Sensor Review

Secured data aggregation in wireless sensor networks

Sathya D., Ganesh Kumar P.,

Article information:

Secured data aggregation in wireless sensor networks

Sathya D.
Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, India, and
Ganesh Kumar P.
Department of Information Technology, Anna University, Regional Campus, Coimbatore, India

Abstract

Purpose – This study aims to provide a secured data aggregation with reduced energy consumption in WSN. Data aggregation is the process of reducing communication overhead in wireless sensor networks (WSNs). Presently, securing data aggregation is an important research issue in WSNs due to two facts: sensor nodes deployed in the sensitive and open environment are easily targeted by adversaries, and the leakage of aggregated data causes damage in the networks, and these data cannot be retrieved in a short span of time. Most of the traditional cryptographic algorithms provide security for data aggregation, but they do not reduce energy consumption.

Design/methodology/approach – Nowadays, the homomorphic cryptosystem is used widely to provide security with low energy consumption, as the aggregation is performed on the ciphertext without decryption at the cluster head. In the present paper, the Paillier additive homomorphic cryptosystem and Boneh *et al.*'s aggregate signature method are used to encrypt and to verify aggregate data at the base station.

Findings – The combination of the two algorithms reduces computation time and energy consumption when compared with the state-of-the-art techniques.

Practical implications – The secured data aggregation is useful in health-related applications, military applications, etc.

Originality/value – The new combination of encryption and signature methods provides confidentiality and integrity. In addition, it consumes less computation time and energy consumption than existing methods.

Keywords Sensors, Wireless sensor networks, Sensor networks, Data aggregation, Aggregate digital signature, End-to-end encryption, Paillier homomorphic cryptosystem

Paper type Research paper

1. Introduction

A wireless sensor network (WSN) is deployed in an open and sensitive environment like health monitoring, military surveillance, industrial monitoring, landslide detection and so on. It consists mainly of two types of nodes: sensor nodes and sink nodes. The sensor nodes are similar to that of a small computer, but they have limited processing capability, memory and battery power. Due to the resource constraint nature of sensor nodes, the direct transmission of raw data from the sensor nodes to the sink nodes consumes more energy and leads to a lot of congestion in the network.

To reduce energy consumption, data aggregation is introduced in a WSN, as shown in Figure 1. More powerful sensor nodes act like aggregators (cluster head) or, in some cases, regular nodes act as aggregators (Castelluccia *et al.*, 2009). These aggregators collect and process the data coming from the other sensor nodes of the network. For example, the aggregation functions like sum, min and max are useful in calculating temperature readings. The aggregator collects the data from n sensor nodes, calculates the sum of all n values and forwards it to the sink node. The sink node, after receiving the sum value, calculates the average temperature by dividing the value by n. The data aggregation saves the energy of sensor nodes and, thereby, increases the lifetime of the network (Papadopoulos *et al.*, 2012).

Security of data aggregation is a challenging task in WSNs. False aggregation may lead to a large damage in the sensor network. For example, in the case of health-related applications, the attacks on sensor nodes may affect the person's life, and in the case of military applications, it may lead to a national security threat. Various attacks like node compromise attack, eavesdropping, collision attack, Sybil attack, blackhole attack, sinkhole attack, selective message forwarding and attacks on data aggregation occur. (Xing *et al.*, 2005). So, the secure data aggregation needs the following key properties: confidentiality, integrity, authentication and freshness of data (Papadopoulos *et al.*, 2012).

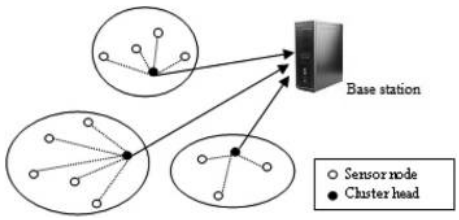
The objective of the present study on *S*ecured *D*ata *A*ggregation (SDA) in WSNs is to securely transmit the aggregated data to the base station by reducing the energy consumption of sensor networks. The Paillier additive homomorphic cryptosystem is used to encrypt the data, and Boneh *et al.*'s aggregate signature method is used to generate the signature at each sensor node (Boneh *et al.*, 2003). The

