ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Special Issue (April)

Online - 2455-3891
Print - 0974-2441

Full Proceeding Paper

SECURED DATA AGGREGATION METHODS IN WIRELESS SENSOR NETWORKS USING HOMOMORPHIC OPERATION - A REVIEW

SHAHINA K*, VAIDEHI V

Department of Computing Science and Engineering, VIT University, Chennai, Tamil Nadu, India. Email: shahina.k2016@vitstudent.ac.in

Received: 29 March 2017, Revised and Accepted: 30 March 2017

ABSTRACT

Wireless sensor networks (WSNs) are energy constrained. Data aggregation is an important mechanism for achieving energy efficiency in such networks. The aggregation reduces redundancy in data transmission which results in improved energy usage. Several security issues are there in data aggregation, which includes data confidentiality, data integrity, availability, and freshness. Such issues become complex since WSN is deployed in hostile and unattended environment. Hence, the sensor nodes may fail and compromised by adversaries. Secure data aggregation (SDA) in sensor network is a topic of research. Many solutions are proposed for SDA, using different encryption methods. Homomorphic encryption is one of such techniques. In homomorphic encryption, all the nodes participate in the aggregation. Here, nodes cannot see any intermediate or final result, but the aggregation is efficient. In this paper, SDA methods are classified and the performance is compared in terms of integrity and confidentiality.

Keywords: Data aggregation, Homomorphic encryption, Wireless sensor networks, Data integrity, Data confidentiality.

 DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19749

INTRODUCTION

Sensor networks consist of small and low-cost sensors, which sense the environmental data. It can monitor the physical parameters and control them from remote areas. Resources are limited for wireless sensor network (WSN). Communication consumes relatively high energy than local processing. Hence, a common aim is to reduce the number of data transmission [1]. An important method for the reduction of data transmission is data aggregation. It significantly saves energy. Hence, data aggregation is important for many critical applications of sensor networks.

Wireless networks are dangerous since it is public. Also nodes placement is hostile in nature and hence nodes may be easily compromised. The various security requirements [2] are:

- Data confidentiality: Protect content of the message
- Data integrity: Ensuring that packet is not modified during transmission
- Authentication: Ensures that the sender is genuine
- Availability: Main aim is to prevent denial of service attacks. Even if any security threats are there, network has to maintain the services
- Freshness: Ensuring that a compromised node does not resend old packets that are already captured.

Data aggregation protocols should be created in related with the security protocols. So that it can provide cooperation between the protocol complexity and security [3]. So ensuring the security in aggregation is a challenge. Many solutions are proposed based on different encryption schemes.

DATA AGGREGATION: OVERVIEW

Data aggregation is the collection of data from different sensors and the aggregator node send the summary of collected data to base station (BS) with appropriate routing mechanism. The routing structure determines the efficiency of aggregation process [4]. Nodes are classified as three types in related with aggregation: Sensor nodes, aggregator node which does aggregation function, and a querier, which sends the query. Aggregator node collects data from many sensor nodes; aggregate the gathered data using aggregation functions (e.g., SUM, COUNT, MIN, and MAX) [5] and then send the result to the sink node. This mechanism will eliminate the redundancy in the collected data and improves network lifetime. Data aggregation is a common method used in sensor networks. All type of sensor data will be fused together to form aggregated data [6]. The security issues, data confidentiality and integrity are important since the network is in aggressive environment. Aggregation is the process of integrating the sensor data using aggregation methods. In this algorithm, it uses the data from different sensor nodes and then combines the data by using aggregation algorithms such as low energy adaptive clustering hierarchy and tiny aggregation (TAG). Through a selected path, the data are transferred to the sink node. In Fig. 1, Data aggregation model: If the nodes 1, 2, and 3 want to send same data, aggregator node, 7 will do aggregation function and send single packet to BS. In Fig. 1, non-data aggregation model, the nodes 4, 5, and 6 want to send the copy of same data, the node 8 will send all the 3 packets separately to BS even if the data are same.

