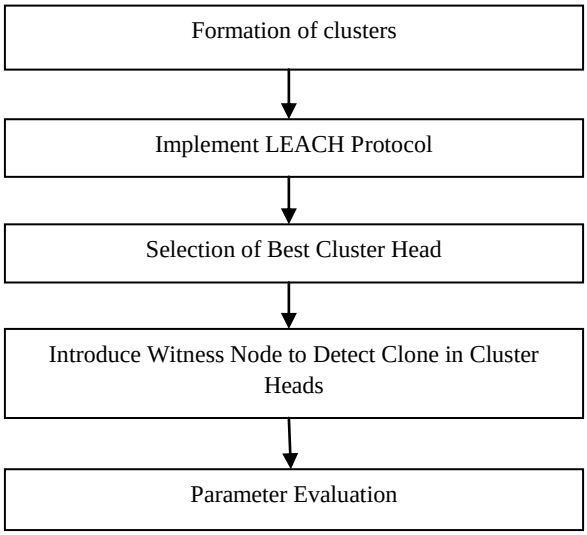
In the wireless sensor networks the network nodes are used for the sensing the information from the various types of non-reachable areas. Wireless sensor nodes has been used for the sensing the information from harsh environment. In these nodes sensors of different types has been used for collecting 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.

Main objective of this work is to design a secure system in which if cluster member replicate then it should be analyze by cluster member and if cluster head itself replicate then it should be analyze by the trustworthy authority.

3. PROPOSED WORK

The nodes sense the information and transmit it to base station. Each and every node has battery life for the sensing, computation and transmission of the data. In MWSN the nodes having mobility the nodes will get move with in

particular area. These nodes deployed have been attacked by using realistic adversary of two different vanishing and persistent adversary models. In these nodes has been used for the detection of clone attack at different nodes. By using the leach protocol clustering is done in which node with the highest energy is chosen as cluster head. Clustering approach is used to maximize the lifetime of network. If clone is present in the cluster (ie cluster member is acting as a clone) this can be detected by cluster head and if cluster head is acting as a clone then witness node will help to detect the clone.



3.1 Flow of work

4. RESULT AND DISCUSSION

In this work clone attack is shown. In clone attack one node steals the ID of another node and then this result to black hole and wormhole attack, in which node start dropping packet and if forward some messages then forward them to by doing alternations which is also called as false information broadcast.

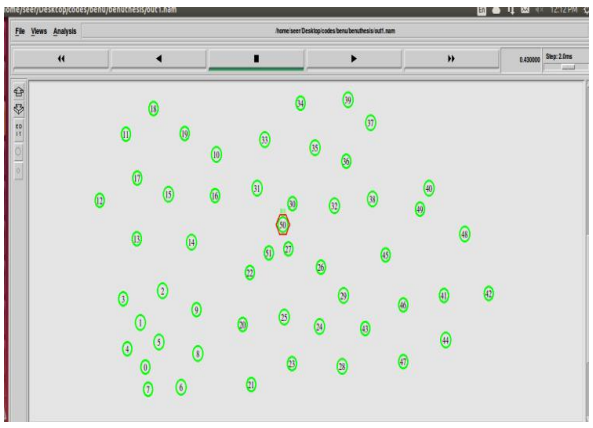


Fig 4.1 initialization of nodes

In above figure initialization of nodes are shown and number of nodes are 50. We simply allocate the location to the nodes. And node 50 is acting as a base station here.

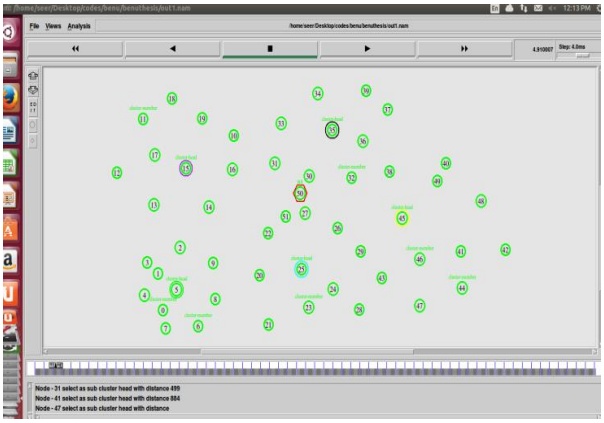


Fig 4.2 Represents cluster Head Selection

In above figure cluster head is chosen by the leach protocol with the highest energy and cluster heads are working as a data aggregator which collects the data from their cluster member and then send it to base station.