The current issue and full text archive of this journal is available on Emerald Insight at: **www.emeraldinsight.com/0260-2288.htm**

Sensor Review
 [ISSN 0260-2288]
[DOI 10.1108/SR-06-2017-0103]

Received 11 June 2017
Revised 23 August 2017
18 November 2017
Accepted 11 January 2018

Figure 1 Data aggregation in WSNs



sensor node transmits the encrypted data to its cluster head along with a digital signature. The cluster head aggregates the encrypted data and digital signature and sends them to the next higher-level cluster head or base station which provides end-to-end confidentiality. Experimental results demonstrate the efficiency of the proposed system in comparison with similar approaches.

The remaining part of the paper is organized as follows: Section 2 gives a brief overview of the literature related to the study. Section 3 presents background details of homomorphic encryption and verification schemes. Section 4 illustrates preliminaries on key distribution and network structure, the Paillier cryptosystem and Boneh *et al.*'s signature scheme. Section 5 presents the proposed system in detail. Section 6 explains experimental results. Finally, Section 7 gives the conclusion.

2. Related works

A variety of security methods have been proposed for securing data aggregation. All these methods concentrate on satisfying security properties and overcoming various attacks. The Secure In-network processing of Exact Sum queries (SIES) method provides both integrity and confidentiality for the aggregation functions like sum, count, average, standard deviation, variance and Q-quantile queries (Papadopoulos *et al.*, 2012). It combines the symmetric additive homomorphic encryption method with secret sharing to protect the individual readings, and the Rivest–Shamir–Adleman (RSA) digital signature algorithm has been used to identify the malicious sensors. Nevertheless, the method does not address passive denial-of-service attacks and an access control in the base station.

An efficient and provably secure aggregation of encrypted data in WSNs uses an additively homomorphic cryptosystem to encrypt the data (Castelluccia *et al.*, 2009). A set of three values (encrypted data, hdr and checksum) is sent to the sink node, where hdr (header) indicates the IDs of all reporting nodes and checksum checks the integrity of the message. To avoid the node exclusion attack of hdr, each node generates a Message Authentication Code (MAC) tag. The sink regenerates the tag and accepts hdr if and only if the result matches the tag. The strength of the method is that an indistinguishable Pseudorrandom Function is used to generate keys. However, there are a few drawbacks of the method like MAC (hdr) increases computation cost and the group key is used for checksum where the violation of group key on any node would completely compromise all the other nodes in the network.

Secure End-to-End Data Aggregation (SEEDA) uses an additive homomorphic encryption to secure the data aggregation (Poornima and Amberker, 2010). Each node ciphertexts the message using a secret key and it is sent to the next higher-level nodes h-1. The h-1 nodes add the received ciphertext of responding nodes to the ciphertext of non-responding nodes assumed to be zero. The aggregated data, along with the count value of non-responding nodes, are sent to the next higher-level nodes h-2. Finally, the sink node decrypts the message and calculates the average based on the count value. The advantage of the method is that it combines the best feature of hop-by-hop and end-to-end data encryption. Moreover, the method does not consider any verification protocol to prove data authentication.

Recoverable concealed data aggregation (RCDA) uses Mykletun *et al.*'s aggregate encryption method and Boneh *et al.*'s aggregate signature method (Chen *et al.*, 2012; Mykletun *et al.*, 2006; Boneh *et al.*, 2003) to secure the data aggregation. Mykletun *et al.*'s method is an additive homomorphic encryption from which the base station can obtain the sum of all the generated data from sensor nodes in the network. RCDA uses a new encoding method by which the base station can obtain individual data of each sensor node. One of the weaknesses of the method is that when the cluster head gets compromised, all the data belonging to its cluster group would be exposed to intruders.

3. Preliminaries

Numerous methods have been proposed to secure data aggregation in WSNs (Jha and Sharma, 2011; Chen *et al.*, 2009). All the security methods would come under either of these two groups: secure data aggregation using plaintext-based method or ciphertext-based method. The main advantage of the ciphertext-based method is that it reduces transmission overhead and, at the same time, it maintains end-to-end confidentiality. The best among ciphertext-based methods is homomorphic encryption, and so, SDA uses homomorphic encryption.