As the effect of aggregation process, number of packets and number of collisions will be reduced and hence the number of retransmissions also. Less number of retransmission leads to low wastage if time and finally it will increase the network throughput [7]. Fig. 2 shows the effect of data aggregation. WSNs are vulnerable to different security attacks. So providing some security is necessary. Secure data aggregation (SDA) methods are of two types; hop-by-hop and end-to-end encryption. Aggregator node decrypts the received data and does the corresponding aggregation function. Finally, encrypts and send to the neighbour, this is the first method. In the second method, intermediate node gets the encrypted data from sender nodes and combines them with its data; finally, the aggregated data will send to next hop.

HOMOMORPHIC ENCRYPTION

There are mainly two types of security solutions for data aggregation; hop-by-hop method and end-to-end method. In hop-by-hop method, encryption/decryption will be done in each hop [8]. It will do security check in each step, every en-route node decrypt the message and do aggregation before the encryption. The solution introduces high delay since the encryption/decryption operations are performed by the every en-route node.

The end-to-end solution overcomes the limitation of the first category. This solution is using privacy homomorphic encryption. It allows direct computation (addition and/or multiplication) on encrypted data itself. For achieving SDA, homomorphic encryption offers low computation and long lifetime [9]. Fully homomorphic technique allows both addition and multiplication on encrypted data. Let us consider D () and E () denotes decryption and encryption, respectively [10]. K_u be the public key and K_r is the private key and Q is the data set, then (1) and (2) are the equations for multiplicative homomorphic and additive homomorphic:

$$a \times b = D_{kr}(E_{ku}(a) \times E_{ku}(b)) \quad (1)$$

$$a + b = D_{kr}(E_{ku}(a) + E_{ku}(b)) \quad (2)$$

It provides end-to-end privacy and no need to perform encryption/decryption operations at en-route nodes. Homomorphic encryption is a special type of cryptographic method, in which operations can be done on ciphertext. The encrypted result which, when decrypted, matches the result of operations performed on the plaintext. If an encryption algorithm satisfies the following equation, it is said to be homomorphic.

$$D(E(x) \text{ c } E(y)) = D(E(x \text{ m } y)). \quad (3)$$

Here, C group is ciphertexts and M group is plaintexts. Operations on c and m are performed in C and M group. Fig. 3 shows the homomorphic property.

LITERATURE SURVEY

This section analyses some SDA methods in WSN. The methods can be classified based on whether the methods cocentralized aggregation through cluster head (CH) or de-centralized. Fig. 4 is the classification diagram. In centralized aggregation through clusters, each node send the sensed data to a leader node that is CH and CH aggregates the data. Finally, it will be send to BS. In decentralized approach, there is no centralized or leader node, anyone can act as aggregator.

Efficient energy interest base reliable data aggregation (EIRDA)

EIRDA protocol [7] for WSNs. Here, sensor nodes are uniformly distributed in cluster. The working of EIRDA has mainly two phases: Setup phase and steady phase. In the first phase, CH will be selected and it sends update CH packets to each node and to the BS. Interest packets will be broadcasted from BS to all the deployed sensor nodes to start the communication. Format of interest packet is <nodeinterest, CHinterest>. Message description and interest ID constitutes node interest. In steady phase, communication initiates and continues.

Aggregator node performs aggregation based on CH's interest and forward the aggregated data to BS. System model of EIRDA is shown in Fig. 5. To check the reliability, beta distribution function with functional reputation concept is used. To create a trusted network, the nodes will exchange their reputation values which help to find a trusted path to CH or aggregator. The method does not lead to any additional energy overhead, but energy will be high if there is any attack. In this method, less number of nodes having same interest, so number of collisions and retransmissions will be less here. Thus, network has relatively high fault tolerance. Among the nodes in the same cluster, selection of CH is rotated, so load will be uniformly distributed. Intruder cannot understand which interest ID makes the network secure, because of the random generation of interest by the sensor nodes.

Integrity protecting hierarchical concealed data aggregation (IHCA)

Ozdemir proposes an IHCA [10] method. Using a key encryption, the BS classifies the aggregated data. To ensure confidentiality, they are also using elliptic curve cryptography. For encryption, every cluster has public keys of other clusters. Each aggregator node receives the messages from all of its cluster members and aggregates the encrypted data by using homomorphic property. Finally, calculates a message authentication code (MAC) for the obtained data. This encryption ensures the security against passive attacks. Even if privacy and integrity between aggregators can be ensured in this method, it may introduce high communication and computation overhead. Fig. 6 shows an example of IHCA protocol. Here, DA_3 aggregates the data from two groups DA_1 and DA_2 and send to BS.

