Developing a Security Protocol based on LCG and Orthogonal Matrices for Wireless Sensor Networks

Md. Abdul Hamid[1], Muhammad Mahbub Alam[2] and Choong Seon Hong[3]

[1,2,3] Department of Computer Engineering, Kyung Hee University
1 Seocheon, Giheung, Youngin, Gyeonggi 449-701 Korea
{hamid, mahbub}@networking.khu.ac.kr and cshong@khu.ac.kr

***Abstract* — In this paper, we focus on devising secure data aggregation protocol by exploiting the concept of orthogonal set of rotation matrices and Linear Congruential Generator (LCG). To suit the stringent property of sensors, our protocol provides acceptable level of security without any secret key pre-distribution. The level of security depends on the LCG based pseudo-random number and the change of angle of rotation matrix. We demonstrate the feasibility of our proposed scheme through analysis.**

***Keywords* — LCG, Orthogonal matrix, Sensor network security, Encryption.**

1. Introduction

The security mechanism without the key exchange (symmetric or asymmetric) is yet to be an area of exploration. In this paper we put an effort in designing such a mechanism that can be applied in wireless sensor network (WSN) for reliable data transfer. Due to the nature of air medium, wireless connectivity is vulnerable to attacker as it is easy to listen or capture the messages that propagate through. Therefore, encryption is a vital part to hide the data from attacks [3]. Our aim is to construct a security protocol that consists of:

- *Initial Encryption*: To add the random noise to the original data message using the LCG generated pseudo random number.
- *Final Encryption*: Initial encrypted message is multiplied with the orthogonal set of rotation matrices.

There are popular encryption (symmetric and asymmetric) and hashing function schemes that are used for the purpose of encryption/decryption. Examples include RC5, MD5, RSA, DES, SHA1 and so and so forth. Many existing security protocols of WSN are using some of these schemes.

In this paper, we contemplate a different design of WSN security for reliable message percolation. We are convinced by the fact that a light weight security mechanism can notably reduce the overhead. By changing the angle of rotation matrices and adding the random noise generated by LCG to sensor data messages, we believe that our proposed cipher is secure enough for WSNs.

Lightweight secure protocol for resource-constrained WSN is challenging and much works are going on in designing storage and computationally inexpensive mechanism [1], [2], [3]. We consider some important issues in engineering our security protocol. Firstly, key storage for individual sensor node needs to be reasonably small. For example, if there are N nodes in the network, then we cannot expect that a node can store $N - 1$ keys to share a secrete key with each of the other nodes. Secondly, in case where quite a good amount of sensor nodes are compromised by an adversary, the communications among other nodes should still be secure. Forward secrecy (nodes leaving the group should not have access to any future keys) and backward secrecy (new nodes joining the group should not have access to any old keys) must be maintained to devise a stalwart network. Thirdly, it should be ensured that both local and global connectivity is maintained. A sensor node should be able to securely communicate with its local neighbors (i.e., sensor physically located within transmission range). Connectivity among local zones should provide global network connectivity [4]. Finally, asymmetric cryptography to WSN is too expensive, because they require expensive computations and long messages that might easily exhaust the sensor's resources [5]. That's why we take symmetric cryptographic operations and spread the load across network in a distributed fashion.

The rest of this article is organized as follows. We make assumptions and define network topology in Section 2. Section 3 describes our approach in details. We briefly analyze our scheme in Section 4 and Section 5 concludes this article.

2. Network Topology and Assumptions

Grouping or Clustering is a good approach to alleviate the scalability problem and to simplify the overall network structure [4], [6]. We adopt a graph theoretic approach to assume our network topology. In [6], a practical deployment has been developed where they have shown that sensor can be deployed in groups and there is a high probability that sensors in the same group are close to each other. Keeping this fact, we design our network model where group based secure data aggregation is possible. We describe our network topology and assumptions based on fig. 1.

The edges covered by one vertex in a vertex cover are the edges incident to it and they form a star [7]. The vertex cover problem can be described as covering the edge set with the

This work was supported by MIC and ITRC project.

fewest stars. In wireless sensor network, our interest is to cover the vertex set with fewest stars possible. Keeping this goal, we design our network model as a heterogeneous network, where three types of entities are present; Sink/Base Station (BS), Group Leader (GL), and ordinary Sensor Nodes (SN).