Homomorphic encryption performs operation on ciphertext, which generates an encrypted result. When an encrypted result is decrypted, it matches the results of the operations performed on plaintext. Each node in a sensor network encrypts the raw data and sends them to the next higher-level node or base station. The higher-level node performs computation on the ciphertext received and forwards it to the next higher-level node. This type of computation continues until it reaches the base station. Finally, the base station decrypts the ciphertext which yields the result of operations performed on the plaintext. The Paillier homomorphic cryptosystem is chosen as the best one among many conventional homomorphic encryption methods and used in SDA, as its encryption cost is less (Sen, 2013). The decryption process is heavier for the Paillier, and it is done only on the server end, hence it is ignored.

A WSN uses broadcast communication to transmit any message in the network. So, the messages have to be authenticated properly before transmission on the network to address the data vulnerability (Rajeswari and Seenivasagam, 2016). As a WSN is a resource constraint network, the energy

consumption needs to be reduced for calculating the authentication protocol. The aggregate signature method is a digital signature that is used to verify the signature of multiple users simultaneously in a single short signature, which reduces energy consumption (Boneh *et al.*, 2003). In SDA, Boneh *et al.*'s aggregate signature method is used for authentication, which withstands node compromise attack and reduces verification delay.

In the recent research studies (Gaubatz *et al.*, 2005; Baek *et al.*, 2008), (Liu *et al.*, 2010), it has been proved that asymmetric key cryptography is feasible to WSNs when a proper algorithm is chosen to provide security. So, SDA uses the asymmetric key encryption and signature methods with different sets of keys for the signature and encryption processes. All these key values are stored in every sensor node. The base station generates all these key values to reduce energy consumption of sensor nodes.

In SDA, the cluster-based method of hierarchical network organization is followed to send the aggregated result to the base station (Fasolo *et al.*, 2007). In this method, the end-to-end encryption is followed, where the raw data from the sensors are forwarded to the cluster head. The cluster head performs homomorphic encryption on the ciphertexts and transmits the aggregate value to the base station, which reduces transmission overhead and saves the energy of the network (Pandey *et al.*, 2010).

4. Algorithms

4.1 Paillier cryptosystem

The Paillier cryptosystem is an additive homomorphic cryptosystem where only on giving the public key and the encryption of m1 and m2, the receiver can compute the value of m1 + m2 (Yi *et al.*, 2015, Sen, 2013).

4.1.1 Algorithm

4.1.1.1 Key generation

- Pick two large prime numbers p and q randomly and independent of each other such that gcd(pq, $(p-1)(q-1)$) = 1. This property will be assured if both the primes are of equal length.
- Compute n = pq and λ = 1cm(p – 1, q – 1).
- Select random integer g where g ε $Z^{*}{}_{n}{}^{2}$.

Make sure that n divides the order of g by checking the existence of the following modular multiplicative inverse: $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$, where function L is defined as L(u) = (u – 1)/n.

Note: The notation a/b denotes the quotient of a divided by b, i.e. the largest integer value v $\geq$ 0 to satisfy the relation a $\geq$ vb:

- The public (encryption) key is (n, g).
- The private (decryption) key is (λ, μ).

If using p, q of equivalent length, a simpler variant of the above key generation steps would be to set $g = n + 1$, $\lambda = \Phi(n)$, $\mu = \Phi(n)^{-1} \bmod n$, where: $\phi(n) = (p-1)(q-1)$.

4.1.1.2 Encryption

- Let m be a message to be encrypted where m ε $Z_{n.}$
- Select random r where r ε Z_n^*.
- Compute ciphertext as: $c = g^m r^n \bmod n^2$.

4.1.1.3 Decryption

- Let c be the ciphertext to decrypt where c ε $Z^{*}{}_{n}{}^{2}$.
- Compute the plaintext message as: $m = (L(c^{\lambda} \bmod n^2).\ \mu \bmod n)$.