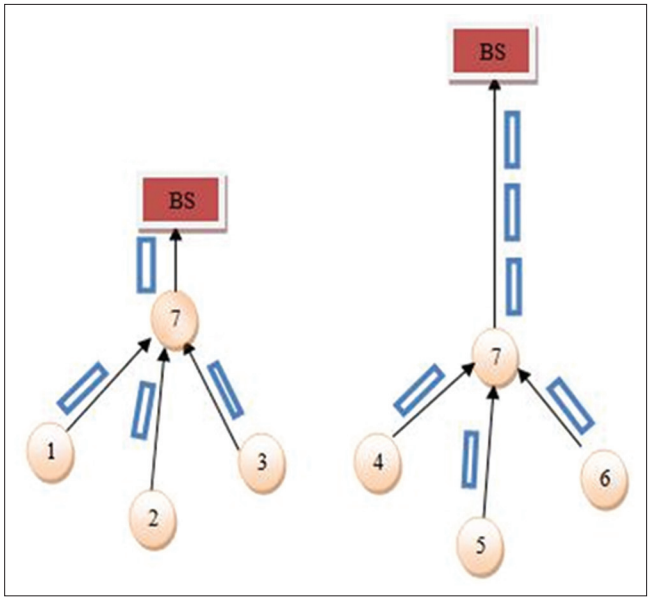

Fig. 1: Aggregation and non-data aggregation mode

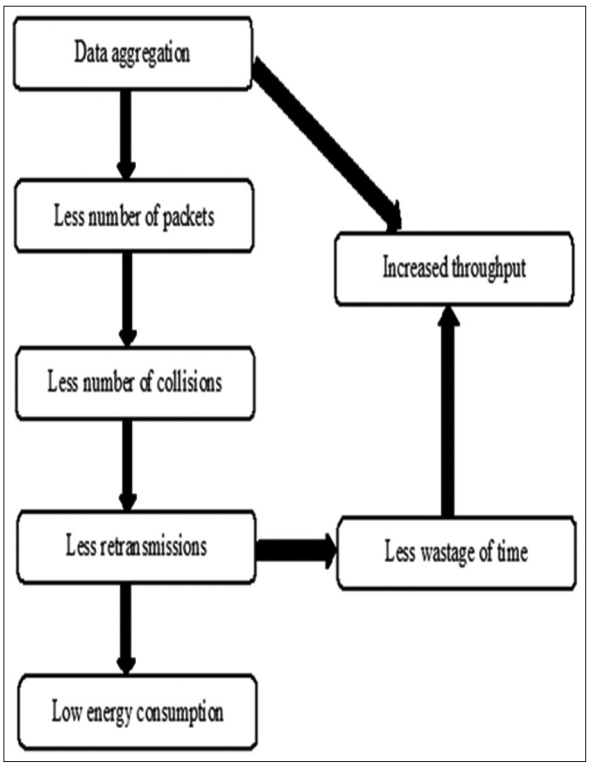

Fig. 2: Overall effect of data aggregation

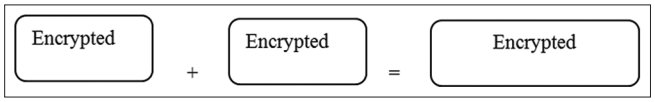

Fig. 3: Homomorphic property

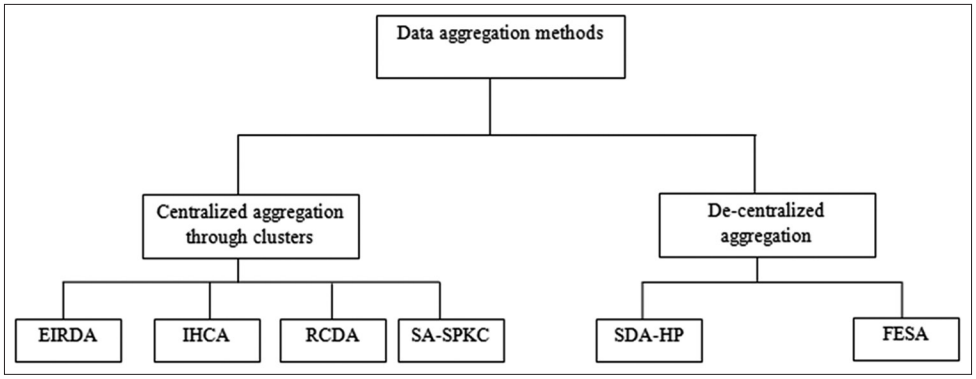

Fig. 4: Classification of data aggregation methods

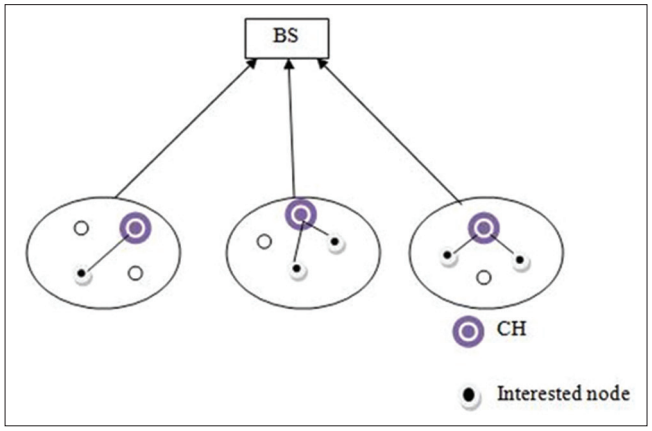

Fig. 5: System model

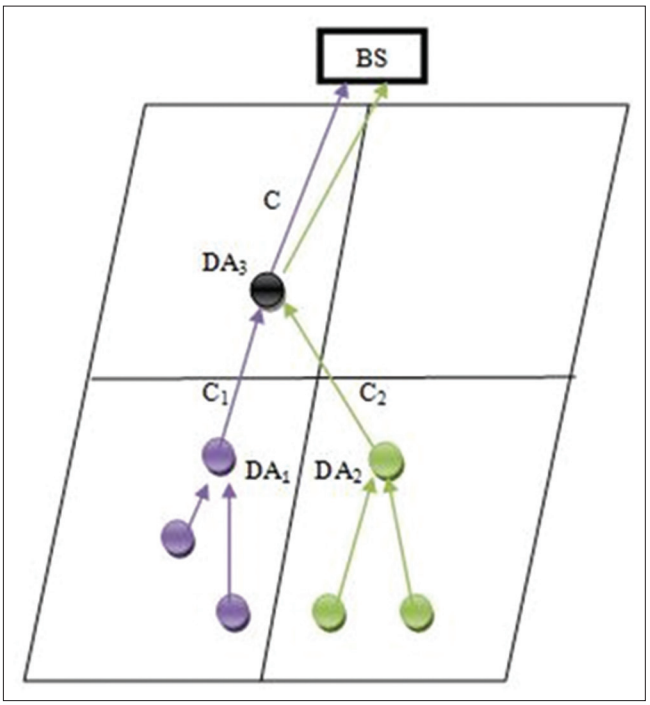

Fig. 6: Example of integrity protecting hierarchical concealed data aggregation

Recoverable concealed data aggregation (RCDA) [11]
The method consists of four stages; Deployment, encryption, aggregation, and verification. In deployment stage, nodes are preloaded with their keys and clusters will be formed using nodes. In encryption stage, nodes encrypt the data and sign it. Finally, data is transmitted to aggregator. Aggregation function is performed in the third phase. Here, the aggregator node aggregates the data by applying homomorphic primitives on ciphertexts and signatures. Finally, both of the results will be send to sink. In the final stage (verification), recovery and verification of data will be there. Fig. 7 shows the process. This scheme proposes two separate aggregation models for homogeneous networks and heterogeneous networks.

