ENERGY EFFICIENCY AND SECURITY BASED MULTIHOP HETEROGENEOUS TRUSTED THIRD PARTY PROTOCOL IN WSN

Nami Susan Kurian

Assistant Professor, Department of Electronics and Communication Engineering,
Rajalakshmi Institute of Technology, Chennai, India

Abstract:- *Energy is one of the most decisive resources for battery powered wireless sensor networks. The key challenging problem in WSN is energy efficiency. To make the system energy efficient, Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm was used. WSNs are influenced to a wide range of attacks due to its distributed nature. Among the attacks, Byzantine attack is a serious menace to WSN, where the adversary has full control over some of the genuine nodes resulting in harming the network resulting in reduced trustworthiness of data. Recovering privacy after compromise requires either the help of a trusted third party(TTP) or access to high-quality cryptographic methods. In this paper, we propose an energy efficient aggregation of data with high security by overcoming the byzantine attack using a new protocol called Trusted Third Party (TTP) protocol. The aggregation technique is done by dividing the sensor nodes into clusters, in which each cluster consists of a cluster head called aggregator. The security over the transmission of data is done by overcoming the byzantine attack through a trusted third party (authentication node). The proposed protocol TTP overcomes the problems of insecurity in data transmission and hence increasing the energy, throughput and lifetime of the network.*

Key Words: **WSN, Data aggregation, Byzantine attack, ns-2**

1. INTRODUCTION

A Wireless Sensor Network [1] consists of spatially distributed sensors to monitor physical or environmental conditions such as temperature, sound, pressure etc and to pass the data through the network to a main location. Each sensor nodes consists of: microcontroller, communication device (radio transceiver) [2], battery, sensors and memory. WSN is an emerging technology that has wide range of potential applications including environmental monitoring medical system, emergency applications (military) and robotic exploration. Energy is one of the most critical resources for WSN. In order to increase the lifetime [12] as long as possible, energy efficiency has become the most important aspect in the design of WSN protocol. By clustering the nodes, optimization in the usage of energy at nodes is possible. Previous researches show that nodes closer to the sink tends to deplete their energy faster than the others.

Data gathering refers to the different ways where intermediate nodes forward data packets toward the sink node while combining the data gathering from different source nodes. Data gathering requires a forwarding paradigm that is different from the classic routing, which typically involves the shortest path "in relation to some specific metric" to forward data toward the sink node. Differently from the classic approach in data gathering and routing algorithms, nodes route packets based on their content and choose the next hop that maximizes the overlap of routes in order to promote in network data gathering.

Three main timing strategies are given below

a. Periodic simple aggregation: This requires each node to wait for a predefined period of time while aggregating all received data packet and then it forwards a single packet with the result of the aggregation.

b. Periodic per-hop aggregation: in this case, aggregated data packet is transmitted as soon as the node hears the transmission from all of its children.

c. Periodic per-hop adjusted aggregation: Tansmission time of a node is adjusted according to this node's position in the gathering tree.

Roles of different nodes in the routing infrastructure creation:

a. Collaborator: A node (slave node) that detects an event and reports the gathered (collected) data to a coordinator node.
b. Coordinator: A node (master node) that also detects an event and is responsible for gathering all the gathered data sent by collaborator nodes aggregates them and sends the result toward the destination (sink) node.
c. Sink: A destination node that is interested in receiving data from a set of coordinator and collaborator nodes.
d. Relay: A node that forwards data toward the sink.

Trust and reputation systems play a significant role in supporting wide range of distributed systems. The trustworthiness assessment at any given moment represents an aggregate of the behaviour of the participants up to that moment and has to be robust in the presence of various fault and malicious behaviour. There are many ways in which attacker can hack the data from the participants of the distributed system.

The most effective and recently suggested security [16] mechanism for WSN is trust and reputation. Sensors deployed in the network may result in node compromising attacks by adversaries who intend to inject false information into the system. As a result trustworthiness has become a challenging task.

