Energy Aware Blind Data Aggregation for Data Intergrity in Wireless Sensor Network

Pallavi Matkar, Lalit Dole

Abstract— Wireless sensor networks consist of sensor nodes with sensing and communication capabilities. This paper presents a new Energy aware routing protocol called SHHRP (Simple Homogenous Heterogeneous Routing Protocol) Simulation result shows that proposed protocol is energy efficient when compared to existing protocol. Though, the base station only fetches the aggregated result, which origin two problems. First, the usage of aggregation function is obliged. Second, the base station cannot confirm the data integrity and authenticity. This paper go to overcome the above two drawbacks. Besides, the design has been concluded and adopted on both homogeneous and heterogeneous wireless sensor networks. This paper also implements Elliptic curve cryptography for encryption and decryption of data in WSN.

Keywords- Blind data aggregation,data integrity,Elliptic Curve Cryptography,SHHRP protocol ,wireless sensor network

I. INTRODUCTION

Wireless Sensor Network is important in many application where infrastructure is not feasible for physical communication. [1].Data aggregation is essential to reduce data redundancy and to improve data accuracy. Clustering is an effective and practical way to enhance the system performance of WSN.[2]. The objectives of clustering are to minimize the total transmission power aggregated over the nodes in the selected path, and to balance the load among the nodes for prolonging the network lifetime. In order to secure WSN,various cryptographic solution have been proposed . ECC is a kind of public-key cryptosystem like RSA. The security level which is given by RSA, can be provided even by smaller keys of ECC. ECC is particularly well suited for wireless communications.

II. RELATED WORK

A WSN typically has little or no infrastructure. It consists of a number of sensor nodes (few tens to thousands) working together to monitor a region to obtain data about the environment[4] Clustering is used to decrease energy consumption and collision.This paper focuses on four phases: Cluster formation, Cluster head election, Data aggregation and Maintenance[5].Aggregation becomes especially challenging if end-to-end privacy between sensors and the sink is required. [6][7]. Since both data aggregation and security are essential for wireless sensor networks, while these data aggregation protocols improve the bandwidth and energy utilization in the network[8][9].

The author in [11] introduce a concept named Recoverable Concealed Data Aggregation (RCDA) in which a base station can recover each sensing data generated by all sensors. Various routing protocols [12] have been proposed to be used for WSNs considering different application demands of WSNs. Security is a very important issue when designing or deploying any network[16][17] or protocol Elliptic Curve Cryptography (ECC), is one of these new algorithms and it is the most promise regarding the energy and time consumption.

III. DESIGN AND IMPLEMENTATION

A. Implementation of SHHRP (Simple Homogenous Heterogenous Routing Protocol)

In this project we are implementing a protocol called SHHRP which is an extension of OLSR protocol[1].The proposed protocol consist of features of OLSR protocol.The drawback of existing protocol is it does not take into consideration energy but only the number of nodes covered at two-hop. Our goal is to make the SHHRP routing protocol energy efficient in order to maximize the network lifetime.

B. Neighbor Sensing

Each node sends hello interval to its 1-hop neighbor's hello message to achieve neighbor sensing which have not to be forwarded. When nodes send the message it contains node neighbor list and their link status, which allow them to deduce the whole 2-hop neighbor and their status.

C. MPR Flooding

Best as possible controlled traffic flooding is the aim of Multipoint Relays (MPR). In MPR flooding, MPRs are selected in such a way that when a flooding message is transmitted by the MPR set it must reaches all 2-hop neighbors. MPR(n), the MPR set of a node n, which is also represented as the smaller subset of symmetric 1-hop neighbors of n, having symmetric links with all 2-hop neighbors of n.

D. Topology Diffusion

The objective of topology diffusion is to create routing tables using periodic topology control messages (TC messages). TC messages are circulated by each node with a non-empty MPR selector set to all network nodes, broadcasting at least links between itself and the nodes in its MPR selector set, to achieve Topology Diffusion.

E. Energy model

When a transmitter transmits one packet to next hop, because of the shared nature wireless medium, all its neighbors receive this packet even it is intended to only one of them.

Manuscript received on July, 2013.

Pallavi Matkar, CSE DEPT, G.H.Raisoni College of Engg,Nagpur, India.

