Improved Security and Avoid Clone Attack in Wireless Sensor Network

Kulwinder Singh[1], Sheenam Malhotra[2]

[1]Department of Computer Science and Engineering, SGGSWU, Fatehgarh Sahib

[2]Assistant Professor, Department of Computer Science and Engineering, SGGSWU, Fatehgarh Sahib

Abstract: ***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.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: Clustering, WSN, Leach protocol, Cluster heads

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. [1]A wireless sensor network (WSN) consists of a number of sensor nodes (few tens to thousands) with the capability of storing, processing and relaying the sensed data, and often has a base station called Sink for further computation. It has very broad application prospects and great potential value in many areas, such as in the military and national defense, environmental monitoring, and biomedical, smart homes, remote monitoring dangerous areas, and so no.[2] WSN, more focus has been given on key management and multi-path routing protocols. The key management can be divided into centralized and pre-allocation approach. The former refers to centralized key distribution, in which the base station and each node share a pair of keys. 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, [3] A primary design goal for wireless sensor networks is to use the energy efficiently. 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 legitimate 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.

1.1Routing Protocols in WSN

We can reduce the energy consumption 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:

1.1.1 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).

1.1.2 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].

1.1.3 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 neighbouring 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).[10]In clustering whole sensor network is partitioned into group of sensor nodes called as cluster with high energy node inside the cluster acting as the cluster head. There are two approaches used in this process, the leader first and the cluster first approach. In the leader first approach the cluster head is selected first and then cluster is formed. In the cluster first approach the cluster is formed first and then the cluster head is selected.

1.2 LEACH Protocol

[4]Construction of Low Energy Adaptive Clustering Hierarchy (or LEACH) is the initial significant developments to conventional clustering approaches in WSN. 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.[9]LEACH uses a time division multiple access (TDMA) principle to avoid collisions, and in order to maintain a balanced energy consumption, suggests that each node probabilistically become a cluster head. The cluster heads are selected without considering the residual energy or the other properties of the sensor nodes.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. Figure 1.2 illustrate the cluster formation of leach protocol in two phases.

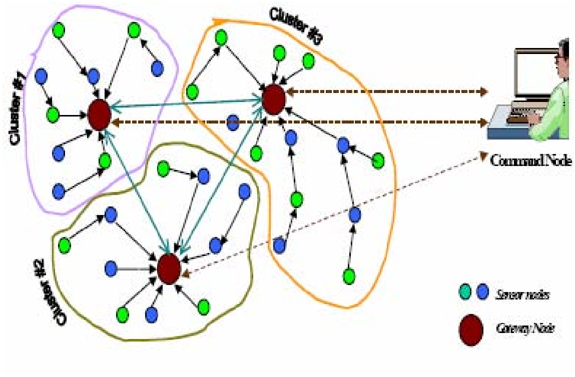

Figure 1.2: Leach protocol

1) **Setup Phase:** [10] The setup phase consists of cluster formation and cluster head selection.
   a) **Cluster formation:** Once the sensor nodes are deployed on the flat surface, the whole area is divided to form rectangular grid like structure called sectors. Sensor nodes are deployed in such a way that every sector will have sufficient number of high energy nodes. Each sector forms cluster of sensor nodes.
   b) **Cluster head selection:** Base station will communicate with all the sensor nodes, determines location and battery life of each sensor node. Base station will select sensor nodes with high energy levels as cluster heads and cluster of cluster heads will be formed within the same cluster. Cluster head with highest energy among the other cluster heads will be chosen as master. At a given time there will only one master within the cluster.
2) **Steady-state Phase:**[9]In this phase, each non-CH node uses its TDMA schedule to transmit its data to its respective CH. When a CH receives this data it uses its next relay node to forward the data to the BS. When a non-CH node finishes its data transmission slot, it enters the sleep state to save its energy.

2. Review of Literature

In 2010 **Xuhui-Chen,** et al **[1]** "Research on hierarchical mobile wireless sensor network architecture with mobile sensor nodes" In traditional wireless sensor network the nodes like the users, the sink nodes and sensor nodes are considered to be static, in the form of single layer planner the network are organized, which cannot adapt to the application of the sensor nodes with mobility. This article starts from the network architecture, introduces the architecture of traditional wireless sensor network, and takes account of the application scenario of mobile sensor nodes. Author proposed architecture of wireless sensor network with mobile sensor nodes.