2. RELATED WORKS

In "Enhanced LEACH Protocol [3] [6] for Wireless Sensor Networks", WSNs are capable of sensing, local processing and wireless communication. Minimizing energy dissipation and maximizing network lifetime are important issues in the design of routing protocols for sensor networks. LEACH stands for Low-Energy Adaptive Clustering Hierarchy) and the drawback of LEACH is improved in this paper. We propose a clustering routing protocol named Enhanced LEACH, which extend LEACH protocol by balancing the energy consumption in the network. The Enhanced LEACH outperforms LEACH in terms of network lifetime and energy efficiency. Through distributing the cluster load overhead over the cluster members, the life time of the entire network extended compared with LEACH protocol [8].

In "An Energy-Efficient Unequal Clustering Mechanism for Wireless Sensor Networks", there subsist a hot-spot problem that cluster heads that are closer to the base station(BS) tend to die faster, because they relay much more traffic than remote nodes. EEUC (Energy-Efficient Unequal Clustering) is proposed to balance the energy consumption among clusters. In EEUC, the size of the cluster near the sink node are much smaller than the clusters far away from the sink node in order to save more energy in intra-cluster as well as inter-cluster communications. Actually, EEUC is a distance based scheme and it also requires every node to have global knowledge such as its locations and distances to the sink node. EECU prolongs the network lifetime and balances the load.

"PEACH: Power-Efficient And Adaptive Clustering Hierarchy Protocol For Wireless Sensor Networks",[3] proposed that most existing clustering protocols consume large amounts of energy, incurred by cluster formation overhead and fixed level clustering, particularly when sensor nodes are thickly deployed in WSN. To solve this problem, PEACH (Power-Efficient and Adaptive Clustering Hierarchy) [5] protocol is proposed for WSNs to minimize the energy consumption of each node, and maximize the network lifetime. In PEACH, cluster arrangement is performed by using overhearing the source and the destination of packets transmitted by the neighbour nodes can be obtained by a node through overhearing. The simulation results show that PEACH can significantly save energy consumption of each node, prolong the network lifetime, and is less affected by the distribution of sensor nodes compared with existing clustering protocols.

"EECS: An Energy Efficient Clustering Scheme in Wireless Sensor Networks" [9], is proposed to produce clusters of unequal size in single hop networks. The cluster formation is based on transmission distance, e.g., distance from the plain node to the cluster-head and distance from the cluster-head to the base-station. EECS uses a weighted function ensure that clusters farther away from the base station have smaller sizes such that more energy could be saved for long-distance data transmission to the base station. Simulations show that EECS is more energy-efficient than LEACH. All candidate nodes broadcast election message within a time interval. In cluster formation phase, EECS tries to find a balancing point between energy consumption between plain nodes to the cluster-heads and that between cluster-heads to the base station. However, it requires more global knowledge about the distances between the cluster-heads and the base station. And this extra requirement of aggregating data globally adds overheads to all sensors.

"A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks" is initiated which a centralized clustering routing protocol. The main idea of BCDCP is the cluster formation where each CH serves an almost equal number of MNs to balance CH overload and uniform CH placement throughout the network. At the beginning of cluster setup, the residual energy from all the nodes in the network is collected by the base station. Based on this information, the BS first computes the average energy level of all the nodes in the network, and then chooses a set of nodes whose energy levels are above the average value. Only the nodes from the chosen set, i.e., those with sufficient energy, can be elected CHs for the current round, while those with low energy can prolong their lifetime by performing the task of ONs. Based on the chosen set, the BS computes the number of clusters and performs the task of clustering, which is accomplished in terms of an iterative cluster splitting algorithm. This algorithm first splits the network into two sub-clusters, and proceeds further by splitting the sub-clusters into smaller clusters [11]. This process will be repeated until the desired number of clusters is achieved.

In "EBRP: Energy-Balanced Routing Protocol for Data Gathering in Wireless Sensor Networks" [15], design of

an Energy-Balanced Routing Protocol (EBRP) by constructing a mixed virtual potential field in terms of depth ,energy density, and residual energy to force packets to move forward toward the sink through the dense energy area. EBRP makes momentous improvements in energy uptake balance, network lifetime, and throughput. EBRP will only find routes for each data source to the same sink.

"Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks" explores reliable data fusion in mobile access wireless sensor networks under byzantine attacks. In this q-out-of-m-rule which is popular in distributed detection and in achieving a good tradeoff between the miss detection probability. The disadvantage is that, the technique cannot be used for network with large size.

