Secure Data Aggregation And Energy Conservation using a Profile Based Scheme

Anikrishnan V.A, Dr. Revathi Venkataraman
M.Tech Scholar, Department of Computer Science and Engineering, SRM University, India
Professor Department of Computer Science and Engineering, SRM University, India

Abstract— *A wireless sensor network is a spatially distributed collection of wireless sensors where each sensor is having their own memory and processing power. But these sensors are limited in processing power, energy and storage. Main purpose of using these sensors is that to monitor physical or environmental conditions, such as temperature, sound, pressure and to collectively send to a particular location. Due to limited energy resources in WSN, aggregation of data from multiple sensor nodes done at the aggregating node. Aggregating node or Cluster Head is a node collects all the information and aggregates the data. That data will be forwarded to the base station however such aggregation is known to be highly vulnerable to variety of attacks. Since WSN are usually unattended they are highly vulnerable to many types of attacks. Thus, achieving trustworthiness of data and reputation of sensor nodes is very crucial for WSN. We introduce profile based misbehavior node elimination in wireless sensor network. After selecting the cluster head, nodes will send the data to Cluster head. Cluster head will check all the node's data whether the data is caused by false information. This is a process which is done by Profile based data collection. CH will be comparing all the sensor's data with it's neighboring node. If any sensor's data show false information, that sensor is considered as malicious node and CH will eliminate that node.*

Keywords- *Data aggregation,Secure data aggregation,energy saving*

1. INTRODUCTION

A wireless sensor network is a spatially distributed collection of wireless sensors where each sensor will be having their own memory and processing power. But these sensors are constrained in processing power, energy and storage. Main purpose of using these sensors is that to monitor physical or environmental conditions, such as temperature, humidity, pressure and to collectively send to a particular location. Wireless sensor networks are used in many applications such monitoring a particular area, military purposes,, air monitoring etc

Because of variety of applications energy and security are major concerns for the sensor networks. Data aggregation [1] is a process that is used to conserve energy in an energy constrained wireless sensor network. Data aggregation reduces data traffic in the wireless sensor networks, and also reduces the amount of data that is needed to send to the base station. The main objective of various data aggregation algorithms is to gather and aggregate data from various sensor nodes in an energy efficient manner so that network lifetime is enhanced. Data aggregation is actually performed using a particular data aggregation function. This aggregated data is transmitted to the base station by selecting the most appropriate path

Data aggregation protocols mainly aims at eliminating redundant data transmission and improving the entire lifetime of energy constrained wireless sensor network. In a wireless sensor network, data transmission takes place in multi-hop fashion where each node sends its data to the nearest neighbor node to the sink node. Since closely placed nodes senses same data, above approach cannot be considered as an energy efficient one. An improvement over the above approach is clustering, where each node sends data to cluster head and then cluster head perform aggregation on the received data and then send that data to sink node or base station. Performing aggregation function over cluster-head still causes some sort of energy wastage. In some cases of homogeneous wireless sensor network, cluster head will die out quickly because of loss of energy and again re-clustering has to be done for which again needs energy consumption.

Clustering is one of the main approaches for achieving data aggregation in wireless sensor network [2]. Grouping sensor nodes into clusters is widely accepted by the research community to satisfy the objective of scalability and also to satisfy energy

efficiency and increased network lifetime in Wireless sensor network. The hierarchical routing and data gathering protocols enable cluster-based organization of the sensor nodes in order that data gathering and aggregation are possible, thus leading to some distinguishable amount of energy conservation. In the hierarchical network structure of cluster network each cluster has a head or leader, which is called the cluster head and it usually performs the above mentioned tasks (data gathering and aggregation), and several common sensor nodes as cluster members. The cluster formation process is a two-level hierarchy where the cluster head nodes will become the higher level and the cluster member nodes becomes the lower level. The sensor nodes will send their data to the corresponding cluster head nodes periodically. These cluster head nodes aggregate the data that has been send by the cluster members (thus decreasing the total number of packets sent) and eventually send them to the base station (BS) either directly to the sink node or through the intermediate communication with other CH nodes in a multihopping fashion.