4.1.1.4 Homomorphic properties. As it is additively homomorphic, the encryption function can be obtained in two ways:

1 By decrypting the product of two ciphertexts, the sum of their corresponding plaintexts would be obtained:

$$D\big(E(m_1, r1) \cdot E(m_2, r2) mod\ n^2\ \big) = m_1 + m_2 \bmod n$$

2 The product of a ciphertext with a plaintext raising g would decrypt to the sum of the corresponding plaintexts:

$$D\big(E(m_1, r1) \cdot g^{m2} mod\ n^2\ \big) = m_1 + m_2 \bmod n$$

4.2 Boneh *et al.*'s aggregate signature method

Boneh *et al.*'s aggregate signature is a digital signature method that supports aggregation (Boneh *et al.*, 2003, Chen *et al.*, 2012). It is used to verify the ciphertext C, which is the encryption of a signature on a given message M. It generates the signatures on arbitrary distinct messages $M_i \varepsilon \{0,1\}^*$. Boneh *et al.*'s aggregate signature method is based on bilinear map e_n, which is defined as $e_n = G_1 X G_2 \rightarrow G_T$. In this, G_1, G_2 and G_T are cyclic groups of prime order n. The signature σ_i is an element of G_1. The five steps of the algorithm are detailed below:

1 *Key generation:* The private key x_i is generated by selecting randomly from Z_p. The public key is $v_i \leftarrow G_2$, where $v_i = x_i$ x g_2. Finally, the output is the key pair (x_i, v_i) for entity i.
2 *Signing:* The message m is signed with private key x_i. Compute h = H(M), where hεG_1, generate signature $\sigma = x_i$ x h and return (m,σ).
3 *Verification:* Compute h = H(M) and accept if $e_n(\sigma, g_2) = e_n(h, v_i)$; otherwise, reject.
4 *Aggregation:* Aggregate k signatures $\delta = \{\sigma_1, \ldots\ldots \sigma_k\}$ for messages M = $\{m_1, \ldots\ldots, m_k\}$, where m_i from entity i and σ_i are a signature of m_i.
5 *Aggregate verification:* Generate aggregate signatures $\delta = \{\sigma_1, \ldots\ldots \sigma_k\} = \sum_{i=1}^{n} \sigma_i$, where $\sigma_1, \ldots\ldots \sigma_k \varepsilon G_1$ and public key set $v = \{v_1, \ldots\ldots v_k\}$, $v_i \varepsilon U_i$. Compute $hi \leftarrow$ H(m_i) for 1$\leq$ i $\leq$ k. Accept if e $(\sigma,\ g_2) = \prod_{i=1}^{k}$e (h_i, v_i) holds where e(σ, g_2), e(h_i, v_i)εG_T.

5. Proposed system

The proposed SDA system can be used in a variety of applications where aggregation functions like sum, avg., count, min., max., median and variance are required. For this, forest fire detection is taken as an exemplar. WSNs play an important role in detecting the forest fire. Temperature, humidity, smoke and gas sensors are deployed in the forest to detect abnormal conditions. All these sensors collect the data and send them wirelessly to the cluster head or base station. These data need security because the loss of any data would lead to a large damage in the ecological system. Further, transmitting all the

data to the base station would consume more resources in WSNs. To reduce energy consumption and to provide security, end-to-end encryption is used in SDA.

Average, min, max temperature, humidity, gas and smoke values are the necessary parameters to monitor the forest fire. So, the SDA chooses the Paillier homomorphic encryption, as it is an additive homomorphic encryption method. By using Paillier homomorphic encryption, the sum of the temperature, humidity, smoke and gas values can be calculated. Likewise, from computing sum, other values like avg., min. and max. can be calculated. The SDA uses Boneh *et al.*'s aggregate signature method for authentication.

The data processing at each sensor node is shown in Figure 2. In SDA, the message m generated from each sensor node is encrypted using the Paillier cryptosystem, which generates ciphertext (c). In addition to this, a digital signature is generated from each node (σ). So, the values (c, σ) are sent to the cluster head or to the base station.

5.1 Encryption and decryption method

- Create ciphertext of a message by using the Paillier cryptosystem as $c = g^m r^n \bmod n^2$.
- Decipher the ciphertext and obtain the message m as $(L(c^\lambda \bmod n^2) \cdot \mu \bmod n) = m$. All the source nodes do a similar type of encryption and create a ciphertext which is aggregated by the cluster head.

