A Security Enhancing Scheme in Leach using Homomorphic Encryption

Neha Chhabra[1], Parikshit Singla[2]

[1]M.Tech Scholar, Department of CSE, DVIET, Karnal, India

[2]Assistant Professor, Department of CSE, DVIET, Karnal, India

Abstract: ***As WSNs grow in application area and are used more frequently, the need for security in them becomes inevitable and vital. However, the inherent characteristics of WSNs incur constraints of sensor nodes, such as limited energy, processing capability, and storage capacity, etc. These constraints make WSNs very different from traditional wireless networks. Consequently, many innovative security protocols and techniques have been developed to meet this challenge. In this paper, we outline security and privacy issues in sensor networks, address the state of the art in sensor network security and energy consumption of different scheme; specially application of public key cryptography also known as homomorphic encryption. Till now it is a known fact that asymmetric key cryptography is not suitable for WSN. But with the introduction of new energy efficient sensor nodes such as TelosB etc. researchers are exploring and evaluating the effect of public key cryptography on WSN.***

Keywords: Secure data aggregation in WSN, Concealed data aggregation, homomorphic encryption

1. Introduction

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through the network to a main location. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attacks. Security is a common concern for any network system, but security in Wireless Sensor Network is of great importance to ensure its application success. Providing security for WSN represents a rich field of research problems as many existing security schemes for traditional networks are not applicable for WSN. Moreover, analysis of security requirements gives right directions to develop or implement the proper safeguards against the security violations [6].

Encryption and key distribution are important primitives to build secure Wireless Sensor Networks (WSN). A large amount of different key distribution schemes were implemented, targeting different types of WSNs. These schemes face issues with respect to their requirements, implementations, and theoretic foundations [2]. Though security is regarded as a standalone component of the architectures of many systems, in case of wireless sensor networks, it must get adequate attention. In most application domains, the sensors are used to collect a specific type of data from particular target areas, and the collected data are often considered secret and are not intended for public disclosure. Hence, efficient and secure mechanisms are needed to transmit acquired data securely to the appropriate recipients.

In security schemes based on symmetric cryptography, when a node is compromised, the adversary can get the secret keys stored in it and personate other nodes who have shared secret keys with the compromised node to forge messages. Random key distribution approaches are prevailing at present. However, few analyses about communication overload in these schemes have been conducted. Rekey and perfect backward secrecy are also serious issues for those random pre-distribution schemes [4]. So how the compromised nodes affect the security of the whole networks is a main factor for evaluation. As a public key cryptosystem, the security of private keys is certainly the focus. The common perception of public key cryptography is that it is complex, slow, power hungry, and not at all suitable for use in ultra-low power environments like wireless sensor networks. To keep energy consumption low, nodes have limited computing power, small RAM, and low storage capacity. Once keys are exchanged and authenticated, efficient block ciphers are required to encrypt network communication in real time. Besides block ciphers, which were designed for a small memory footprint and smaller block size, modern microcontrollers used in sensor nodes come with implementations of the Advanced Encryption Standard (AES). From the practical point of view, group key distribution [5] and public key based might be the tendency. The progress in efficiently implementation of Elliptic Curve Cryptosystem (ECC) and Hyper Elliptic Curve Cryptosystem (HECC) and advances in sensor hardware will make public key cryptosystem practicable in few years [3].

In many applications of wireless sensor networks, the base station is more interested in aggregated data than exact individual values from all sensors. By aggregating data, it is also greatly helpful to reduce the amount of data to be transmitted for conserving valuable energy. Indeed, current in-network aggregation schemes are beneficial to communication energy consumption but they are designed without considering possible security issues [1]. Furthermore, wireless sensor networks are often designed with neighbor nodes sharing keys or with decryption at aggregator nodes. In either situation the potential for aggregator nodes to be physically compromised means that data confidentiality is at high risk. Therefore secure data aggregation is desirable where data can be aggregated without the need for decryption at aggregator nodes. Aggregation becomes especially challenging if end-to-end

confidentiality between a source and a destination is required. Current proposed secure data aggregation schemes are rather elementary and more practical schemes are demanded. It is worthwhile to pay more attention how to apply homomorphic encryption to secure aggregation effectively. In the meantime, it is of great help to focus on specific popular aggregation protocols of WSNs to design realistic secure aggregation.

2. Objectives

Based on the above discussion we can say that homomorphic encryption provides a better security as compared to secret key cryptography (SKC) can be employed in WSN scenario where we need to protect our data during communication and also in aggregation phase. However it may consume more power than SKC. It will also remove the requirement of key distribution which is a major issue in SKC. So, we set following objective for our paper work:

1. Proposing new encryption schemes including homomorphic encryption techniques in LEACH algorithm for security enhancement in aggregation and communication of data and node energy consumption efficiency.
2. Evaluation of above said schemes by simulation in MATLAB environment for network life elongation and measurements of energy dissipation during the operation.