Lalit Dole, CSE DEPT, G.H.Raisoni College of Engg,Nagpur, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Moreover, each node situated between transmitter range and interference range receives this packet but it cannot decode it. These two problems generate loss of energy. Our proposed model consist of cell voltage and remaining energy.The cell voltage is given under 3.3v.

```
    // discharge at .33 A for 1700 seconds
  sem->SetCurrentA (1.33);
  now += Seconds (1701);
 // discharge at 4.66 A for 628 seconds
  Simulator::Schedule (now,
                &SimpleDeviceEnergyModel::SetCurrentA,
                sem,
                4.66);
          now += Seconds (600);
```

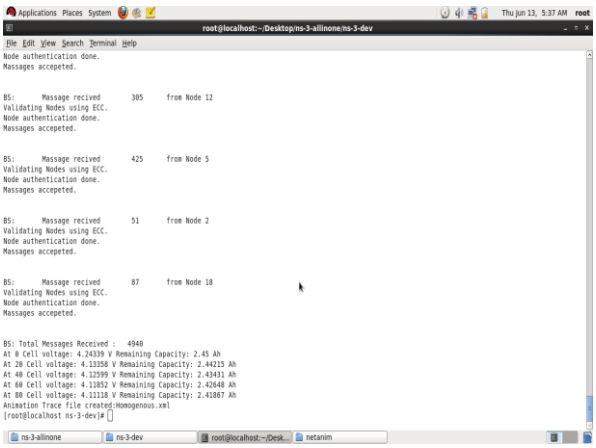

FIGURE 1. SCENARIO OF HOMOGENOUS WSN

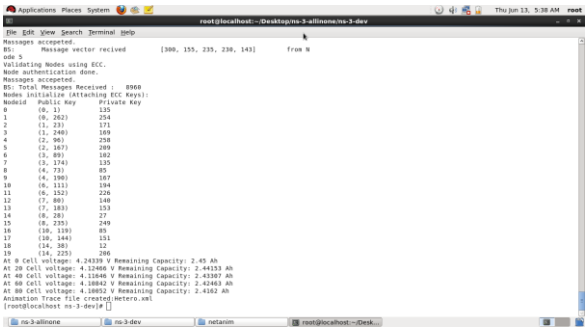

FIGURE 2. SCENARIO OF HETEROGENEOUS WSN

F. Implementation of secure Data Aggregation

Our work, focuses on scenario that after collecting information, each sensor node encrypts its data according to elliptic curve encryption and sends it to the nearest aggregator. Then, aggregators aggregate the received encrypted data (without decryption) and send it to the base station, which in his turn decrypts the data and aggregates it.

G. Computing the Average for data aggregation

The arithmetic mean is the "standard" average, often simply called the "mean"[3]. The aggregation function for average can be carried out by summation of nodes divide by number of nodes.This would give average for calculating data aggregation.

H. Computing Public and private key

Elliptic curve cryptography is used for encryption of data. It uses Galios finite field equation to calculate public and private key[2].Finite field equation can be given by $y2 = x3 + ax + b$ mod p.By satisfying the equation public key and private key can be calculated.

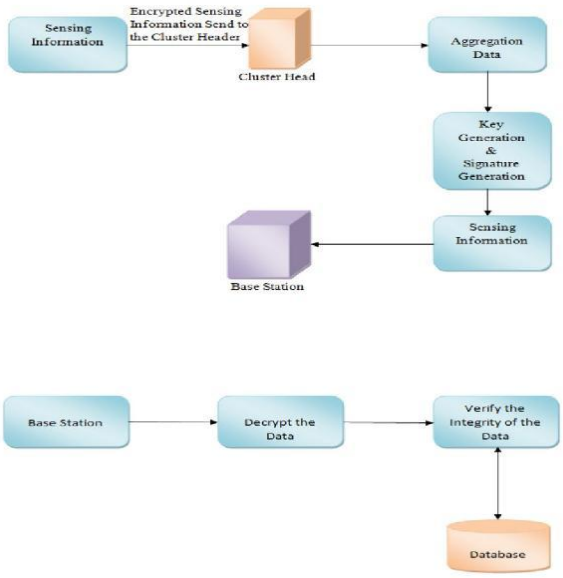

FIGURE 3. AGGREGATION AND KEY GENERATION

I. Implementation on Homgenous and Heterogenous Sensor Network

In homogenous sensor network it consist of four phase: Setup, Encrypt, Aggregate, and Verify. The Setup procedure is to prepare and install necessary secrets for the BS and each sensor. When a sensor decides to send sensing data to its CH, it performs Encrypt and sends the result to the CH. Once the CH receives all results from its members, it activates Aggregate to aggregate what it received,and then again encrypt it and then sends the final results to the BS. The last procedure is Verify. The BS first extracts individual sensing data by decrypting the aggregated ciphertext. Afterward, the BS verifies the authenticity and integrity of the decrypted data based on the corresponding aggregated signature.