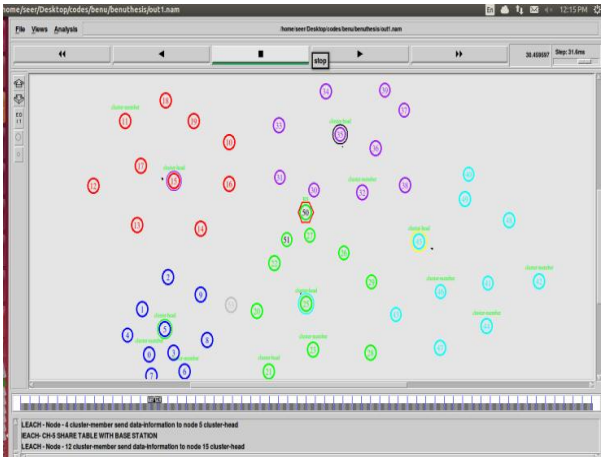


Fig 4.3 Represents cluster Formation

In this figure clusters are form and each cluster is representing with different color.

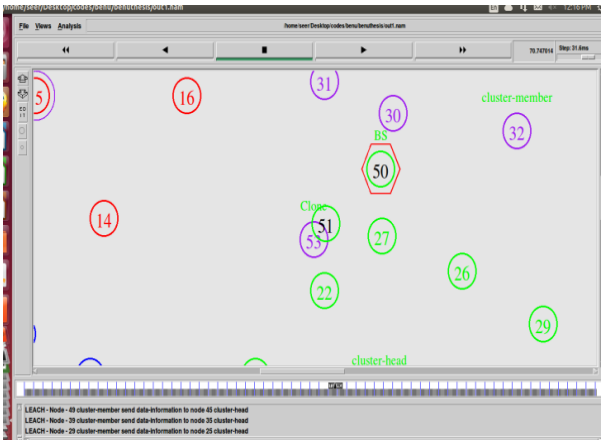


Fig 4.4 Represents Duplicate Node

In above figure node 53 is acting as a clone. Its new node adding in a network in cluster with purple color.

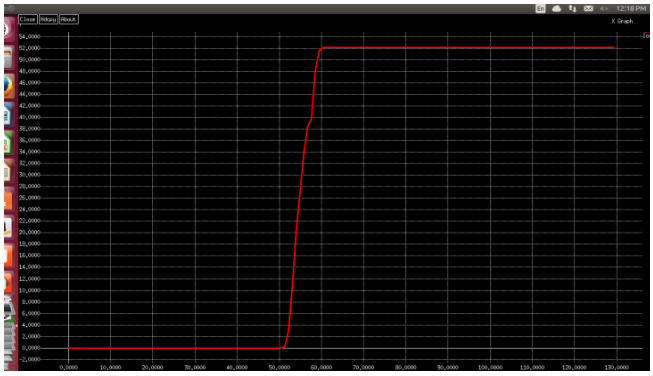


Fig 4.5 Packet Loss

This figure is use to represent the Loss of packets. Loss is defined as the number of packet loss when we transfer packets over the network

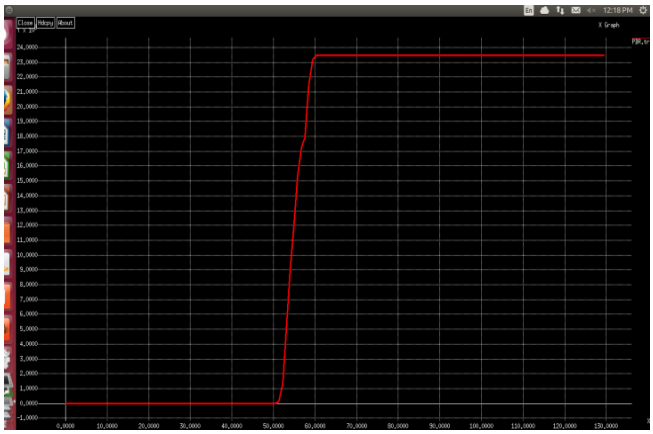


Fig 4.6 Packet Delivery Ratio

In this X-axis represent the Time and Y-axis represent the Bytes send over the network. This figure is use to represent the Packet Delivery Ratio. Packet Delivery Ratio is defined as the number of packet deliver with respect to time.