Computational overhead is because of the encryption and signature by all sensor nodes. To reduce communication overhead, the message size=476 bits (161*2=322 bits for ciphertexts and 154 bits for signatures). Total number of bits sent=n*(476+h).

Secured and efficient aggregation using stateful public key cryptography (SA-SPKC) [12]
This technique will handle the privacy and data integrity. Communication and computation overhead is less by the usage of homomorphic encryption. Mainly two phases are there in this method, forwarding and aggregation. In forwarding phase, every sensor sends their own state which can use in the second phase. To provide integrity, it adopts aggregate MAC with homomorphic property. The result will help for authentication and integrity verification (IV) with all individual data. In aggregation phase, the nodes will encrypt and authenticate the received data. This is done by using the state which is shared with the BS. Then, CH collects the ciphertexts and tags into single one and one tag using the homomorphic and the X-or operation, respectively. At last, the BS verifies the aggregated data by decrypting and retrieving the real message. After that, it does IV and authentication of sender nodes.

SDA with homomorphic primitives (SDA-HP) [13]
It uses homomorphic MAC and encrypted data together; hence it provides both confidentiality and integrity. SDA-HP provides end-to-end authentication mechanism which is free from several security threats. Furthermore, integrity of aggregate data is provided. The different stages of SDA-HP consist of tree formatting phase, key generation phase, sign-encrypt phase, aggregation phase, and decrypt-verify phase as shown in Fig. 8. This scheme introduces less amount of bandwidth consumption. In tree formatting phase, it will construct an aggregation tree using TAG protocol. Key generation phase is using $K=(p,q,r_1,\ldots,r_i,\ldots,r_d,s_1,\ldots,s_i,\ldots,s_d)$, total 2d+1 private keys and a single public key n=pq, p and q are large primes.

SDA with fully homomorphic encryption (FESA) [14]
This technique provides end-to-end confidentiality. It uses a simple aggregation method with a group of effective homomorpphic encryption methods. For the early detection of false data, it does the IV in both aggregation and forwarding phases using MACs. It has a specific network model as in Fig. 9, which is MFN group structure. Relating with aggregator node, there are monitoring node forwarding node and neighbouring node. Monitoring node computes the data and neighboring and forwarding nodes in the same group verify