5.2 Signature form

Signature is generated for each message by using the aggregate signature method as $\sigma = x_i \times h$ and returns (c, σ) to the cluster head.

5.3 Aggregation at cluster head

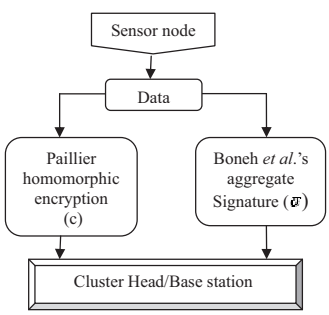
The cluster head receives ciphertexts and signatures as (c_1,σ_1), $(c_2, \sigma_2), \ldots\ldots (c_n, \sigma_n)$ from the sensor nodes $(1, 2, 3, 4, \ldots\ldots n)$, respectively. The cluster head performs aggregation of all the ciphertexts and signatures as given below:

$$c^1 = c_1 \cdot c_2 \ldots\ldots\ldots\ldots c_n$$

$$\sigma = \sum_{i=1}^{n} \sigma_i$$

and sends these parts (c^1, σ_i) to the upper-level cluster head or to the base station. The base station again aggregates the result and verifies the signature to ensure authentication.

Figure 2 Data processing at each sensor node



5.4 Decryption at base station

According to the Paillier homomorphic property, the product of two ciphertexts would lead to a sum of their corresponding plaintexts. Here, the product of $c_1 \cdot c_2 \ldots\ldots\ldots\ldots c_n$ gives the sum of all messages $(m_1, m_2, \ldots m_n)$ for sensor nodes 1,2,.....n:

$$D\Big(E(m_1, r1) \cdot E(m_2, r2) \ldots\ldots\ldots\ldots E(m_n, rn) mod\ n^2\Big)$$
$$= (m_1 + m_2 + \ldots\ldots\ldots\ldots\ldots m_n) \bmod n = m$$

5.5 Verification at base station

Verification is done using Boneh *et al.*'s aggregate signature method. $h_i \leftarrow H(m_i)$ is computed and accepted if $e(\sigma, g_2) = \prod_{i=1}^{k} e(h_i, v_i)$ holds.

In SDA, the Paillier homomorphic encryption provides data confidentiality. Generally, homomorphic encryption performs the aggregation function on the ciphertext itself. So, the keys are not disclosed to the real world even at the cluster heads, which provide an end-to-end encryption leading to confidentiality. The data integrity is also satisfactory because if any of the ciphertext is altered, it would not match the signature at the base station.

6. Experimental results

SDA is implemented using the NetBeans IDE 7.3 over the Intel Lab data set (Papadopoulos *et al.*, 2012). In Intel Lab, the Mica2 Dot sensors with weather boards are used to collect the humidity, temperature, light and voltage values for every 31 s. The Tiny DB in-network query processing system is used to collect the data built on the Tiny OS platform. From the data set, five parameters such as date, time, epoch, mote id and temperature are taken for implementation. The encryption is carried out on the temperature readings.

As of the existing research, the implementation is performed on the computer system with a 2.66 GHz Intel core i5 processor with 4 GB RAM. Although the performance of the CPU is faster than the real sensor nodes, it can be used to demonstrate the performance of the allied methods. The SDA is compared with the existing systems like SIES (Papadopoulos *et al.*, 2012), SEEDA (Poornima and Amberker, 2010) and Efficient and Provably Secure Aggregation (EPSA) of encrypted data in WSNs (Castelluccia *et al.*, 2009).

Figures 3, 4, 5 and 6 show the encryption, decryption, aggregation and the total computation time of the proposed and the existing methods, respectively. A comparison is done