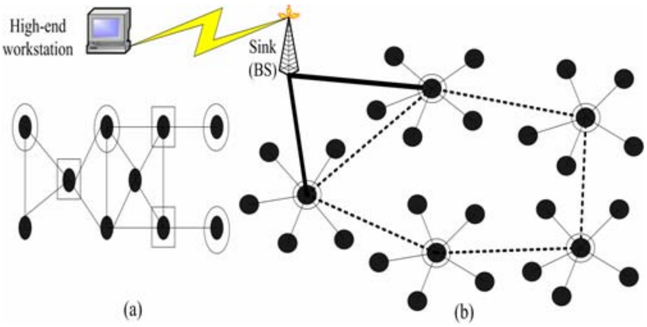

Figure 1. (a) Minimal cluster set (circles) and minimum cluster set (squares). (b) Proposed network model (circles as stars) for our scheme.

We assume that SN is simple, inexpensive and stringent in resources (power, memory and computation), while GL is rich is resources and more compromise-tolerant and having transmission range more than $2R_{SN}$, where R_{SN} is the transmission range of an ordinary sensor node. We also assume that one GL can communicate with its neighbor GL to forward aggregated messages towards sink (Base Station). There is no communication link among SNs within one group and between SNs in different group Fig. 1(b). We assume that once the sensors are dispersed over the area of interest, they remain relatively static. We consider the sensors in the whole network as a graph $G = (V, E)$, where V is the set of sensors in the network and E is the set of direct communication links. A direct communication link is present between SNs and its corresponding GLs if and only if they are within the transmission range of one another. In fact, it is easy to see that each group leader (or vertex) in fig.1b is at the center of a star. Thus for each group leader in overall network, we have one star where all the other nodes in the star are just one hop apart.

3. Our Approach

Sensory data is aggregated locally by the nodes that are under one group. Each sensor node sends its sensed data to its leader encrypted based on LCG [8], [9] and orthogonal rotation matrices [10]. Group leader's responsibility is to forward the aggregated data to the base station via other group leaders (multi-hop) on its way. Final verification is performed by the base station only. Initial encryption is performed using LCG generated random number and final encryption is performed using the orthogonal rotation matrices (based on angle rotation). We describe these two step encryption process in the following sections.

3.1 Initial Encryption (LCG based data encryption): The linear congruential generator consists of the following four numbers:

- m, the modulus, $m > 0$
- a, the multiplier, $0 \leq a \leq m$
- c, the increment, $0 \leq c \leq m$
- S_0, the seed, $0 \leq S_0 \leq m$

from which a sequence of random numbers $< S_n >$, $n \geq 0$ can be generated by setting

$$S_n = (aS_{n-1} + c) \bmod m$$

These numbers should be chosen in such a way, that the random number stream provides a long cycle time and has good statistical properties (Statistical randomness). Plumstead and Boyer in [11] and D.E. Knuth in [8] have shown that it is easy to decipher the LCG unless it is designed with good parameters that provide statistical randomness. We adopt Hull and Dobell's idea [9] to provide statistical randomness on LCG. According to their theory, the linear congruential sequence S_0, S_1, S_2, S_3,…..generated by

$$S_n = (aS_{n-1} + c) \bmod m$$

has a period of length m and provides maximal statistical randomness if the following conditions hold:

1. gcd (b, m) = 1: b is relatively prime to m.
2. p/(a-1), for every prime p such that p/m: if p is a prime number that divides m, then p divides (a-1)
3. If m is divisible by 4, then (a-1) is divisible by 4.

The seed S_0 is the only secret that needs to be shared, other parameters a, c and m can be public as Plumstead's testing algorithm discovered the fact that the system won't be more secure if we keep all of them secret. Therefore, initial encryption with the secret seed S_0, our target is to scramble this secret in such a way so that we can hide all the random numbers from the attacker to defend chosen-plaintext attack. Initial encryption is performed by ordinary sensor node (SN) in three steps described below (fig. 2).