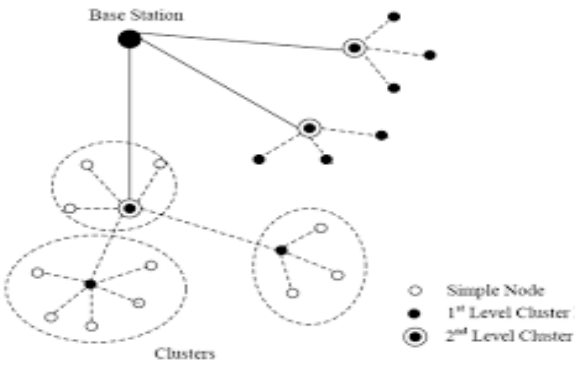

Figure: 1 clustering in WSN and transmission to base station

2. PROBLEM DEFINITION

Wireless sensor systems (WSNs) are progressively utilized as a part of various applications, like observing various environmental conditions, monitoring of earth or air. Wireless sensor networks are normally deployed in such kind of places where the sensor information can be falsely injected or can be eavesdropped. It is also possible to change the data which is being sent by the sensor nodes by hackers by using the link or by hacking the node. Sensor nodes are relatively more constrained in energy, processing power and storage as compared to other networks so we should be careful during the design of any security and routing protocol for the sensor networks, the scarcity of resource is an important factor that should be considered. Especially the energy is very constrained for the sensor networks and it is directly connected to overall lifetime of the network

Due to the scarcity of computational power and energy, data aggregation from multiple sensor nodes are done at the aggregating node is usually accomplished by simple methods such as averaging. Such aggregation is known to be highly vulnerable to many kinds of node compromising attacks. WSN is not having tamper resistant hardware for this reason they are vulnerable those different kinds of attacks. In that case, achieving trustworthiness of data and reputation of sensor nodes is very critical for WSN. On this context many kind of cryptographic systems are implemented and used for preventing attacks like flooding and jamming attacks. But it cannot prevent collusion or false data injection attacks on this context we are introducing a false data injection prevention using a profile based scheme.

3. RELATED WORK

In [3] an IF filtering mechanism is used for prevention from collusion attacks it demonstrates that several existing iterative filtering algorithms, while significantly more robust against collusion attacks than the simple averaging methods, are nevertheless vulnerable to a novel sophisticated collusion attack they introduce. In [4] the main objective is to provide a useful fully-distributed inference algorithm for clustering, based on belief propagation. The algorithm selects cluster heads, based on a unique set of global and local parameters, which finally achieves, under the energy constraints, improved network performance. Different kind of energy conservation scheme is discussed in [5]. Considering that energy saving acts as one of the hottest topics in wireless sensor networks, The main focus here is primarily on duty cycling schemes which represent the most compatible technique for energy saving and it also focuses on the kinds of data-driven approaches that can be used to improve the energy efficiency. In [6] a new technique for intra cluster routing which is more energy efficient than a well known routing protocol Multihop Router that performs multihop routing.. By using the new technique it shows that they had increased the network lifetime and total number of packet sent in the network. a novel energy-aware routing approach for sensor networks. A

gateway node acts as a cluster-based centralized network manager that sets routes for sensor data, monitors latency throughout the cluster, and arbitrates medium access among sensor is discussed in [7]

4.PROPOSED WORK

On the context of collusion attack or false data injection attack we are going to use a profile based scheme for the eliminating the malicious node. In addition to this energy conservation is also being done separately in addition to the energy conservation that happens during the data aggregation process.