3. PROPOSED SCHEME

3.1 NETWORK MODEL

For the sensor network topology, we consider 50 nodes. The sensor nodes are divided into clusters, and each cluster has a cluster head which acts as an aggregator. Data are periodically collected and aggregated by the aggregator. In this paper we assume that the aggregator itself is not compromised and concentrate on algorithms which make aggregation secure when the individual sensor nodes might be compromised and might be sending false data to the aggregator. We assume that each data aggregator has enough computational power to run an IF algorithm for data aggregation.

3.2 Byzantine Attack

Byzantine [13] failures are hard to detect. The network seems to be operating normally in the viewpoint of the nodes, though it may actually be exhibiting by Byzantine behaviour.

Byzantine attack involves:
Injecting false information into the nodes.
Creating routing loops.
Routing packets on non-optimal paths.
Selectively dropping packets.

3.3 Adversary Model

Even though there are many attacks pertaining to the network layer in the network protocol stack, the most dangerous attack is byzantine attack. In the byzantine attack [14] model adversary can compromise a set of sensor nodes and can inject any false data through the compromised node. We assume that when a sensor node is compromised, all the information inside the node becomes accessible by the adversary. Through the compromised sensor nodes the adversary can send false data to aggregator, with the purpose of changing the values inside that. We consider that adversary has enough knowledge about the aggregation algorithm. Finally we assume that aggregated nodes cannot be compromised in the network model. In order to overcome this drawback we are using trusted third party and iterative filtering algorithm.

3.4 Trusted Third Party

The TTP protocol is the authentication node that gives authentication ID to each node in a cluster. A malicious node is an external node that tries to inject false data or fetch the original data in the transmission. When this malicious node attacks a node in any cluster, TTP comes to know that an external node is about to access the data in the network. Now the TTP changes the authentication ID for that cluster within a few milliseconds.

So that the malicious node gets confused with the ID it supposed to inject or fetch the original data. The transmission continues normally in a secured manner.

A malicious node is trying to enter the network, it is identified by a trusted third party. The malicious node tries to compromise the adversary node and tries to either inject the false data or take the original data from the node. The authentication node thus starts changing identification number for the nodes in that cluster and the malicious node gets confused in transmitting the false data to the nodes.

In TTP models, the relying parties use this trust to secure their own interactions. TTPs are common in any number of commercial transactions and in cryptographic digital transactions as well for example, would issue a digital identity certificate to one of the two parties in the next example. Then becomes the Trusted-Third-Party to that certificates issuance. Likewise transactions that need a third party recordation would also need a third-party repository service of some kind or another.

The proposed algorithm can be divided into three phases. In Phase 1, creation of node takes place. Some and formation of clusters takes place. At the first cluster head is randomly chosen and based on energy level from next transmission. Chances is given for all the nodes to become a cluster head. In Phase 2, the cluster head transmits the data to the nearest hop which helps in less consumption of less energy, since energy is directly proportional to the distance between the nodes. This method is implemented using DSDV algorithm. In Phase 3, a malicious node tries to enter the network which either injects false data into the node or fetches the original data from the node while transmission. This is called byzantine attack and can be overcome using trusted third party protocol (TTP). TTP changes the identification code of each node in that cluster so that the malicious node gets confused. Thus secure transmission is obtained.

PHASE 1

When an event is detected by one or more nodes, the leader election algorithm starts and sensing nodes will be running for leadership (group coordinator); For this election,

all sensing nodes are eligible. If this is the first event, the one that is closest to the sink node will act as the leader node. Otherwise, the node that is closest to an already established route will act as leader node. In the case of a draw, i.e., two or more concurrent nodes have the same distance in hops to the sink (or to an established route), the node with the smallest ID maintains qualification.

Another possibility: using of the energy level as a tiebreak criterion. At the end of the election algorithm only one node in the group will be announced as the leader (Coordinator). The remaining nodes that detected will be the Collaborators. The Coordinator gathers the information collected by the Collaborators and sends them to the sink. A key advantage of this algorithm is opportunistic aggregation.

PHASE 2

In this phase, the nodes start transmitting the data. This is done using the Destination Sequence Distance Vector (DSDV) algorithm. In this algorithm, the data from one node is directly transmitted to next nearest node, which results in consumption of less energy. Power is directly proportional to energy. Thus if the distance between the nodes is less then power consumed will be less, inturn the energy consumed will be less.