In 2010 **Xiao Zhenghong,** et al **[2]** "A secure routing with intrusion detection for clustering wireless sensor networks" In this paper Author propose a social closeness based method in a mobile healthcare disease control system to detect any clone attacks that may be launched to disrupt the normal operations of the system. Our social closeness based method exploits the social relationships among users for clone attackdetection. Specifically, Author defined a new metric called community between, which considers mobile users' community information.

In 2012 **N. Marriwala,** et al **[3]** "An approach to increase the wireless sensor network lifetime" A wireless sensor network consist of small devices, called sensor nodes that are equipped with sensors to monitor the physical and environmental conditions such as pressure, temperature, humidity, motion, speed etc. The nodes in the wireless sensor network were battery powered, so one of the important issues in wireless sensor network is the inherent limited battery power within network sensor nodes.

In 2011 **Muhammad Arshad,** et al **[4]** "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.

In 2013 **MdAzharuddin,** et al **[5]** "A Distributed Fault-tolerant Clustering Algorithm for Wireless Sensor Networks" main problem of WSN is to reduce energy consumption and limited power sources of the sensor nodes. To reduce the energy consumption clustering is the main method and increase the scalability. in a cluster based WSN, cluster heads (CHs) consume more energy due to extra work load owing to data collection, data aggregation and their communication to the base station.So that efficient cluster formation is very challenging by considering the energy consumption of the CHs. This is also very difficult with the fault tolerant issue of WSNs as the sensor nodes are prone to failure.

In 2008 **ThanderThein,** et al **[6]** "Increasing Availability and Survivability of Cluster Head in WSN", Recently WSN has become one of the most interesting networking technologies since it can be deployed without communication infrastructures. The cluster-based wireless sensor network (WSN) can enhance the whole network lifetime. In the clustered environment, the data gathered by the sensors is communicated to the base station (BS) through a hierarchy of cluster-heads (CHs). Once CH is destroyed, it is no longer operational and all common nodes belonging to that cluster lose communication ability.

In 2010 **Ruchi Mittal,** et al **[7]** "Wireless sensor networks for monitoring the environmental activities" The area of sensor network has a long history and many kind of sensor devices are used in various real life applications. Here, Author introduce Wireless sensor network which when combine with other areas then plays an important role in analyzing the data of forest temperature, bioinformatics, water contamination, traffic control, telecommunication etc.Due to the advancement in the area of wireless sensor network and their ability to generate large amount of spatial/temporal data

3. Methodology

The proposed work is based on clone attack. In Clone 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.Figure 3.1 describe the flow working of proposed algorithm.

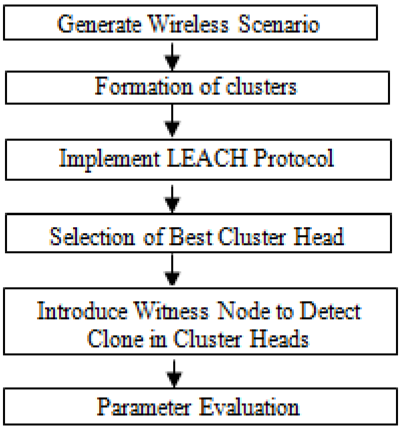
Generate Wireless Scenario
Formation of clusters
Implement LEACH Protocol
Selection of Best Cluster Head
Introduce Witness Node to Detect Clone in Cluster Heads
Parameter Evaluation

Figure 3.1: Flow diagram for proposed work

Proposed Algorithm is given below:

1. Start

2. Generate the wireless scenario so one node can communicate with other node easily.

3. Base station select cluster head from each cluster based on formulation that each start up node has same energy level.

4. Apply leach protocol using threshold equation.

$$\boldsymbol{T(n)} = \begin{cases} \dfrac{\boldsymbol{P}}{\boldsymbol{1 - P * \left(rmod\frac{1}{p}\right)}} & \boldsymbol{if\ n\ \text{€}\ G} \\ \boldsymbol{0} & \boldsymbol{Otherwise} \end{cases} \qquad Eq\ 3.1$$

If n < T (n), then that node becomes a cluster- head.Where T(n)= Threshold, P = desired % of CH , r = current round , G =set of nodes not CH in 1/p rounds. NowCalculate the distance between the cluster head and sensor node.

$$\boldsymbol{d(x,y) = \sqrt{x_2 + x_1} + \sqrt{y_2 - y_1}} \qquad Eq\ 3.2$$

Now Cluster head receives data from Non-Cluster head nodes and aggregates them. And send to the Base station.