Figure 3 Encryption time

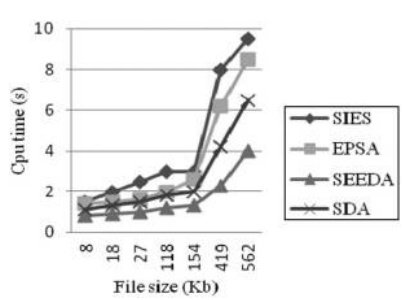


Figure 4 Decryption time

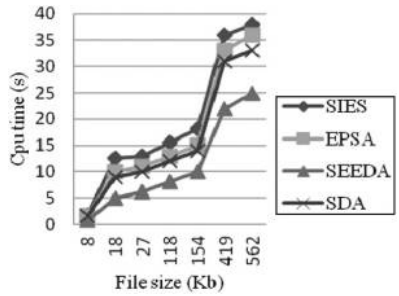


Figure 5 Aggregation time

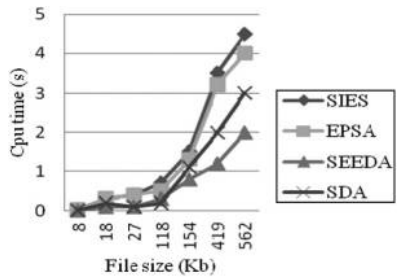
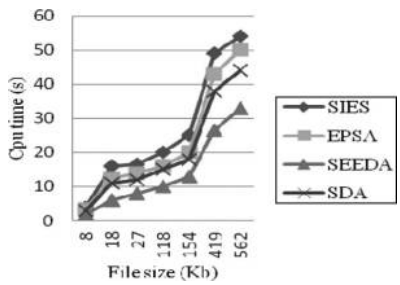


Figure 6 Total computation time by varying the file size



on the temperature readings of file size 8, 18, 27, 118, 154, 419 and 562 kB. In this, the number of nodes is assumed as 10 and the number of cluster heads is assumed to be 1. The time consumption is calculated in seconds (s). The total computation time comprises the time taken for encryption, signature generation, aggregation, decryption and verification. The aggregation time is the aggregation of data and signatures at the cluster head.

From the comparison, the SIES method is found to consume more encryption and decryption time due to the generation of individual RSA signature at the sensors and at the cluster head. Moreover, as the signature verification is to be done individually at the base station, it consumes more computation time. The EPSA method also consumes large encryption and decryption time compared to SDA due to the additional header field at each level. SEEDA has less encryption, decryption and aggregation time than all the other methods because it has no verification protocol. Similarly, SDA incurs less encryption, decryption and aggregation time than SIES and EPSA because it uses homomorphic encryption and aggregate signature methods.

Figure 7 shows the total computation time for 10 sensor nodes, 18 kB of file and varying cluster heads, whereas Figure 8 shows the total computation time for one cluster head, 18 kB of file and varying sensor nodes. SIES consumes more computation time in both the cases, as it does not have an aggregate signature. EPSA also consumes more computation time in both the cases, as it has additional header fields at each level.

The computation time is related directly to the energy consumption of the sensor nodes. If it is less, it, in turn, reduces the energy consumption of the sensor nodes. The energy consumption of a device is calculated using the formula given below (Murat and Kenji, 2011):

$$E = V \times I \times \Delta T$$

where E is the energy in Joules (J), V is the voltage, I is the current in amperes and T is the time in seconds. Always, V and I are constant for any hardware. As the implementation is carried out on the computer system, the power consumption of the CPU is considered for computing the energy. For the CPU, the voltage and current can be assumed as 3 V and 8 mA (milliamperes), respectively. Hence, the energy consumption for the encryption of 8 kB of data in SDA is calculated as $E = 3 \times 0.008 \times 1.5$ W s/J, respectively. Similarly, the energy is calculated for all the other methods of various data sizes.

Figures 9, 10, 11 and 12 show the energy consumption of the existing and the proposed method for 10 sensor nodes, one cluster head and various file sizes. Figure 13 represents the energy consumption for 10 sensor nodes, 18 kB of file and varying cluster heads, whereas Figure 14 shows the energy consumption for one cluster head, 18 kB of file and varying sensor nodes. The energy consumed for encryption and aggregation is less for all the methods compared to that of