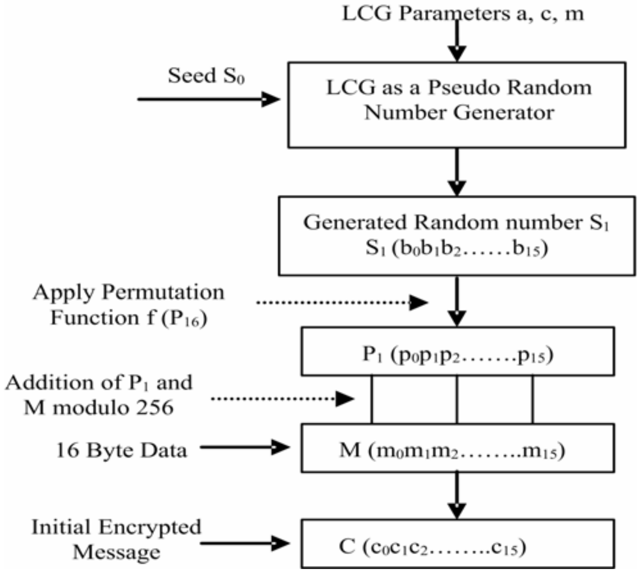
LCG Parameters a, c, m
Seed S₀
LCG as a Pseudo Random Number Generator
Generated Random number S₁
S₁ (b₀b₁b₂……b₁₅)
Apply Permutation Function f (P₁₆)
P₁ (p₀p₁p₂…….p₁₅)
Addition of P₁ and M modulo 256
16 Byte Data
M (m₀m₁m₂……..m₁₅)
Initial Encrypted Message
C (c₀c₁c₂……..c₁₅)

Figure 2. Initial data encryption using LCG generated random number

Step 1: LCG based pseudo random number generation: For initial encryption of 16 byte data (plaintext), we generate 16 byte random number S_1.

Step 2: We apply permutation function f (P) on S_1. S_1 is split into 16 1 byte random number $b_0b_1b_2\ldots\ldots b_{15}$ respectively. A permutation function is defined as follows:

$$f(P_k) = p_0p_1p_2\ldots\ldots p_{15}, \qquad 0 \le k \le 15$$

where, $p_0 = b_0$ mod 16 and $p_k = b_k$ mod 16 for k = 1,2,….,15.

Step 3: The data is encrypted with the permuted values by simply addition modulo 256 operations.

$$C_i = p_i + m_i \pmod{256}, \qquad i = 0,1,2,...,15.$$

C_i is the encrypted message that is to be put as input to the final encryption using orthogonal matrices.

3.2 Final Encryption (Based on orthogonal matrices): We use the property of orthogonal set of rotation matrices to encrypt the initial encrypted data. Orthogonal transformations correspond to and may be represented using orthogonal matrices. The set of orthonormal transformations forms the orthogonal group, and an orthonormal transformation can be realized by an orthogonal matrix. Data encryption can be performed by orthogonal matrices if the sender and receiver are agreed on chosen rotation angles of matrices. The orthogonal ration matrices can be defined as the matrices that are composed of 2-dimensional sub-matrices ordered along he main diagonal, while all other entries are null. Therefore, an orthogonal matrix Q_i with dimension D = 2n is represented in a pseudo diagonal form [12] by the following equation:

$$Q_i = diagonal\left[\begin{pmatrix} \cos\theta_{i1} & sen\theta_{i1} \\ -sen\theta_{i1} & \cos\theta_{i1} \end{pmatrix}, \begin{pmatrix} \cos\theta_{i2} & sen\theta_{i2} \\ -sen\theta_{i2} & \cos\theta_{i2} \end{pmatrix}, \ldots, \begin{pmatrix} \cos\theta_{in} & sen\theta_{in} \\ -sen\theta_{in} & \cos\theta_{in} \end{pmatrix}\right]$$

Property of orthogonality preserves the equality between the transpose and its inverse, $Q_i^{-1} = Q_i^T$ and $Q^TQ = I$ (Identity matrix). More simply, an orthogonal matrix can be represented by a vector defining the rotation angles of each sub-matrix of the main diagonal of Q_i, as

$$\overline{\theta_i} = (\theta_{i1}, \theta_{i2} \ldots, \theta_{in})$$

To encrypt the data C_i (that is initially encrypted by SN using LCG), the orthogonal matrices hold by each SN and corresponding GL will be Q_i and Q_i^c, where $Q_i \cdot Q_i^c = I$ (identity matrix), where Q_i^c is the complementary matrix of Q_i. The final encryption and message exchange between a SN and GL are performed as described below.

Step1: $C_{SNi} = C_i \cdot Q_{SNi}$: Represents the n-dimensional rotation of data vector using the rotation matrix Q_{SNi}.

Step2: $C_{GL} = C_{SNi} \cdot Q_{GL}$: Original information is rotated by two distinct and independent matrices.

Step3: $C_{SNi} = C_{GL} \cdot Q^c_{SNi} = C_i \cdot Q_{GL}$: Sensor node SN removes her rotation by one complementary rotation matrix.

