



Aggregation of Encrypted Data using a Secure Paillier Key in Wireless Sensor Networks

Antony Xavier Branson^{1,*}, Sai Shanmuga Raja², S.GEETHA¹, T. Kirubadevi¹, N. Kanya³,

¹Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute, Chennai- 600095, Tamil Nadu, India.

²Department of Computer Science and Engineering, Shanmuganathan Engineering College, Pudukkottai District, Tamil Nadu, India.

³Associate Professor, Department of Information Technology, Dr. M. G. R. Educational and Research Institute,

Chennai- 600095, Tamil Nadu, India.

antony.cse@drmgrdu.ac.in

Abstract.

In wireless sensor networks, data aggregation is a critical strategy for energy conservation. Compromised aggregators, on the other hand, might provide fake results and attempt to steal data from the system. Several data-gathering strategies are using wireless sensor networks, each with its drawbacks. It is proposed SPAED (Secure Paillier key-based encrypted data aggregation). SPAED encrypts data using homomorphic encryption. Data is encrypted using the Paillier key. Before authentication, the source data is decrypted. In comparison to other asymmetric systems, SPAED provides a high-level of security upon this aggregated result while consuming the least energy.

Keywords: Encrypted Data, Secure Paillier Key, Sensor Network, Homomorphism Encryption, simulation.

DOI Number: 10.14704/nq.2022.20.8.NQ44224

NeuroQuantology 2022 ;20(8):2050-2055

1.

Introduction

WSNs are made up of millions of tiny electronic devices. Sensor nodes communicate via wireless channels, ensuring data transmission and reception between sensors in Wireless Sensor Networks (WSNs) [1]. WSNs and other new technologies suffer from resource constraints such as power supply, memory storage, processing speed, communication bandwidth, and storage memory capacity [2]. WSNs enable previously impractical uses. Numerous applications have emerged due to the miniaturisation of MEMS (Micro-

electromechanical Systems) and the use of networking-based technology. Additionally, the Paillier function [3] is used to encrypt data delivered towards the base station at the node level prior to its aggregation [4].

A group is an arrangement of sensor nodes that share sensory data such as temperature and pressure [5]. These concerns were emphasised for members who seem to have safe access to group information. Multiple groups and rekeying are possible with such a scheme [6]. Quantum cryptography protects network communications by encoding data in



the form of a polarised photon that could be transmitted via the air. [7] described a method to merge quantum cryptography & IEEE 802.11 wireless network security.

WSN cluster hierarchy architecture (i.e. LEACHES) has been proposed. This proposal is part of a larger solution known as SOOA (Secure Object-Oriented Architecture) for Wireless Sensor Networks (SOOAWSN) [8]. Unlocking post-distribution security services with a key management approach. TinyOS were used for development and testing. This approach is suitable for WSNs with hundreds of nodes [9].

To embed data, the adjacent pixels are selected for the random groups and reversibly embedded into the image [10]. It is composed of a pixel and several host pixels. Prior to the encryption of MCGs, the reference pixels' least significant bits (LSBs) are reset. Privacy homomorphic encryption (PH) is dependent on SEDA-ECC & divide-and-conquer [11]. To obtain

an aggregated subtree result, the tree was divided into 3 subtrees having equivalent sizes using an aggregation tree disjoint approach [12]. The poor deployment environment of trust sensing-based secure routing techniques, along with limited energy has a serious impact on typical network attacks [13].

2. Secure Paillier Key Based Data Aggregation

Homomorphic encryption enables certain computations using ciphertexts that produce an encrypted version identical to the plaintext result. Modern communication system architectures seek this feature. Many existing algorithms are homomorphic [14]. This is the Paillier encryption scheme. Table 1 and 2 shows the Paillier encryption and signature scheme. SPAED aims to ensure data integrity, SPAED uses public-private key pairs. The SPAED algorithm has four phases.