We are using cluster based approach for data aggregation and for securing this data aggregation and ensuring conservation of energy we are going below mentioned things

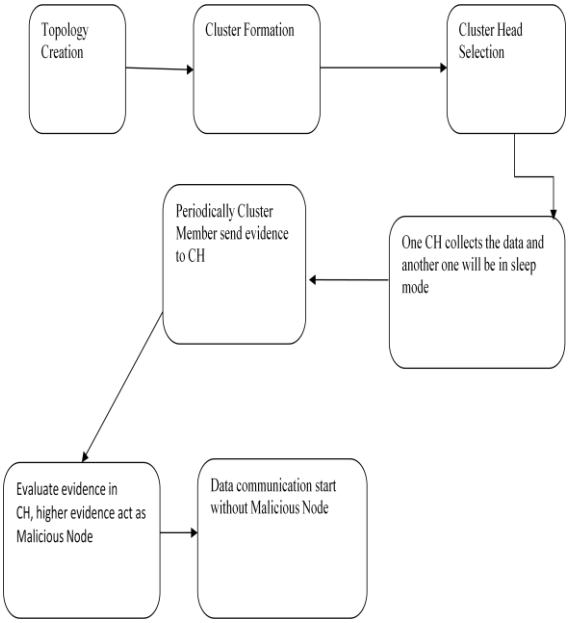

Figure: 2 proposed work

4.1. Cluster formation from network of sensor nodes

Usually, grouping sensor nodes into clusters has been widely accepted by the research community to satisfy the main objectives like scalability and high energy efficiency which in turn causes prolong network lifetime in large-scale Wireless sensor networks [8]. The corresponding hierarchical routing and data gathering protocols imply cluster-based organization of the sensor nodes in order that data fusion and aggregation are possible, thus leading to significant energy savings. In the hierarchical network structure each cluster has a leader, which is also called the cluster head (CH) and usually performs the special tasks referred above (fusion and aggregation), and several common sensor nodes (SN) as members. The cluster formation process eventually leads to a two-level hierarchy where the CH nodes form the higher level and the cluster-member nodes form the lower level. The sensor nodes periodically transmit their data to the corresponding CH nodes. CH nodes aggregate the data (thus reducing the total number of sent packets) and transmit them to the base station (BS) either directly or through multihop transmission with other CH nodes.

Nodes cooperate to form clusters, and each cluster consists of a CH along with some Cluster Members (CMs) located within the transmission range of their CH. While a node takes part in the network, it is allowed to declare itself as a CH. In this model, if a node proclaims itself as a CH, it propagates a CH Hello Packet (CHP) to notify neighboring nodes periodically. The nodes that are in this CH's transmission range can accept the packet to participate in this cluster as cluster members. On the other hand, when a node is deemed to be a CM, it has to wait for CHP. Upon receiving CHP, the CM replies with a CM Hello Packet (CMP) to set up connection with the CH. Afterward, the CM will join this cluster; meanwhile, CH and CM keep in touch with each other by sending CHP and CMP

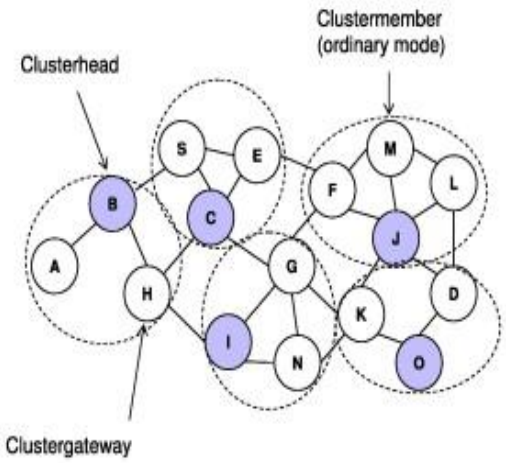

Figure 3: Formation of Clusters

4.2. Profile data collection from cluster members

Sensor node sends a data to CH, CH will validate the sensor's data with neighbour's data, if any sensor node's data is not related to remaining node's data. It will allocate a high threshold profile value to the particular sensor. Based on the scenario all the nodes

collect the profiles. By doing this it is easy to find out which of the node is having false data.