Finally group leader, GL can recover the information by applying her complementary rotation matrix O^c_{GL}. Each SN and corresponding GL must choose rotation angles (encryption key here) for the matrices Q_i in a random manner. This way GL can aggregate sensory data from each individual SN and aggregated data verified by GL can be forwarded to the sink (BS). To forward the data, GL can encrypt and send via intermediate forwarding GLs. The GL and base station should also choose the rotation angles. Thus, receiving the aggregated data from GL, base station can verify the confidentiality. Sensory data is collected from local groups in a 3-way handshake so that each individual SN can verify that it has sent the identical data to its group leader.

4. Analysis

Adversary can track the original information sent by GL if he captures the angle of rotation matrices. To further eliminate this problem, group leader can add a random number generated from LCG when aggregated data is encrypted using rotation matrices. In case of local data aggregation, even if the adversary knows the rotation angles between SN and corresponding GL, he won't be able to infer the message as data is scrambled in initial encryption based on LCG generated random noise. Moreover, suppose a single message is successfully eavesdropped and broken, the angles and the random number can be modified for the remaining each new messages. So, the whole scheme is unlikely to be fully compromised by the adversary as the number of possibilities to check the consecutive messages is the same.

According to the permutation function in LCG based encryption, one permutation function corresponds to 256^{16} / 16! = 2^{84} values for one 16 byte pseudo random number. Therefore, it is not feasible for an adversary to search the possible values of 16 byte random number.

Decryption is straightforward in this scheme. Sensor nodes and corresponding group leaders choose rotation angles and can obtain the same LCG parameter a, m and c and the seed S_0 through key distribution protocol. Therefore, receiver and sender can generate the same angle and LCG based generated random number (S_1 in our proposed scheme). And based on S_1 same permutation function can be recovered. So, first using angle, receiver can obtain initial encrypted message and using LCG parameter receiver can recover original message that was sent by the ordinary sensor nodes.

Further investigation on some important issues need to be explored. How the authenticity can be ensured, how the modeling of our assumed network can be realized and what is the computational complexity for individual sensor nodes and group leader, are possible research issues. At present we are developing these issues to effectively design our protocol.

5. Conclusions

We devise a stalwart security protocol for wireless sensor networks to achieve confidentially for sensory data by exploiting the random noise (generated by LCG) and orthogonal set of rotation matrices. Local sensed data is aggregated maintaining message privacy and transmitted via group leaders over the channel towards the base station. The proposed scheme's security level depends on the statistical randomness of LCG generated pseudo random number and the angle of orthogonal rotation matrices.

REFERENCES

[1] Karlof, C. and Wagner, D., “Secure routing in wireless sensor networks: Attacks and countermeasures”, Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci " Wireless sensor networks: a survey”, Computer Networks 38 (2002), Elsevier Science B.V., pp.393–422.

[3] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, Wireless Sensor Network Security: A Survey, 2006 Auerbach Publications, CRC Press.

[4] Y.P. Chen and A. L. Liestman, “A Zonal Algorithm for Clustering Ad Hoc Networks”, International Journal of Foundations of Computer Science. 14(2):305-322, April 2003.

[5] A. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1996.

[6] Donggang Liu, Peng Ning, and Wenliang Du. Group-Based Key Pre-Distribution in Wireless Sensor Networks. In Proc. ACM WiSE’05, September 2, 2005.

[7] Douglas B. West, Introduction to Graph Theory, August 23, 2000, 2nd Edition

[8] D.E. Knuth, Deciphering a Linear Congruential Encryption. IEEE Transactions on Information Theory, Vol. IT-X, no. 1, January 1985, pp.49–52.

[9] D.E. Knuth, The Art of Computer Programming, Vol 2: Seminumerical Algorithms, Addison-Wesley, 1969.

[10] I. Ingemarsson, "Commutative Group Codes for the Gaussian Channel", IEEE Transactions on Information Theory, vol. IT-19, no. 5, pp. 215-219, March 1973.

[11] J.P. Plumstead (Boyar), Inferring a sequence generated by a linear congruence, in: Proceedings of the 23rd Annual IEEE Symposium on the Foundations of Computer Science, 1982, pp. 153–159.

[12] E. Biglieri and M. Elia, “Signal Sets Generated by Groups", The Information Theory Approach to Communications, Ed. G. Longo, Springer, 1977, pp. 263-306.