Table . Paillier’s encryption scheme

Table 1: Paillier’s encryption scheme

Setup	<p>RSA algorithm $n = pq$</p> <p>Set $\lambda = lcm(p-1, q-1)$</p> <p>select $g \in \mathbb{Z}_n^*$ such that $n \parallel ord_n(g)$</p> <p>publish n, g and keep λ in secret.</p>
Encryption	<p>Compute the ciphertext</p> $C = g^m r^n \bmod n^2$
Decryption	$m = \left(\frac{c^\lambda - 1 \bmod n^2}{n} \right) / \left(\frac{g^\lambda - 1 \bmod n^2}{n} \right) \bmod n$

Table 2. Paillier’s signature scheme



Table 2: Paillier's signature scheme

Setup	RSA algorithm $n = pq$ Set $\lambda = lcm(p-1, q-1)$ select $g \in \mathbb{Z}_n^*$ such that $n \parallel ord_n(g)$ publish n, g and keep λ in secret.
Signing	$s_1 < -\rho\left(\frac{H(m)^t - \text{mod } n^2}{n}\right) \text{mod } n$ $s_2 < -((H(m)g^{-s_1})^t \text{mod } n)$ Signature (m, s_1, s_2)
verification	$H(m) = g^{s_1} s_2^n \text{mod } n^2$

2052

• **Generate Phase for Key**

Consider the collection of elliptic curve points which constitute the cyclic group as E, with $ord(E) = n = q_1q_2q_3$. Three random points (r_1, r_2, r_3) are chosen at random from E. $P = q_2q_3 * r_1$, $Q = q_1q_2 * r_2$, and $H = q_1q_2 * r_3$, with P, Q, and H in the sequence q_1, q_2 , and q_3 , respectively.

• **Encryption**

The amount of space required in a sensor node for a message M is determined by $M_i \in \{0, 1, \dots, TM\}$, where I denotes network nodes. A random sensor $r_{ai} \in \{0, 1, \dots, n-1\}$ encrypts the data M_i using the public key in the network. Cipher text $C_i = M_i * P + Q + r_{ai} * H$, whereas + denotes the addition of elliptic curve points and * denotes the multiplication of elliptic curve scalars given in equation 1.

Phase:

This phase combines the encrypted messages. The gathering is done via ciphertext.

$$C_{ia} = \left(\sum_{j=1}^k M_{ij}\right) * P + \zeta_i * Q + \left(\sum_{j=1}^k r_{aj}\right) * H \tag{1}$$

Decryption:

The base station can decrypt the aggregated result M_i from the ciphertext during decryption given in equation 2.

$$M_1 = \sum M_{ij} = \log_{g_p}(q_2q_3 * c_i) \tag{2}$$



Finally, the data's integrity is verified using aggregated results.

- **Performance Review**

Performance of existing system E_TT compared to proposed NKM_TT system using simulation results. Table 1 depicts 50 nodes randomly placed in a 1000x1000m area. Simulations are used to compare packet delivery, packet loss, delay, and throughput rates.

Table 3. Parameters for simulation

Parameter name	Value of parameter
Time of Simulation	30
Nodes Number	50
Routing Protocol	SPAED and SEDA-ECC
Traffic Model	CBR
Simulation Area	1000x1000
Range of Transmission	250
Type of Antenna	Omni
Type of Network Interface	WirelessPHY
Type of Channel	Wireless

- **Packet Rate**

Packet delivery rate is defined as the ratio of all packets sent to all packets received in a network. It is given by equation 3 below, where n is the network's node count.

2053

$$PDR = \frac{\sum_0^n PktsReceived}{time} \tag{3}$$

- **Packet Received Rate**

Fig.1. Packet Receipt Rate versus Simulation Time in Seconds.

The proposed scheme's PDR is shown in Fig.1. SPAED is higher than PDR for SEDA-ECC.

- **Packet Loss**

Packet Loss Rate is the ratio of lost packets while sending to receivers as shown in equation 4, where the network's node count is n.

$$PLR = \frac{\sum_0^n PktsLost}{time} \tag{4}$$

Fig.2. Rate of Packet Loss versus Simulation Time in Seconds.



Total loss of packet of SEDA-ECC and SPAED are compared in Figure 2. High-security routing has reduced packet loss.

- **Mean Delay**

The time difference between average delay sending and receiving packets. It is given by equation 5, where n is the network's node count.

$$Delay = \frac{\sum_0^n (PktRecvTime - PktSentTime)}{n} \quad (5)$$

Fig. 3. Delay Average versus Simulation Time in Seconds.