In heterogenous network consist of H-sensor and L-sensor H-sensor act as cluster head because of more computation power. RCDA-HETE is composed of five procedures: Setup, Intracluster Encrypt, Intercluster Encrypt, Aggregate, and Verify. In the Setup procedure, necessary secrets are loaded to each H-Sensor and L-Sensor. Intracluster Encrypt procedure involves when L-Sensors desire to send their sensing encrypted data to the corresponding H-Sensor. In the Intercluster Encrypt procedure, each H-Sensor aggregates the received data and then encrypts and signs the aggregated result. Finally, the Verify procedure ensures the authenticity and integrity of each aggregated result.

IV. SIMULATION RESULT

In the proposed work, nodes are randomly deployed. Homogeneous and Heerogeneous network structure is created. Using the recovery property, the base station verifies all the data by the two processes. A network structure is created within the network. The performance of the network is evaluated in terms of parameters such as Throughput, Packet Delivery Ratio (PDR), Aggregation Delay and proposed protocol

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Throughput is the average rate of successful message delivery over a communication channel

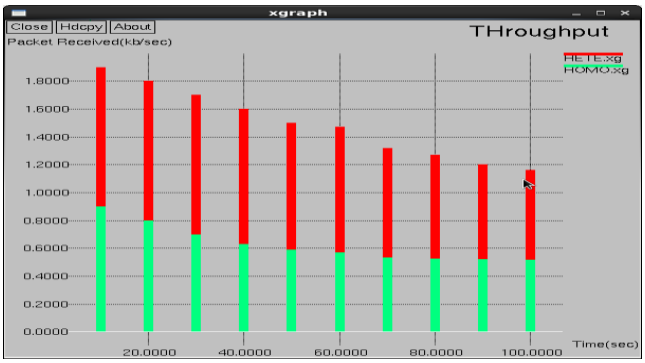

FIGURE 4. THROUGHPUT

The given graph shows the throughput for homogenous and heterogenous sensor network. As the number of sending packet increases the simulation time also increases.

The **packet delivery ratio (PDR)** is defined as the ratio of the number of packets received by the destination and the number of packets transmitted by the source.

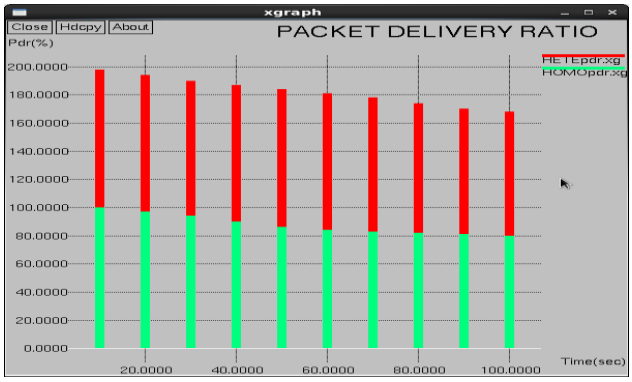

FIGURE 5. PACKET DELIVERY RATIO

The given graph shows the packet delivery ratio for homogenous and heterogenous sensor network which shows that time required for packet delivery ratio is more for heterogenous sensor network as compared to homogenous sensor network.

Aggregation delay is also evaluated by measuring time spent on processing time on aggregating cipher texts and signatures in the proposed schemes.

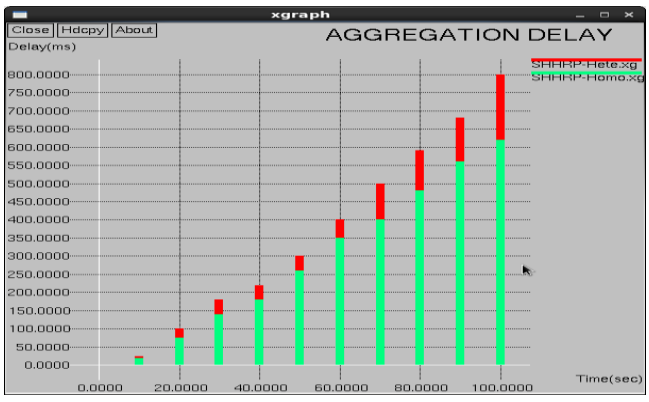

FIGURE 6. AGGREGATION DELAY

The given graph shows the aggregation delay in homogenous and heterogenous sensor network.In homogenous sensor network sensor node sense single value so the time required for aggregation delay is less as compared to heterogenous sensor network where it sense multiple value.

Energy versus time shows the ratio of proposed protocol energy in comparison with existing protocol energy.