3. Proposed Simulation of Encryption Schemes

In this paper, we have considered three encryption schemes for simulation purpose. These are described as:

3.1 Concealed data Aggregation (CDA)

In the first scheme, the sensor nodes encrypt data using RSA homomorphic algorithm signature generation. Cluster heads aggregate the whole data into one without decrypting it and again sending data to base station. This type of scheme is also called concealed data aggregation (CDA).

3.2 In-network Aggregation (INA)

In the second scheme, the sensor nodes encrypt a newly generated session key using RSA homomorphic algorithm signature. The sensor node use this session key to encrypt data using AES algorithm and then RSA encrypted session key and session key encrypted data is sent to the Cluster heads(CHs). CHs decrypt data using session key which is retrieved by CH's own private key and then aggregate the whole data into one and again use RSA encryption for sending session key and session key encrypted data to base station. This type of scheme is also called in network aggregation (INA).

3.3 RSA based key distribution

In this scheme, Base Station first distributes a common session key for each round which is encrypted by individual node's public keys. Each sensor node decrypts the session key using its own private key. This is also called key exchange mechanism. Once distribution of key is completed data can be sent to CH and BS using SKC's AES Algorithm.

4. Parameters and Results

Sensor nodes are assumed of the type of TelosB containing ZigBee transceiver CC2420. Below is the power consumption for signature generation and verification and key exchange for client side and server side of TelosB estimated by Piotrowski et.al.[7].

Table 4.1: Power consumption calculated at 3V supply voltage. Power consumption per bit at transmission speed of 250 kbit/s with 0 dBm output power

Length	Length of the field Area	100 m
Width	Width of the field Area	100 m
bsX	x coordination of base station	50 m
bsY	y coordination of base station	200 m
initEnergy	Initial energy of each node	6750 Ws
transEnergy	Energy for transferring of each bit (ETX)	0.209e-6 Ws/bit
recEnergy	Energy for receiving of each bit (ETX)	0.226e-6 Ws/bit
fsEnergy	Energy of free space model	10e-12 Ws/bit
mpEnergy	Energy of multi path model	1.3e-15 Ws/bit
aggrEnergy	Data aggregation energy	5e-9 Ws/bit
siGEnergy	Signature generation energy	68.97e-3 Ws for RSA-1024
siVEnergy	Signature verification energy	2.70e-3 Ws for RSA-1024
keyexEnergy	Key exchange energy	15.40e-3 Ws
encEnergy	Encryption Energy (AES)	2.025e-7 Ws

The sole criterion for evaluation is based on the Sum of energy consumption and No. of Dead nodes over the number of rounds of operation for achieving the security by three encryption scheme for LEACH protocol. The following figures shows the comparison of two factors i.e. sum of energy and no. of dead nodes for three mentioned schemes