4.3. Malicious node detection ,elimination and termination from the communication between other nodes

After collecting the profiles, CH validates the profile values, if any sensor gets high profile threshold value. That sensor caused by false data injection. So CH will eliminate the sensor node from a network. The elimination is done by comparing the value that each node posses with the threshold value. If the value mismatches with the other values contained by other nodes then it is labeled as malicious node and is being eliminated from the communication with the other nodes. Cluster head performs this operation

4.4. Data Aggregation on data which is send by the cluster member

Data aggregation is a process of aggregating the sensor data using an aggregation function. Finally CH aggregates all the data and it will forward the data to corresponding sink node. This process will continue till network life time. Data aggregation is a process which is performed to conserve energy

4.5. Sleep and wakeup energy conservation:

This is an additional model for conserving energy in the network, what it is meant to be is really simple. There are a number of nodes which are in on state which will be waiting for the data to be received but may not receive data all the time. Such things will reduce energy associated with each node. Since WSN nodes are energy constrained and therefore energy wastage should be prevented. For this purpose we will make nodes go into sleep mode when they are not engaged in transmission and will switch it back to awake mode. Thus energy can be conserved in the network

5. ALGORITHM

1) Clusters are formed among different sensor nodes
2) Cluster heads are selected from each cluster
3) A particular threshold value is assigned for the node values for checking malicious behaviour
4) If a sensor node is in Cluster head's range then go to step 4
{
5) Sensor node sends data to Cluster head
}
6) Cluster head collects the profiles of each cluster member
7) Cluster head compares the node value with the initially assigned threshold value. If the node value lies in the threshold range go to step 8
{
8) Mark that node as malicious node and Eliminate that node from communication
}
9) After eliminating the node ,data will be transmitted to sink node

6. SIMULATION RESULTS AND ANALYSIS

Our proposed work is a simulation based one; simulation is done on NS2 which is a widely used simulator. Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks.

Malicious node elimination can be shown in simulation process and other parameters including energy conservation are shown as following. After simulation we have analyzed the delay, packet rate and amount of energy conserved. And it is shown in three different graphs as shown below

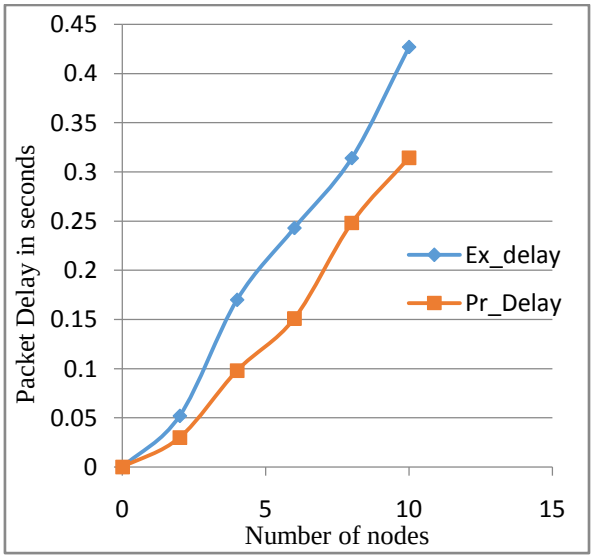

Figure 4: Analysis of packet delay in our proposed system and normal sensor network

Packet delays in two systems are plotted in the above graph. Two systems are shown with two different

colors. First one is normal sensor network and second one using data aggregation process. We can see considerable reduction in the packet delay with increase in number of nodes. This is shown in figure 4. And in figure 5 analysis of packet data rate is shown with the two, systems the one which is not having data aggregation and the one with data aggregation and having energy conservation scheme