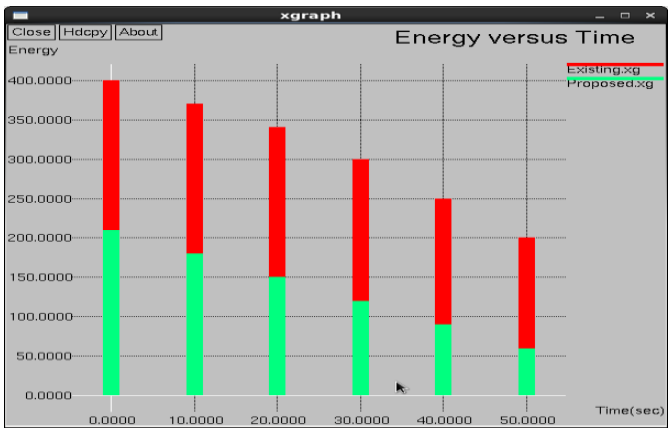

FIGURE 7.ENERGY VERSUS TIME

The given graph shows energy versus time of existing and proposed protocol.The graph proves that the proposed protocol is energy efficient compared to existing protocol.The proposed protocol called SHHRP consumes less energy for sending packet compared to existing protocol

V. CONCLUSION

The study has concluded that proposed energy aware protocol called SHHRP(Simple Homogenous Heterogenous Routing Protocol) for homogenous and heterogenous sensor network is energy efficient compared to existing protocol. Number of node alive, indicating better network lifetime of network. Data aggregation is also an important aspect in wireless sensor network.This study also presents blind data aggregation schemes for homogeneous and heterogeneous WSNs in which the base station can securely recover all sensing data rather than aggregated results. With blind data aggregation it provides end-to-end encryption.

However, we implemented that base station can retrieve each and every sensing value even the data is aggregated. Another important aspect in wireless sensor network is of security.Taking security into consideration we have used Elliptic curve cryptography for encryption and decryption of data.

FUTURE SCOPE

In future scope research can be carried out to develop every sensor node to be capable of both aggregating and forwarding data in order to improve network security and efficiency. However due to time and resource constraint the research could not take the study to next level. For future work, a model with high density of heterogeneous wireless sensor nodes with its topology is proportionately increased according to the application to have good energy efficient and increasing lifetime network may be investigated

REFRENCES

1. Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou," Sensor Network Security: A Survey," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER 2009
2. Huang Lu, Jie Li, Mohsen Guizani, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, 25 Feb. 2013. IEEE computer Society Digital Library. IEEE Computer Society.
3. Li Lan-ying, Jiang Xiu-li; Zhong, Shenghai, Hu Lei. Energy Balancing Clustering Algorithm for Wireless Sensor Network Networks Security, *Wireless Communications and Trusted Computing, 2009*. NSWCTC '09. International Conference on Volume 1, 25-26 April 2009 Page(s):61 – 64
4. Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal'" Wireless sensor network survey ," Department of Computer Science, University of California, Davis, CA 95616, United States, J. Yick et al. / Computer Networks 52 (2008) 2292–2330
5. Nandini. S. Patil, Prof. P. R. Patil, "Data Aggregation in Wireless Sensor Network," Proc. IEEE International Conference on Computational Intelligence and Computing Research, 2010.
6. R. Rajagopalan and P. Varshney, "Data-Aggregation Techniques in Sensor Networks: A Survey," IEEE Comm. Surveys Tutorials, vol. 8, no. 4, pp. 48-63, Oct.-Nov. 2006.
7. K. Wu, D. Dreef, B. Sun, and Y. Xiao, "Secure data aggregation without persistent cryptographic operations in wireless sensor networks", Ad Hoc Networks, vol. 5, no.1, pp. 100-111, 2007
8. S. Ozdemir, "Secure and Reliable Data Aggregation for Wireless Sensor Networks", LNCS 4836, H. Ichikawa et al. (Eds.), pp. 102-109, 2007
9. Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin, and Hung-Min Sun, "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 4, APRIL 2012
10. S. Vijayanand, R.M. suresh, "AN OVERLOOK ON ROUTING TECHNIQUES IN WIRELESS SENSOR NETWORKS," *IET-UK International Conference on Information and Communication Technology in Electrical Sciences*, Dr. M.G.R. University, Chennai, Tamil Nadu, India, 2007, pp.557-998
11. Pardeep Malik "Elliptic Curve Cryptography For Security Inwireless Networks"Statistics 2011 Canada: 5th Canadian Conference in Applied Statistics/ 20th conference of the Forum for Interdisciplinary Mathematics - Interdisciplinary Mathematical Statistical Techniques, July 1- 4-2011, Concordia University, Montreal, Quebec, Canada
12. Sonali U. Nimbhorkar, and Dr. L. G. Malik "A Survey On Elliptic Curve Cryptography (ECC)" International Journal of Advanced Studies in Computers, Science and Engineering vol.1 ,issue 1 pp. 1-5, July, 2012