PHASE 3

In this phase, a malicious node is introduced in the network which either injects false data or fetches the original data the node. This event is termed as byzantine attack, to overcome this attack we propose an trusted third party model. Which assigns a authenication ID to the affected node in an cluster. Thus the malicious node gets confused, it cannot inject false data or fetch the original data. By this way the secured transmission is obtained.

4. PERFORMANCE EVALUATION

Energy efficiency of sensor nodes for LEACH and TTP protocol are shown in the below figure. Energy efficiency is the most challenging attribute for WSN. In TTP protocol, the security is incorporated along with optimized routing algorithm. As the data transmission is too secured, the number of retransmissions and dropping of packets can be reduced to greater extent. But in case of LEACH protocol, no security is assured and chances of dropping the packets are more. Hence we can conclude that energy consumption in case of proposed protocol, TTP is less due to the secured routing technique thereby increasing the lifetime of the network.

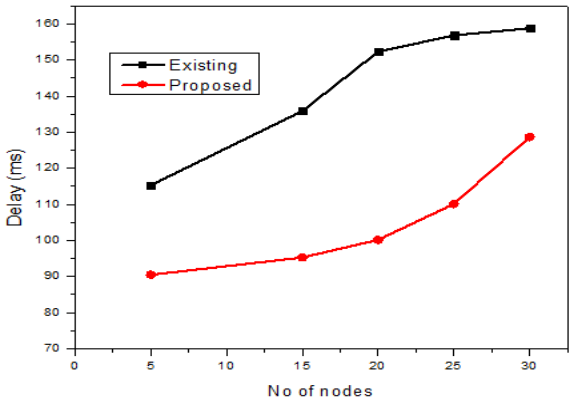

Chart -1 Delay for Existing Vs Proposed model

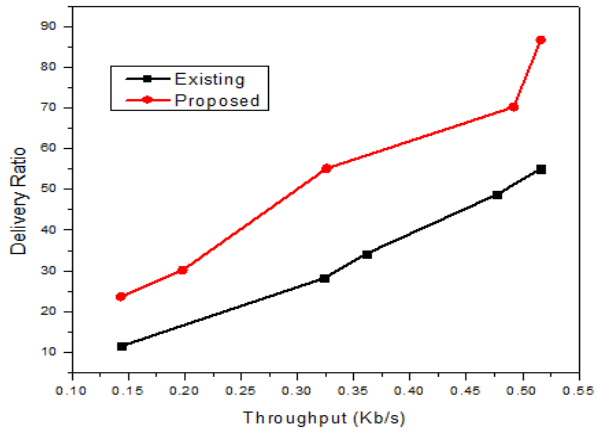

Chart -2 Delivery ratio Vs throughput 38

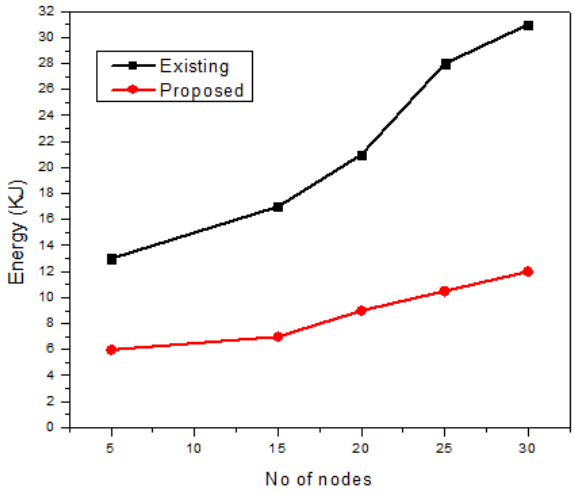

Chart -3 Energy consumption for existing Vs proposed model

Energy efficiency of sensor nodes for LEACH and TTP protocol are shown in the below figure. Energy efficiency is the most challenging attribute for WSN. In TTP protocol, the security is incorporated along with optimized routing algorithm. As the data transmission is too secured, the

number of retransmissions and dropping of packets can be reduced to greater extent. But in case of LEACH protocol, no security is assured and chances of dropping the packets are more. Hence we can conclude that energy consumption in case of proposed protocol, TTP is less due to the secured routing technique thereby increasing the lifetime of the network.

