Secure Cluster Head Election and Effective Cluster Based Data Aggregation in WSN

Shrutika. S. V\textsuperscript{1}, Siddarth Misale\textsuperscript{2}, Supriya. A. C\textsuperscript{3}, Sushma. P\textsuperscript{4}, Sonali Joyce Lobo\textsuperscript{5}

Department of Information Science and Engineering
DSCE, Bangalore, India

Abstract:
A wireless ad hoc network having a number of resources and a network which organized itself is called as Wireless Sensor Network. In WNS data is gathered by sensor nodes and these gathered data is sent to the base station (BS). In WSN, data sending directly to the base station can raise various problems. With the data collection, network lifetime is also the major principle for design of data aggregation technique in sensor network. Most of the energy of the remote sensor network is utilized for data sending. Data aggregation is performed to avoid such problems related to energy. Clusters are utilized to perform data aggregation in present systems. We propose an energy-effective system in which data collection nodes are utilized for gathering data from cluster head inside the cluster. In this project, we propose a system that overcomes the cons to find attacked nodes as well as the cluster heads.

Keywords: Wireless Sensor Network, SCDA protocol, Cluster, Base station, Data aggregation.

1. INTRODUCTION
Progression in the field of detecting and systems administration innovations have prompted the rise of Wireless Sensor Networks (WSNs). It comprises of spatially-dispersed self-ruling sensors which is utilized to screen physical conditions, for example, temperature, vibration, movement, and so on. They have picked up prominence in different fields of life and they are being utilized in numerous applications, for example, mechanical mechanization, office and home computerization, auxiliary wellbeing observing, traffic checking, medicinal consideration, ungracious territory, automated investigation, and agribusiness observation. WSN's replaces customary wired sensor arrange with high residual energy by local radio communication. This method is a new way to create balance between the loads of the cluster heads.

2. LITERATURE SURVEY
In [1] author R. Velmani and B. Kaarthick, talk about the Wireless Sensor Networks (WSNs) assume an indispensable job in the present certifiable applications. The viability of WSNs absolutely relies upon the information gathering plan. Various information gathering plans, for example, multipath, chain, tree, group and crossover topologies are accessible in writing for gathering information in WSNs.

In [2] K. Akkaya and M. Younis, This paper surveys on routing protocols for sensor networks and classification for the various approaches pursued. The three main categories explored in this paper are data-centric, hierarchical and location-based. Each routing protocol and discussed under the appropriate category.

In [3] Q. Mamun, this paper discusses about the different performance metrics of WSN topologies. Defining a system using these performance evaluation metrics model, all topologies are compared against each other.

In [4] Cheng Zhao proposed the novel methodology for compressive data aggregation in Wireless Sensor Network by the use Tree-let based clustering method of data compression which makes it energy efficient. The proposed methodology used sparsification tool to retrieve sparsity from large amount of data for compressive sensing recovery.

In [5] M. Ye, C. Li, G. Chen, and J. Wu introduced a novel clustering method called EECS for wireless sensor networks. This clustering method is appropriate for applications which aggregate data periodically. At the time of electing better cluster head distribution this method helps in selecting cluster heads with high residual energy by local radio communication. This method is a new way to create balance between the loads of the cluster heads.
System Architecture

System diagram of the proposed SCDA protocol is shown above fig 2.1. Network is divided into clusters and cluster head is selected for each cluster. Direction of node travel is purely random in nature and is independent of other nodes within network. Entire network consists of three types of nodes – normal nodes, CH nodes and intruder nodes. Normal nodes will either be source nodes or intermediate nodes to route packets to CH. CH will collect data from its member nodes and route it to nearest next CH node towards Base Station node. Intermediate CH node will route data to next nearest CH node and finally data will be sent to Base Station. Irrespective of node type, the behavior and properties of all nodes remain same throughout the simulation. There will be one change that differentiates the features of normal nodes with respect to CH nodes is their transmission range. As CH nodes must communicate with nearest CH node, the transmission range of CH node should be higher than normal node. Hence, CH node will adjust to higher transmission range once they form CH node. Intruder nodes are the nodes which are vulnerable to the network. They are part of the network which may take various activities to interrupt the system. Intruders defined in this protocol may take following behaviors.

- Read Source Node Information
- Random Routing
- Act as Destination

Other nodes are equipped with the knowledge that if they found any intruder nodes in their neighborhood, then those nodes will be removed from their neighbor node set. Although generation of new position is random, it is also taken care that new points obtained will not be outside of specified network area. If new values obtained are out of region, then boundary values are set in such cases. Recalculation of values is avoided which will add extra cost to the algorithm.

3. PROPOSED WORK

After referring to some research papers that we went through we were able to come up with a method called as black hole. In networking, black holes refer to places in the network where incoming or outgoing traffic is silently discarded (or “dropped”), without informing the source that the data did not reach its intended recipient. Utilizing this procedure, we create a Black hole in the system where in it will confirm the ip address of both source and destination, if there is any outsider application intruding to gather the information from the cluster head, Black hole will verify the ip address, if the address isn't right the Black hole will naturally discard the information and provide the security. The proposed system provides security mechanism to avoid the drawback mentioned in the existing system. This mechanism checks whether the data is transferred to the valid base station depending on the IP address provided for authentication. The application verifies and validates the IP address and transmits the data to the valid Base Station. The cluster head has to avoid responding to the requests of the malicious node. Figure 3(a) and (b) shows the shortest path and broadcasting of data using shortest path to reduce the flooding and energy.