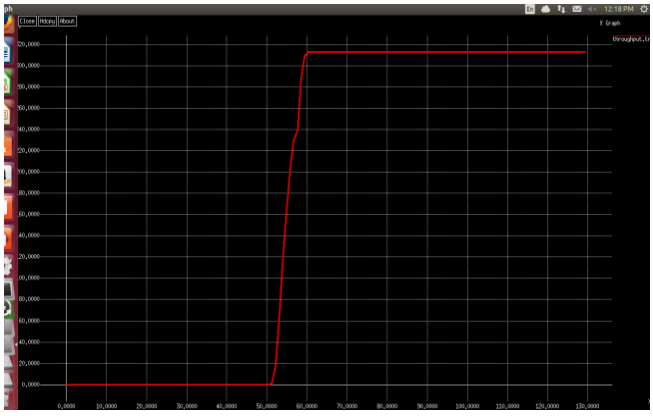


Fig 4.7 Throughput

This figure is use to represent the Throughput. Throughput is defined as the number of packet delivered successfully over the network.

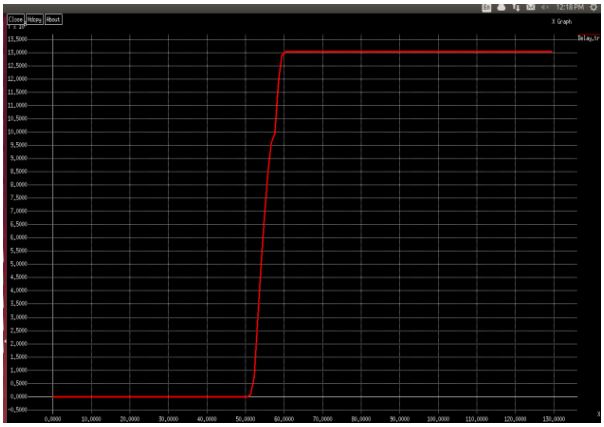


Fig 4.8 Packet Delay

This figure is use to represent the Packet Delay. Packet Delay is defined as the Delay between packets during transmission.

5. 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. 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. 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. We remove this clone attack by using witness approach. We generate four parameters i.e Packet Loss, Packet Delay, Packet Delivery Ratio, Throughput and on the basis of these parameters we conclude that our system gives us better performance.

6. REFERENCES

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

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

[3] Xuhui Chen “Research on hierarchical mobile wireless sensor network architecture with mobile sensor nodes”, 978-1-4244-6495-1, pp. 2863 – 2867, IEEE, 2010.

[4] Yong-Sik Choi “A study on sensor nodes attestation protocol in a Wireless Sensor Network”, 978-1-4244-5427-3, 1738-9445, IEEE, 2010.

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

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

[7] Marriwala, N.; Rathee, P. "An approach to increase the wireless sensor network lifetime" 978-1-4673-4806-5, 495 – 499, IEEE, 2012.

[8] GuanglaiChen "Notice of Retraction the design of wireless wave height sensor network node based on Zigbee technology", 978-1-4244-8036-4, 3683 – 3686, IEEE, 2011.

[9] Sivasankar, P.T.; Ramakrishnan, M. "Active key management scheme to avoid clone attack in wireless sensor network"

[10] U. Ahmed and F.B. Hussain, "Energy efficient routing protocol for zone based mobile sensor networks", in proceedings of the 7th international Wireless Communications and Mobile Computing conference (IWCMC), pp. 1081-1086.

[11] Y. Han and Z. Lin. "A geographically opportunistic routing protocol used in mobile wireless sensor networks", in proceedings of the 9th IEEE international conference on Networking, Sensing and Control (ICNSC), pp. 216-221.

[12] A. Aronsky and A. Segall. "A multipath routing algorithm for mobile Wireless Sensor Networks", in proceedings of the 3rd Joint IFIP Wireless and Mobile Networking Conference. pp. 1-6.

[13] Yonatan Aumann, Yehuda Lindell" Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries" e 4th Theory of Cryptography Conference (TCC), 2007,pp 1-57

[14] Pekka Nikander Andrei Gurtov Thomas R. Henderson," Host Identity Protocol (HIP): Connectivity, Mobility, Multi-homing, Security, and Privacy over IPv4 and IPv6 Networks" Communications Surveys & Tutorials, IEEE (Volume:12 , Issue: 2), pp 186 – 204

[15] Priyanka Dubey, Shilpi Sharma, Aabha Sachdev " Review of First Hop Redundancy Protocol and Their Functionalities", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 5- May 2013,pp 1085-1088.