Figure 7 Total computation time by varying the cluster heads

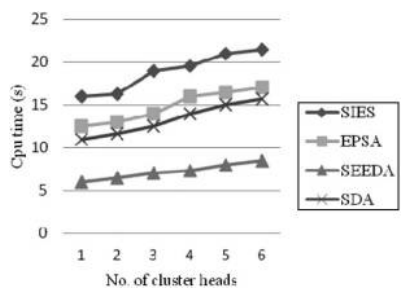


Figure 8 Total computation time by varying the sensor nodes

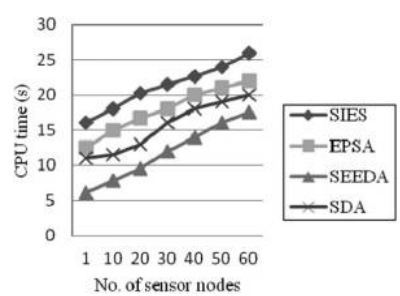


Figure 9 Energy consumption for encryption

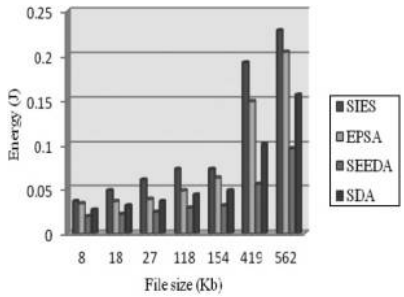


Figure 10 Energy consumption for decryption

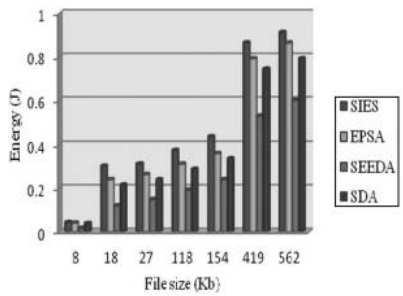


Figure 11 Energy consumption for aggregation

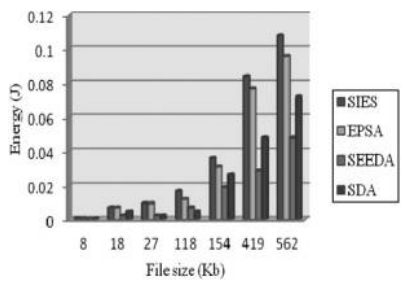
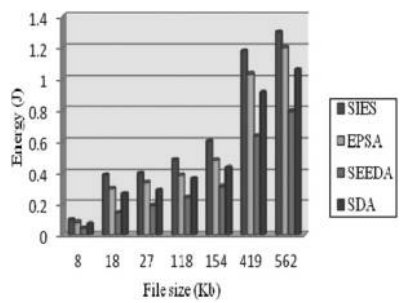


Figure 12 Total energy consumption by varying the file size



decryption. As the decryption is to be done at the base station, the energy consumption can be ignored. The total energy consumed is the sum of energy consumption for encryption, decryption and aggregation. The energy consumed for encryption, decryption and aggregation for SDA is less compared to SIES and EPSA methods.

Figure 13 Total energy consumption by varying the cluster heads

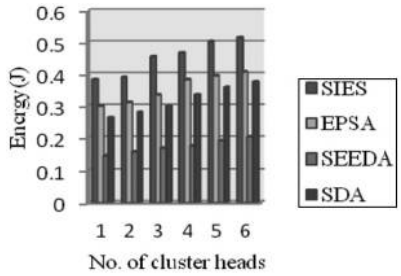
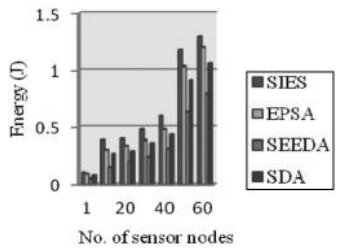


Figure 14 Total energy consumption by varying the sensor nodes



7. Conclusion

In the present study, secured data aggregation of encrypted data is achieved on WSNs. Data confidentiality is provided by using the Paillier additive homomorphic encryption, whereas the data integrity and authenticity are satisfied by using Boneh *et al.*'s aggregate signature. Even though the aggregate signature adds additional cost, it is still suitable for WSNs. The performance of computation time and energy consumption is compared with other similar approaches, which proves that the proposed system is feasible for securing data aggregation.

References

Baek, J., Tan, H., Zhou, J. and Wong, J. (2008), "Realizing stateful public key encryption in wireless sensor network", *IFIP International Information Security Conference-SEC 2008, Springer-Verlag*, Springer, Milano, Vol. 278, pp. 95-107.