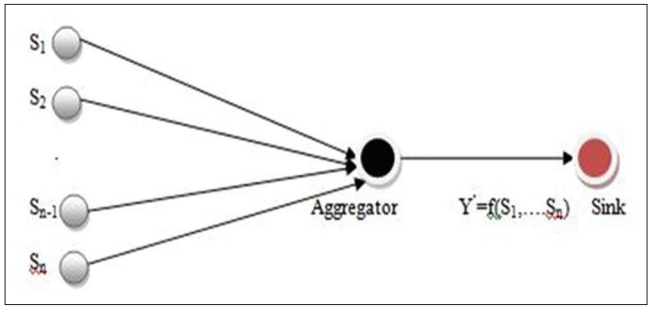

Fig. 7: Data aggregation with recoverable concealed data aggregation

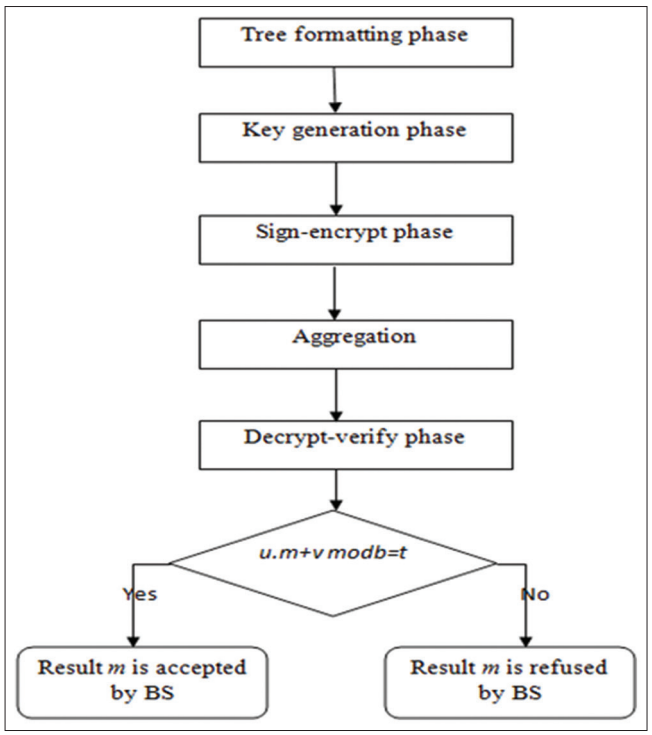

Fig. 8: Different phases of secured data aggregation with homomorphic primitives

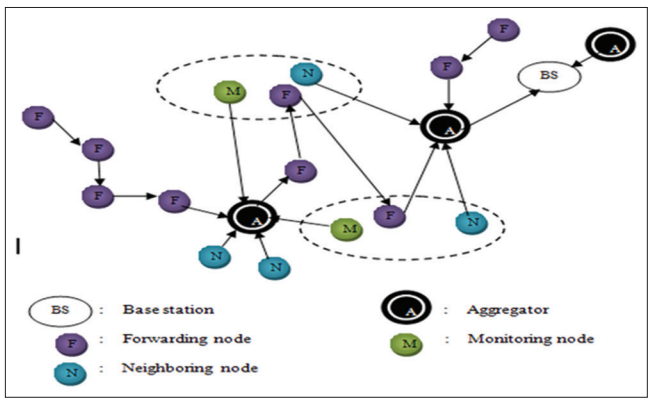

Fig. 9: Network structure of secured data aggregation with fully homomorphic encryption

the integrity. It proposes an additive homomorphic encryption. The technique also provides a proof of security. When comparing with other methods, this method is efficient in terms of communication overhead and energy consumption.

Table 1: Analysis of aggregation methods

Method	Integrity	Confidentiality	IM	IV
IHCA	×	×	Hash	Aggregation
EIRDA	✓	✓	MAC	Forwarding and BS
RCDA	×	✓	MAC	Forwarding and BS
SA-SPKC	✓	✓	Hash	Forwarding and BS
SDA-HP	✓	✓	MAC	Forwarding and BS
FESA	✓	✓	MAC	Aggregation and BS

IM: Integrity method, IV: Integrity verification, IHCA: Integrity protecting hierarchical concealed data aggregation, EIRDA: Efficient energy base reliable data aggregation, RCDA: Recoverable concealed data aggregation, SA-SPKC: Secured and efficient aggregation using stateful public key cryptography, SDA-HP: Secured data aggregation with homomorphic primitives, FESA: Secured data aggregation with fully homomorphic encryption, MAC: Message authentication code

Table 2: Analysis of aggregation methods

Method	Encryption	AF	CC	EC
IHCA	Hop by hop	Additive	Medium	Medium
EIRDA	Hop by hop	Additive	Medium	Medium
RCDA	End to end	SUM	High	Medium
SA-SPKAC	End to end	MIN/MAX	Medium	High
SDA-HP	End to end	SUM	High	Low
FESA	End to end	Additive	High	Medium

IHCA: Integrity protecting hierarchical concealed data aggregation, EIRDA: Efficient energy base reliable data aggregation, RCDA: Recoverable concealed data aggregation, SA-SPKC Secured and efficient aggregation using stateful public key cryptography, SDA-HP: Secured data aggregation with homomorphic primitives, FESA: Secured data aggregation with fully homomorphic encryption, AF: Aggregation function, CC: Communication cost, EC: Energy consumption

COMPARATIVE ANALYSIS

This section includes the comparison of above-discussed aggregation methods in terms of security requirements, communication cost, and energy consumption. Data aggregation is mainly for reducing the energy consumption. WSNs are deployed in open hostile environment, so aggregated data may be subjected to different attacks; hence, it is necessary to increase security. Employing homomorphic encryption achieves end to end confidentiality. Aggregator performs homomorphic operation, which can directly access encrypted data. Integrity property prevents the adversaries from communication. The above-mentioned different techniques use hash function or MACs for providing integrity. It employs either hop by hop encryption or end to end encryption and aggregation is done by either aggregation or forwarding and BS. Aggregation functions may be SUM, COUNT, MIN/MAX, etc. Relative communication cost and energy consumption are given as different ranges that are low, medium and high.