Energy efficiency [7] of sensor nodes for LEACH and ESAB protocol are shown in the below figure. Energy efficiency is the most challenging attribute for WSN. In ESAB protocol, the security is incorporated along with optimized routing algorithm. As the data transmission is too secured, the number of retransmissions and dropping of packets can be reduced to greater extent. But in case of LEACH protocol, no security is assured and chances of dropping the packets are more. Hence we can conclude that energy consumption in case of proposed protocol, ESAB is less due to the secured routing technique thereby increasing the lifetime of the network.

5. CONCLUSION

LEACH protocol selects the cluster heads randomly, which results in faster death of some nodes. In addition, LEACH protocol does not provide secured data transfer over the network. In the proposed protocol, we put forward TTP protocol which provides an energy efficient aggregation of data with high security by overcoming the byzantine attack. The aggregation technique is done by splitting the sensor nodes into clusters, in which each cluster consists of a cluster head called aggregator. The cluster head is elected on the basis of considering the nodes with the highest amount of energy. Security over the transmission of data is done by overcoming the byzantine attack through trusted third party algorithm. The proposed protocol TTP overcomes the problems of insecurity in data transmission and hence increasing the energy, throughput and lifetime of the network. TTP protocol not only helps in secured transmission of data but also helps in optimizing the usage of energy in each node in a greater extent.

REFERENCES

[1] Miguel Angel Erazo Villegas, Seok Yee Tang,Yi Qian, “Wireless Sensor Network Communication Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring”.

[2] Adinya John Odey, Daoliang Li, “Low Power Transceiver Design Parameters for Wireless Sensor Networks,” in Wireless Sensor Network.

[3] Rajashree.V.Biradar , V.C .Patil, Dr. S. R. Sawant , Dr. R. R. Mudholkar, “Classification and comparison of routing protocols in wireless sensor networks”, in Special Issue on

[4] Ubiquitous Computing Security Systems. Bhavana Narain, Anuradha Sharma, Sanjay Kumar and Vinod Patle, “Energy efficient mac protocols for wireless sensor networks: a survey”, in International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.3, August 2011.

[5] Shio Kumar Singh 1, M P Singh 2, and D K Singh, “Routing Protocols in Wireless Sensor Networks – A Survey”, in International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.

[6] Owais Ahmed, Ahthsham Sajid and Mirza Aamir, Comparison of Routing Protocols to Assess Network Lifetime of WSN”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 3, November 2011.

[7] Pallavi S. Katkar, Prof. (Dr.) Vijay R. Ghorpade, “A Survey on Energy Efficient Routing P”, in International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 81-83.

[8] Ravneet Kaur, Deepika Sharma and Navdeep Kaur, “Comparative Analysis Of Leach And Its Descendant Protocols In Wireless Sensor Network”, in International Journal of P2P Network Trends and Technology-Volume3Issue1- 2013.

[9] Jamal N. Al-Karaki Ahmed E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey”.

[10] Stephanie Lindsey, Cauligi S. Raghavendra, “PEGASIS: Power-Efficient Gathering in Sensor Information Systems”.

[11] Ossama Younis and Sonia Fahmy, “HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks”.

[12] Ingook Jang, Suho Yang, Hyunsoo Yoon, “EMBA: An efficient multihop broadcast protocol for Asynchronous duty-cycled wireless sensor networks,” in IEEE transactions on wireless communications.

[13] Jing Yang Koh, Joseph Chee Ming Teo and Wai-Choong Wong, “Mitigating Byzantine Attacks in Data Fusion Process for Wireless Sensor Networks using Witness” .

[14] Mohan.N, Akram pasha, “Distributed Detection of Byzantine Attacks in WSNs: A Short Critical Survey,” In International Journal of Computer Science and Information Technology Research.

[15] Fengyuan Ren, Member, Jiao Zhang, Tao He, Chuang Lin, and Sajal K. Das, “EBRP: Energy-Balanced Routing Protocol for

[16] Data Gathering in Wireless Sensor Networks”, in IEEE transactions parallel and distributed systems, vol. 22, no. 12, december 2011.

[17] Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks Mohamed M.E.A. Mahmoud, Xiaodong Lin, Senior Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE, in ieee transactions on parallel and distributed systems, vol. 26, no. 4, april 2015.