4.1 Concealed data Aggregation (CDA)

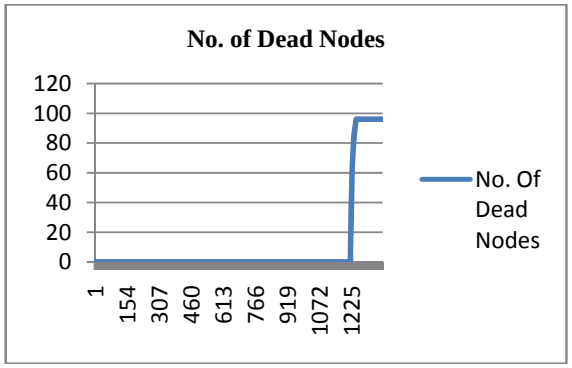

Figure 1: No. of dead nodes over no. of rounds of operation

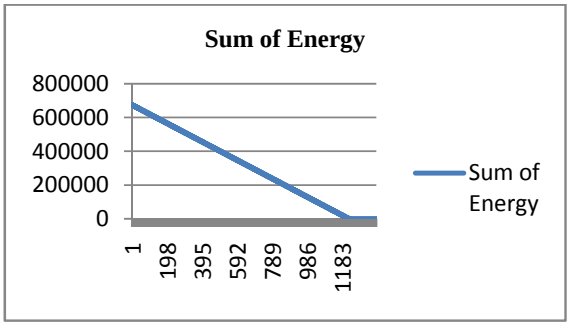

Figure 2: Sum of energy of all the nodes over no. of rounds of operation

4.2 In-Network Aggregation (INA)

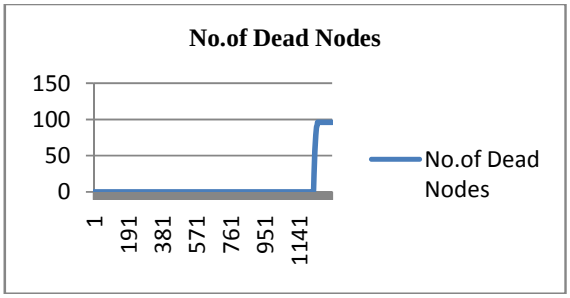

Figure 3: No. of dead nodes over no. of rounds of operation

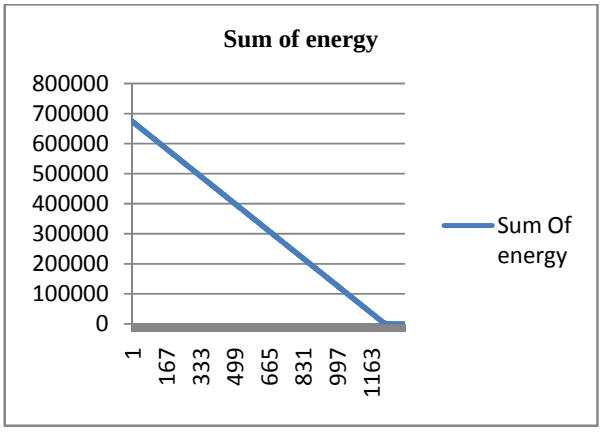

Figure 4: Sum of energy of all the nodes over no. of rounds of operation

4.3 RSA based key distribution

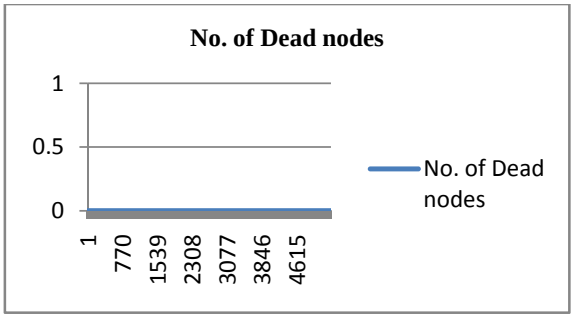

Figure 5: No. of dead nodes over no. of rounds of operation

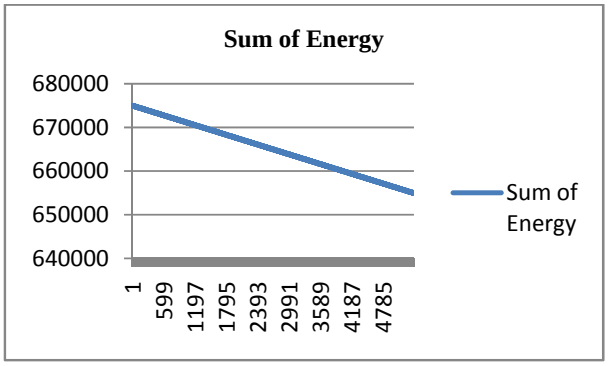

Figure 6: Sum of energy of all the nodes over no. of rounds of operation

5. Conclusion & Future Scope

In this paper, we look at encryption schemes for providing security for data aggregation which has a significant impact on the overall reliability and energy dissipation of sensor nodes. There is a tradeoff between energy consumption and security. In RSA based key distribution less energy is consumed during the operation but it is less secure as compared to other two schemes. In future scope we can try to choose other mechanisms for maintaining security as well as less energy consumption in wireless sensor networks.

References

[1] N. Behboudi and A. Abhari. , "A Weighted Energy Efficient Clustering (WEEC) for Wireless Sensor Networks. Seventh International Conference on Mobile Ad-hoc and Sensor Networks (MSN), pp.146-151, 2011.

[2] M. Ilyas and I. Mahgoub., Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, International Journal of Distributed Sensor Networks, vol. 4, no. 4, pp. 369- 369, 2008.

[3] Liu and P. Ning. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Proc. 7th International Conference on Information Processing in Sensor Networks (IPSN 2008), pp. 245–256, 2008.

[4] S. Q. Ren, D. S. Kim, and J. S. Park. A Secure Data Aggregation Scheme for Wireless Sensor Networks. In Frontiers of High Performance Computing and Networking ISPA 2007 Workshops, pages 32–40. LNCS 4743, 2007.

[5] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones. Applying Secure Data Aggregation techniques for a Structure and Density Independent Group Based Key Management Protocol. In Third International Symposium on Information Assurance and Security (IAS 2007), pages 44 49, 2007.

[6] Pathan, A.-S. K., Lee, H.-W., and Hong, C. S., “Security in Wireless Sensor Networks: Issues and Challenges,” Proceedings of 8th IEEE ICACT 2006, Volume II, 20-22 February, Phoenix Park, Korea, pp. 1043-1048, 2006.

[7] Piotrowski, K., Langendoerfer, P., and Peter, S., “How Public Key Cryptography Influences Wireless Sensor Node Lifetime,” Proceedings of ACM SASN 2006, Virginia, USA, pp. 169-176, 2006.

Author Profile

Neha Chhabra received her B.Tech (CSE) degree from Kurukshetra University, Kurukshetra , in 2010. Currently she is persuing M.Tech (CSE) from Doon Valley Institute of Engineering & Technology, Karnal. She has 1 year teaching experience in Gurunanak Institute Mullana.

Parikshit Singla received his B.Tech (CSE) degree from Kurukshetra University, Kurukshetra in 2002. M.Tech (CSE) degree in 2008. He is currently working as Assistant Professor in Deptt. of Computer Science & Engineering, Doon Valley Institute of Engineering & Technology, Karnal. His research interests are Computer networks and Image Processing.