Now energy dissipated is calculated and subtracted from the remaining energy of every node. Energy is calculated as.

$$\mathbf{E_{re} = E\text{-}(E_r\text{+}(E_t + E_{da})\text{*}distance)} \qquad Eq3.3$$

Where E_{re} = Remaining Energy,E_r= Energy Dissipated in receiving data ,E_t = Energy Dissipated in Transmission **,** E_{da} = Energy Dissipated during data collection.

5. Select the best cluster head which has maximum residual energy and minimum distance.

6. In the next step when routing is started then witness node introduce and detect the clone node in cluster head.

7. Measuring parameter: Detection of clone node, Network overhead during transmission node, Energy consumption of node, Communication between node.

8. End

4. Results and Discussion

Fig 4.4 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.

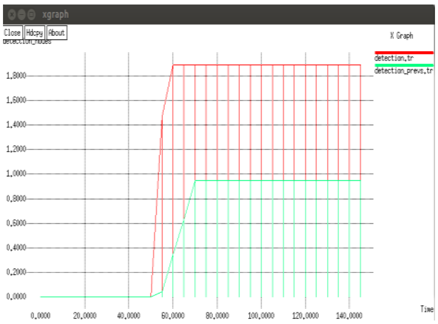

Figure 4.4: Detection of clone attack

Fig 4.5 illustrates the communication between the nodes. This graph represents that communication that has been done by transmitting the information from the sensor nodes to the base starvation in the purposed approach and previous approach that has been transmit data under clone attack to the base station.

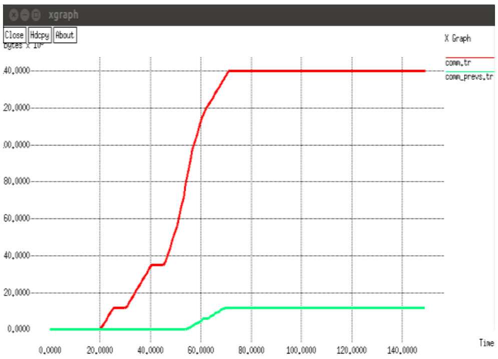

Figure 4.5: Communication between nodes

Fig 4.6 illustrates the network overhead. The overhead in a network is related to the load occurred on a single node in the network. This figure represents network overhead occurred over the network due to malicious identities available in the network. In this graph the node 0.00 can transmit the packet with network overhead with efficient energy level but node 0.30 will be loss transmission with less energy level on network head.

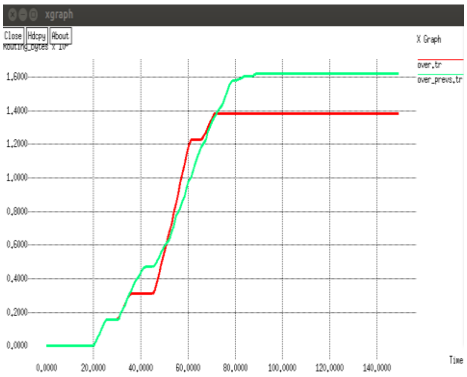

Figure 4.6: Network Overhead of a Node

Fig 4.7illustrate 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.

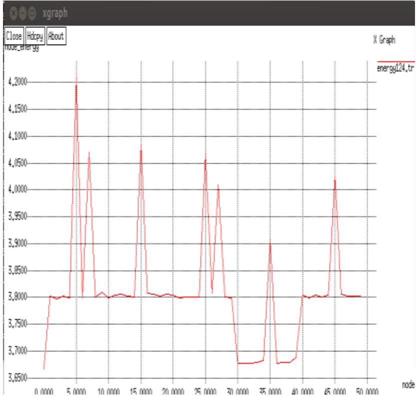

Figure 4.7: Energy consumption of a Node

Table 4.1: Comparison Table based on performance evaluation parameter

Analysed parameter	LEACH Protocol (Existing work)	Modified LEACH Protocol (Proposed work)
Detection of clone node	0.90 ms	1.90 ms
Communication b/w node	10.00 ms	40.00 ms
Network overhead	1.61 ms	1.40 ms
Energy consumption	37.00 J	38.00 J