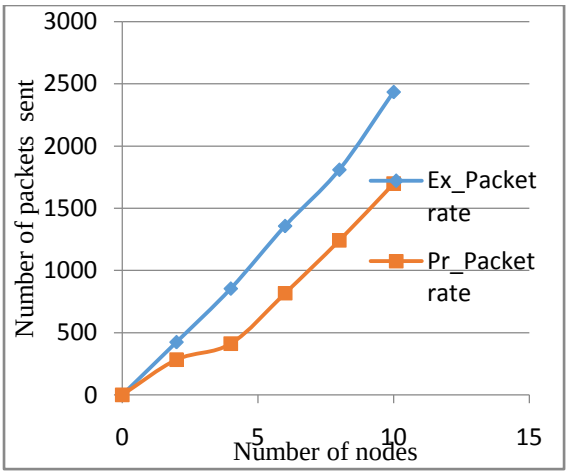

Figure 5: Analysis of packet data rate in our proposed system and normal sensor network

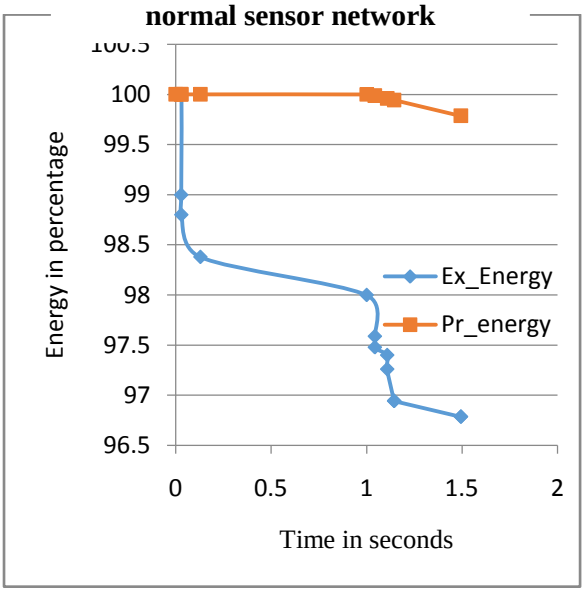

Figure 6: Analysis of amount of energy remaining in our proposed system and normal sensor network

7. CONCLUSION

Data aggregation is a process that is used for energy conservation where energy is the major limitations that a sensor network faces. Since Sensor nodes are vulnerable to many attacks, the data aggregation process is not at all secure. Many techniques has been used for securing the data aggregation process till date. But those techniques are for different sort of attacks. In our proposed work, we are using a technique that is used to prevent mainly false data injection or collusion attack. Apart from that energy conservation technique is also used and the results and analysis are shown as plotted graphs in the previous section. From this we can come to a conclusion that Energy has been conserved using the energy conservation scheme and has been used along with secured data aggregation scheme

REFERENCES

[1] Data Aggregation in Wireless Sensor Network Nandini. S. Patil, Prof. P. R. Patil B.V.. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] Solution of Energy-Efficiency of sensor nodes in Wireless sensor Networks Mohit Saini Assistant Professor, Doon Business School, Dehradun (U.K), India Rakesh Kumar Saini Assistant Professor, Department of MCA,DIT UniversitK. Elissa, IJARCSE Volume 3, Issue 5, May 2013

[3] Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence ofCollusion Attacks Mohsen Rezvani, Student Member, IEEE, Aleksandar Ignjatovic, Elisa Bertino, Fellow, IEEE and Sanjay Jha, Senior Member, IEEE,Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[4] Efficient Clustering for Improving Network Performance in Wireless Sensor Networks Tal Anker1,2 , Danny Bickson1?,Danny Dolev1 and Bracha Hod1 1 The Hebrew University of Jerusalem, Israel {anker, daniel51, dolev, hodb}@cs.huji.ac.il 2 Marvell Semiconductor, CA, USA tala@marvell.com

[5] Energy Saving in Wireless Sensor Networks Zahra Rezaei , Shima Mobininejad Department of Computer Engineering Islamic Azad University, Arak Branch , Arak , Iran

[6] Energy Aware Intra Cluster Routing for Wireless sensor networks A. Akhtar et. al., in 2010

[7] Energy-Aware Routing in Cluster-Based sensor networks A. M.Younis.et.al in 2002

[8] Constraints And Approaches For Distributed Sensor Network Security (Final)1 September 1, 2000 David W. Carman Peter S. Kruus Brian J. Matt