International Conference on
<Conference Name>
<College Name>, <Place>, India. <Conference date>. pp. x – y.

Secure Data Aggregation in Wireless Sensor Networks - A Survey

Paresh Solanki[1] and Gaurang Raval[2]

Institute of Technology
Nirma University, Ahmedabad, Gujarat, India
[1] M.Tech (CSE) Sem-III Student,
[2] Assistant Professor, CSE Department

Abstract

The primary use of wireless sensor networks (WSNs) is to collect and process data. 70% of energy consumption is due to data transmission. Because of the hostile environment and unique properties of wireless sensor network all raw data samples are not directly sent to the sink node, but data aggregation is applied. Also, Wireless sensor nodes are often deployed in an open environment such as a battlefield or other similar applications. Data confidentiality and integrity are vital issues in such conditions, hence secure aggregation is required. Hop by hop secure data aggregation is resource consuming compared with end to end secure encrypted data aggregation. Currently various efficient schemes are available for end to end secure encrypted data aggregation. This paper provides the survey on existing hop by hop and end to end secure data aggregation schemes.

Keywords— *Data aggregation, end to end encryption, wireless sensor networks.*

1. INTRODUCTION

In wireless sensor networks, sensor nodes collect the data from hostile environment and send it to sink node where it is processed, analyzed and used by the application. In these resource constrained networks, the general approach is to send the data jointly which is generated by different sensor nodes, while being forwarded toward the base station such in-network processing of data is generally known as data aggregation. It consumes less energy and limited resources of sensors are used. When base station queries to the network, all nodes do not send their data to sink node directly but aggregator node first receives the data from sensor nodes and aggregates the data and then sends it to sink node. Data aggregation reduces the number of data transmissions thereby improving the bandwidth and energy utilization in the network. Because of the peculiar characteristics of sensor network, security of data aggregation is most crucial in certain environments. There is a strong conflict between security and data aggregation protocols. Security protocols require sensor nodes to encrypt and authenticate any sensed data prior to its transmission and prefer data to be decrypted by the base station. On the other hand, data aggregation protocols prefer plain data to implement data aggregation at every intermediate node so that energy efficiency is maximized. Moreover, a data aggregation results in alterations in sensor data and therefore it is a challenging task to provide source and data authentication along with data aggregation. Due to these conflicting goals, data aggregation and security protocols must be designed together so that data aggregation can be performed without sacrificing security. In this paper we present survey on existing secure data aggregation schemes providing secure communication.

2. SECURE DATA AGGREGATION REQUIREMENTS

The data security requirements in the WSNs are similar to those in traditional networks. However, there are some unique specifications that can only be found in WSNs that require more attention during design process. This section provides brief information about requirements for data aggregation security [2].

Data Confidentiality ensures that information content is never revealed to anyone who is not authorized to receive it. it is minimal security requirement of WSN. *Data Integrity* ensures that the content of a message has not been altered, either maliciously or by accident, during transmission process. *Data Freshness* ensures that the data are recent and that no old messages have been replayed to protect data aggregation schemes against replay attack. *Data Availability* ensures that the network is alive and that data are accessible. *Authentication* ensures that reported data is the same as original one. Receiver can verify that received message is sent by the claimed sender or not. *Key management* should be kept as simple as possible as it accounts for energy and bandwidth consumption.

3. DATA AGGREGATION STRATEGIES

The main objective of data aggregation is to increase the network lifetime by reducing the resource consumption of sensor nodes (such as battery energy and bandwidth). Data aggregation techniques are tightly coupled with how packets are routed through the network. There are several protocols that allow routing and aggregation of data packets simultaneously. These protocols can be categorized into: *tree-based data aggregation protocols* and *cluster-based data aggregation protocols.*

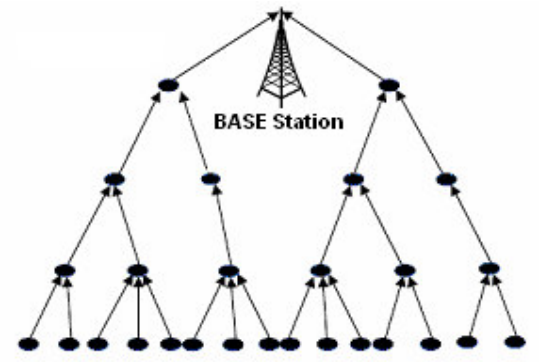

Fig. 1: Tree based data aggregation

To reduce the latency present in the tree-based data aggregation, recent work on data aggregation tends to group sensor nodes into clusters so that data gets aggregated in each group for improved efficiency. Figure 1 shows the tree based data aggregation and Figure 2 shows the cluster based data aggregation.