Data Flow Diagram

Figure 3.1 shows flow diagram of data transfer in the network. As shown above, source node will generate the data packets and will be forwarded to neighbor nodes. Neighbor node can be a normal node or intruder node or CH node. Based on the type of node, following action will be taken:

a. Normal node: This node will decrypt the queue and verify if the node address of sender node matches to decrypted value or not. If matched, then it finds next neighbor hop and forwards the packet. If no match found, then concludes that
sender is an intruder node. Thus, notifies its previous hop node that data is sent to intruder node. Therefore, remove it from neighbor list. And, forward to next neighbor node.

b. **Intruder node:** This node will try to corrupt the data packet and takes some action. It can either of the below actions - Read Source Node Information, Random Routing, Act as Destination.

c. **CH node:** This node will collect data and forwards it to nearest CH node. If BS node falls within its range, then data will be directly forwarded to BS.

4. IMPLEMENTATION

Main theme of this phase to assign the task when the outline of the working framework is the position of hypothetical and this is transformed into a working framework of the system. It can the most important and basic stage of accomplishing the fruitful new framework and giving the customers that can be viable with work and new framework of the system is to be formed. This implementation stage includes arranging the modules, examination of modules of various frameworks. And this phase also outlines the most important techniques to achieve the goal and strategies of the system.

**Project implementation and module development**

- Network Creation
- Source Data Generation
- Formation of CH
- Periodic Update
- Route Identification

**Network Creation:** Nodes are important components in WSN which are capable of transmission of packets within the network. Every node has its own set of associated properties which help in many aspects. It is a composition of software and hardware models within it. Hardware components describe various parameters description and values for each. Also, type of material used and its capability to handle different application sets. Whereas software model covers the type of transmission mechanism how the packets should be routed to different nodes within the network. Every node upon receiving data must undergo various layers defined in TCP/IP model and take appropriate action defined at each layer.

**Source Data Generation:** All source nodes are of similar nature. Generation of data within each of them will be same. Data will be generated at each source node with periodic value of time 0.2 seconds. There may be chances that CH node will be within the transmission range of source node. In that case, direct one hop transmission will be done by source node to CH node. Otherwise, will find next hop node by calling find Next Hop() method and forwards the data to it. If no next hop node is available, then packets will be dropped. Such cases may arise due to randomness the deployment of the node and will be minimal as the distribution is uniform throughout the network. Data generation at source nodes is operated by calling start and stop functions.

**Formation of CH:** Selection of CH is a major component in this protocol. Because, protocol is defined to ensure the energy spent for miscellaneous activities should be minimal. Also, energy is an important parameter of consideration for CH formation. Hence, protocol is designed with minimal energy expenses for CH selection process.

**Periodic Update:** As the entire network is mobile in nature, it is the duty of CH node to broadcast their updates to all its neighbors. During this phase, all CH sends broadcast message to share their updated location. Period of sending CH info is set to 0.5 seconds. Every member node upon receiving this message will check if they have already forwarded or not. If not, will forward to their neighbor nodes. Two hop forwarding is done to reach CH range defined in prior.

**Route Identification:** In this phase, all CH nodes will broadcast and will collect the information from each other. Once the node changes its role to behave as CH node, then its transmission range will increase from 100.0 meters to 200.00 meters. The reason for this is that, CH nodes will be far away from each other as they will be one per cluster. So, the transmission of data between the clusters occur via CH nodes will only. Means, neighbor CH nodes which are close to BS will become next hop to route data. Thus, route identification will occur once CH are found.

5. PERFORMANCE RESULTS AND DISCUSSIONS

The system observes the information at data collection node and find out valid or invalid information. When any invalid information is recognized by the system, it detects the node which contains malicious information in every cluster which is accessed by attacker as well as restricts the attacker’s information and only authenticated information is sent to the sink node.
6. CONCLUSION

In this project, aSecure Cluster Head Election And Efficient Cluster Based Data Aggregation (SCDA) in clustered WSN is studied. The approach is bring reduced energy consumption model to collect data. Cluster head nodes are selected by energy comparison with neighbor nodes in the network. CH nodes will have the responsibility of transmitting data to neighbor CH nodes. Encryption process is applied to data packet before transmission to ensure the data being transmitted is safe from intruder nodes within the network. Thus, the protocol is designed for applications where security is in demand. Further, periodic updates will be sent by CH nodes to inform member nodes about their CH role information. Member nodes collect this data and update their CH information. Source node generate the data and forwards it to CH nodes via next hop nodes. CH nodes will share their locations to neighbor CH nodes. This information is required to form route path through which it traverses and collects data from all CH. Efficiency is achieved in terms of energy and saving time of data collection. Thus, QoS parameters are achieved better using this proposed protocol. In the future, protocol is extended further to harvest energy to sensor nodes which improves the lifetime of the network. Also, variable energy is harvesting is studied to find the improvisation of the network with constant and variable harvesting energy constraints.

7. REFERENCES