The estimated average delay for the proposed approach SPAED vs the actual system SEDA-ECC is shown in Figure 3. The greater the network's throughput, the lesser the latency.

2054

- **Throughput**

The total number of successfully received packets is called Throughput. The average throughput is calculated using equation 6, where n is the network's node count.

$$Throughput = \frac{\sum_0^n Pkts\ Received(n) * Pkt\ Size}{1000} \quad (6)$$

Fig. 4. Throughput

Figure 4 shows that SPAED has a higher average throughput than SEDA-ECC. The security activity boosted network performance.

- **Residual Energy**

The amount of energy is called residual energy which was left in the node at the moment. Figure 5 shows the residual energy graph.

Fig. 5. Residual Energy versus Simulation Time in Seconds.

Figure 5 shows that SPEAD uses less energy and thus has more residual energy than the existing scheme.

- **Conclusion**

WSNs struggle to provide hierarchical data aggregation without data loss. WSNs propose secure Paillier key-based encryption aggregation. SPAED uses homomorphic encryption. The paillier key encrypts data. The source data is decrypted before authentication.

Compared to other asymmetric schemes, upon that aggregated result, SPAED does have the high-level of security with the least amount of energy use.

- **References**

- Aziz Nor Azlina Ab., Aziz Kamarulzaman Ab., and Ismail Wan Zakiah wan,



"Coverage Strategies for Wireless Sensor Networks," World Academy of Sciences, Engineering and Technology, vol. 26, no. 0026:2009, pp. 145-150, February 2009.

- Chen, Z., Wang, J., Zhang, Z., & Xinxia, S. (2014). A fully homomorphic encryption scheme with better key size. *China Communications*, 11(9), 82-92.
- D. Choi, S. Choi, and D. Won, "Paillier's cryptosystem revisited," in Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS'01), pp. 206-214, Philadelphia, Pennsylvania, USA, Nov. 2001.
- Tristan Daladier Engouang, YUN LIU, and Zhen-jian Zhang, "Aggregate over Multi-hop Homomorphic Encrypted Data in Wireless sensor networks," in 2014 2nd International Conference on Electrical, Control and Computer Engineering, vol. 1, Taiyuan, 2014, pp. 1-5.
- Chen, Z., Wang, J., Zhang, Z., & Xinxia, S. (2014). A fully homomorphic encryption scheme with better key size. *China Communications*, 11(9), 82-92.
- Jyothi Metan, K. N. Narasimhamurthy (2015) group key management technique based on logic key tree in the field of wireless sensor network, *international journal of computer applications*, Vol.117, No.12, pp. 9-15.
- Priyanka Bhatia and ronaksumbaly (2014) framework for wireless network security using quantum cryptography, *International journal of computer science and engineering*, Vol.2, No.27, pp.1-17.
- Mohammed A. Abuhelaleh, Khaled M. Elleithy (2010) security in wireless sensor networks: key management module in SOOAWSN, *international journal of network security & its applications*, Vol.2, No.4, pp. 67-78.
- Alibagherinia, Akbarbemana, Sohrabhojjatkah, Alijougharpour (2014) A key management approach for wireless sensor networks, *International journal of information technology, modeling and computing* Vol.2, No.3, pp.1-9.
- Lin, Y. H., Chang, S. Y., & Sun, H. M. (2013). CDAMA: concealed data aggregation scheme for multiple applications in wireless sensor networks. *IEEE Transactions on Knowledge and Data Engineering*, 25(7), 1471-1483.
- Smart, N. P., & Vercauteren, F. (2010, May). Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In *Public Key Cryptography* (Vol. 6056, pp. 420-443).
- Zhou, Q., Yang, G., & He, L. (2014). A secure-enhanced data aggregation based on ECC in wireless sensor networks. *Sensors*, 14(4), 6701-6721.
- Qin, D., Yang, S., Jia, S., Zhang, Y., Ma, J., & Ding, Q. (2017). Research on Trust Sensing based Secure Routing Mechanism for Wireless Sensor Network. *IEEE Access*.
- Lin, R. L., Wang, J., & Du, H. (2013). Improved fully homomorphic encryption over integers. *Jisuanji Yingyong Yanjiu*, 30(5), 1515-1519.