Applications in which the confidentiality of data are more important; homomorphic encryption is very useful. Integrity helps the network for preventing attackers. Energy consumption is the total energy consumed by the sensor networks for collecting the data. Consumption of energy is linearly dependent on the amount of data transmission. Before transmitting to the next level, sensors have to generate ciphertexts. The execution time for generating this ciphertext will be the communication cost. Homomorphic encryption plays a key role for achieving security in data aggregation with less computation and energy. Tables 1 and 2 show the comparison of SDA methods discussed above.

SCOPE FOR FUTURE WORK

An efficient data aggregation protocol which provides both high security and performance is needed. Homomorphic encryption can be either additive or multiplicative on encrypted data. Fully homomorphic encryption is closed under both addition and multiplication.

Homomorphic operation with multiple functions is widely desirable now. Mobility is an important extension for WSN. SDA can be extended for mobile sensors with the usage of homomorphic properties. Nowadays most of the research considers static networks, but many applications can achieve significant results if mobility is considered. Hence, it is required to extend this work to support mobility with the application of homomorphic encryption properties. It is needed to propose new mechanism for creation and maintaining of clusters with less overhead. End-to-end security solution prevents several attacks; these methods use much amount of resource for detecting the attacks. So efficient mechanisms are needed for detection of security attacks with less overhead.

CONCLUSION

It is known that WSN use data aggregation to save energy. SDA provides data aggregation on encrypted data. Homomorphic solution found to be very effective in SDA. This paper presented the survey of SDA techniques which use homomorphic operations and compared their performance in terms of integrity, confidentiality, range of communication cost, and energy consumption. A novel SDA method using homomorphic encryption with less computation overhead is required.

REFERENCES

1. Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. Elsevier Comput Netw 2002;38(4):393-422.
2. Parli BH, Narayan SS. Security issues in wireless sensor networks: Current research and challenges. International Conference on Advances in Computing, Communication and Automation (ICACCA) IEEE; 2016. p. 1-6.
3. Tahir H, Asim S. Wireless sensor network: A security perspective. Multitopic Conference, IEEE International; 2008.
4. Wan S, Zhang Y, Chen J. On the construction of data aggregation tree with maximizing lifetime in large-scale wireless sensor networks. IEEE Sensors J 2016;16(20):7433-40.
5. Ranjan R, Karmore SP. Survey on secured data aggregation in wireless sensor network. IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems; 2015.
6. Krithika S, Preshiya DJ. Enhanced data aggregation techniques for compromised node attacks in wireless sensor networks. IEEE WiSPNET Conference; 2016.
7. Sethi H, Devendra P, Patel RB. EIRDA: An energy efficient interest based reliable data aggregation protocol for wireless sensor networks. Int J Comput Appl 2011;22(7):20-5.
8. Gaikwad S, Kulkarni UV. Comparative analysis of hop-to-hop and end-to-end secure communication. Int J Adv Res Technol 2013;2(7):473-7.
9. Ertaul L, Yang JH, Saldamli G. Analyzing homomorphic encryption schemes in securing wireless sensor networks. IJCSNS Int J Comput Sci Netw Secur 2015;15(5):1-11.
10. Ozdemir S, Xiao Y. Integrity protecting hierarchical concealed data aggregation for wireless sensor networks. Int J Comput Telecommun Netw 2011;55:1735-46.
11. Chen CM, Lin YH, Lin YC, Sun HM. RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks. IEEE Tans Parallel Distrib Syst 2012;23(4):81-6.
12. Rafik O, Mohammed F. SA-SPKC: Secure and Efficient Aggregation Scheme for Wireless Sensor Networks using Stateful Public Key Cryptography. IEEE Conference Publications; 2013.
13. Zhou Q, Yang G, He L. An efficient secure data aggregation based on homomorphic primitives in wireless sensor networks. Int J Distrib Sensor Netw 2014;7:11.
14. Li X, Chen D, Li C, Wang L. Secure data aggregation with fully homomorphic encryption in largescale wireless sensor networks. Sensors 2015;15:952-73.