5. Conclusion & Future Scope

The existing LEACH protocol increases the lifetime of network. Wireless sensor network mainly depend upon energy consumption, routing, fault tolerance. The existing work can increase the efficiency of node and find the shortest path. But the node is not secure during transmission because clone node copy the id of transmitted node and send it into different predict location. In proposed work, with help of modified LEACH protocol witness node is created which can introduce and detect the clone node. So the location of clone node is easily found and increases the energy level of each node during transmission. Because LEACH protocol works on additional parameter i.e Detection of clone node, Energy consumption of node, Communication between nodes, Network overhead during transmission of node.

6. Future scope

The proposed work has taken in WSN. In future any topology can be taken in RSN (Random Sensor Network). In the future reference this work can be used in real world application for data transmission and sensing in wireless sensor network. NS-2 tool for simulation but in future this work can be simulated on the simulation like QUALNET, MATLAB etc.

References

[1] Xuhui Chen, "*Research on Hierarchical Mobile Wireless Sensor Network Architecture with Mobile Sensor Nodes*", International Conference on Biomedical Engineering and Informatics (BMEI), IEEE, ISSN 978-1-4244-6498-2, Vol.56, Issue No.14, pp.: 2863 – 2867, China, 2010.

[2] Xiao Zhenghong, Chen Zhigang, "*A Secure Routing Protocol with Intrusion Detection for Clustering Wireless Sensor Network*", International Forum on Information Technology and Application (IFITA), IEEE, ISSN 978-0-7695-4115-0, Vol.8, Issue No.12, pp.:1253 – 1258, China, 2010.

[3] Marriwala, N. Rathee, P, "*An Approach to Increase the Wireless Sensor Network Lifetime*", World Congress on Information and Communication Technologies (WCICT), IEEE, ISSN 978-1-4673-4806-5, Vol.3, Issue No.6, pp.: 495 – 499, India, July, 2012.

[4] Muhammad Arshad, "*Efficient Cluster Head Selection Scheme in Mobile Data Collector Based Routing Protocol*", International Conference on Intelligent and Advanced System (ICIAS), IEEE, ISSN 978-1-4577, Vol.13, Issue No.10, pp.:1967-7, Krachi, Febuary, 2011.

[5] MdAzharuddin et al [1] "*A Distributed Fault-tolerant Clustering Algorithm for Wireless Sensor Networks*", International Conference on Advance in Computing, Communication and Informatics (ICACCI), IEEE, ISSN 978-1-4673-6217-7, Vol.4, Issue No.12, pp.:23-33, India, 2013.

[6] ThanderThein, "*Increasing Availability and Survivability of Cluster Head in WSN*", International Conference on Grid and Pervasive Computing Workshops (ICGPCW), IEEE, 2008, ISSN 978-0-7695-3177-9, Vol.45, Issue No.21, pp.: 281 – 285, Korea, 2008.

[7] Ruchi Mittal, "*Wireless Sensor Networks for Monitoring the Environmental Activities*" IEEE, ISSN 9781-4244-5967-4,Vol .5, Issue No.12, pp.:1 – 5, India, 2010.

[8] P.T Shivasankar, Ramakrishna, M. Ramakrishna "*Active Key Management Scheme to Avoid Clone Attack in Wireless Sensor Network*", International Conference on Intelligent and Advanced System (ICIAS), IEEE, Vol.7, Issue No.45, pp.:76-12, India, August, 2013.

[9] RS. Elhabyan, "*Weighted Tree Based Routing and Clustering Protocol for WSN*", Canadian Conference on Electrical and Computer Engineering (CCECE), IEEE 2013, ISSN 978-1-4799-0033-6, Vol.8, Issue No.6, pp.: 1 – 6, Canada, June, 2013.

[10] V.V Deshpande, "*Energy Efficient Clustering in Wireless Sensor Network using Cluster of Cluster Heads*", IEEE, ISSN 978-1-4673-5999, Vol.5, Issue No.12, pp.:97-105, India, September, 2013.