Boneh, D., Gentry, C., Lynn, B. and Shacham, H. (2003), "Aggregate and verifiable encrypted signatures from bilinear maps", *22nd International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, Springer, Warsaw, Vol. 2656, pp. 416-432.

Castelluccia, C., Chan, A.C.F., Mykletun, E. and Tsudik, G. (2009), "Efficient and provable secure aggregation of encrypted data in wireless sensor networks", *ACM Transaction on Sensor Networks*, Vol. 5 No. 3, pp. 1 36.

Chen, X., Makki, K., Yen, K. and Pissinou, N. (2009), "Sensor network security: a survey", *IEEE Transactions Surveys and Tutorials*, Vol. 11 No. 2, pp. 52-73.

Chen, C.M., Lin, Y.-H., Lin, Y.-C. and Sun, H.-M. (2012), "RCDA: recoverable concealed data aggregation for data integrity in wireless sensor networks", *IEEE Transaction on Parallel and Distributed Systems*, Vol. 23 No. 4, pp. 727 -734.

Fasolo, E., Rossi, M., Widmer, J. and Zorzi, M. (2007), "In-network aggregation techniques for wireless sensor

networks: a survey", *IEEE Wireless Communications*, Vol. 4 No. 2, pp. 70-87.

Gaubatz, G., Kaps, J.P., Oztruk, E. and Sunar, B. (2005), "State of the art in ultra-low power public key cryptography for wireless sensor networks", 3rd IEEE International Conference on Pervasive Computing and Communications Workshops, IEEE, Kauai Island, HI, pp. 146-150.

Jha, M.K. and Sharma, T.P. (2011), "Secure data aggregation in wireless sensor network: a survey", *International Journal of Engineering Science and Technology*, Vol. 3 No. 3.

Liu, J.K., Baek, J., Zhou, J., Yang, Y. and Wong, J.W. (2010), "Efficient online/offline identity-based signature for wireless sensor network", *International Journal of Information Security*, Vol. 9 No. 4, pp. 287-296.

Murat, A. and Kenji, Y. (2011), "Security and attacks in wireless sensor networks", in Klinger, K. (Ed.), *Wireless Technologies: Concepts, Methodologies, Tools and Applications, Information Resource Management Association*, Information Science Reference, an Imprint of IGI Global, USA, pp. 1811-1846.

Mykletun, E., Girao, J. and Westhoff, D. (2006), "Public key based cryptoschemes for data concealment in wireless sensor networks", IEEE International Conference on Communications, IEEE, Istanbul, Vol. 5, pp. 2288-2295.

Pandey, V., Kaur, A. and Chand, N. (2010), "A review on data aggregation techniques in wireless sensor network", *Journal of Electronic and Electrical Engineering*, Vol. 1 No. 2, pp. 01-08.

Papadopoulos, S., Kiayias, A. and Papadias, D. (2012), "Exact in-network aggregation with integrity and confidentiality", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 24 No. 10, pp. 1760-1773.

Poornima, A.S. and Amberker, B.B. (2010), "SEEDA: secure end- to –end data aggregation in wireless sensor networks", 7th International Conference on Wireless and Optical Communications Networks - IEEE explore, IEEE, Colombo, pp. 1-5.

Rajeswari, S.R. and Seenivasagam, V. (2016), "Comparative study on various authentication protocols in wireless sensor networks", *The Scientific World Journal*, Vol. 2016 No. 2016,

Sen, J. (2013), "Homomorphic encryption: theory and application", in Sen, J. (Ed.), *Theory and Practice of Cryptography and Network Security Protocols and Technologies*, InTech, Intech, Croatia, pp. 1-31.

Xing, K., Srinivasan, S.S.R., Rivera, M.J., Li, J. and Cheng, X. (2005), "Attacks and countermeasures in sensor networks: a survey", *Network Security*, Springer, New York, pp. 251-272.

Yi, X., Bouguettaya, A., Georgakopoulos, D., Song, A. and Willemson, J. (2015), "Privacy protection for medical sensor data", *IEEE Transaction on Dependable and Secure Computing*, Vol. 13 No. 3, pp. 369-380.

Corresponding author

Sathya D. can be contacted at: sathy.spj@gmail.com