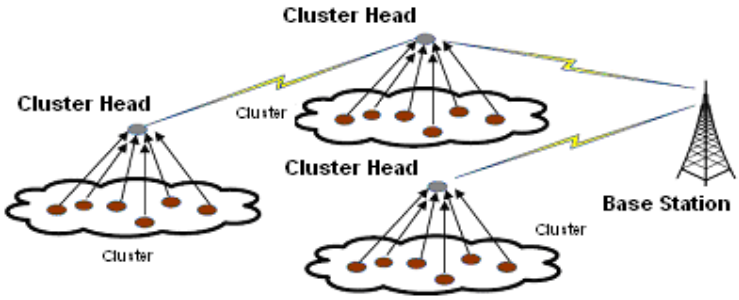

Fig. 2: Cluster based data aggregation

4. SECURE DATA AGGREGATION SCHEMES

Due to hostile environments and unique properties of wireless sensor networks, it is a challenging task to protect sensitive information transmitted by wireless sensor networks. Data aggregation protocols must be satisfying the security requirements as explained earlier. Security requirements of wireless sensor networks can be satisfied using either symmetric key or asymmetric key cryptography. Due to resource constraints of sensor nodes, symmetric key cryptography is preferable over asymmetric key cryptography. Many protocols provide security and data aggregation together in hop by hop fashion and end to end fashion. In hop by hop secure data aggregation protocols, data aggregator must decrypt every message received, perform aggregation on this decrypted data and again encrypt the aggregation result before forwarding it to the base station. In addition, these schemes require data aggregators to establish secrete keys with their neighboring nodes. So hop by hop secure data aggregation protocols does not provide confidentiality at data aggregators and result in latency because of encryption and decryption process. Number of other secure data aggregation schemes exist which are based on end to end secure data aggregation.

5. SDA USING PLAIN SENSOR DATA

First secure data aggregation (SDA) was proposed by Hu et al. [3] who studied the problem of data aggregation once one node is compromised. The authors propose security mechanisms to detect node misbehavior (dropping, modifying messages, and transmitting false aggregate values). The key idea of this work is delayed aggregation. Instead of aggregating messages at the immediate next hop, messages are forwarded unchanged over the first hop and then aggregated

at the second hop. This is achieved using a key chain; the base station periodically broadcast authentication keys. Hence, sensor nodes need to buffer the data to authenticate it once the authentication key is broadcasted by the base station. Moreover, the proposed scheme only offers data integrity, freshness and authentication. it does not provide data confidentiality. Data can be altered once a parent and child in the hierarchy are compromised. Once a compromised node is detected, no practical action is taken to reduce the damage caused by this compromise which affects the data availability in the network. Much worse, once a grandfather node detects a node compromise, it could not decide whether the cheating node is the child or the grandchild.

SDA scheme is improved in ESA by Jadia et al [4] Instead of using µTESLA to authenticate the base station's broadcast in the validation process to reveal the shared key with sensors, the authors used one-hop pairwise keys (to encrypt data between a node and its parent) and two-hop pairwise keys (to encrypt data between a node and its grandparent). This will improve the secure aggregation scheme by adding data confidentiality and reducing the memory overhead since data does not need to be stored until the key is revealed. However, the system will still break as soon as two consecutive nodes in the hierarchy are compromised.

Przydatek et al. [5] proposed a secure information aggregation (SIA) scheme. Random sampling mechanisms and interactive proofs are used to check the correctness of the aggregated data at the base station. The authors claim that, by constructing efficient random sampling mechanisms and interactive proofs, it is possible for the user to verify that the aggregated data provided by the aggregator is a good approximation of the true value even when the aggregator and a fraction of the sensor nodes are compromised. In particular, the authors present efficient protocols for securely computing the median and the average of the measurements, estimation of the network size, and finding the minimum and maximum sensor reading. The correctness of data is checked by constructing a Merkle hash tree. In this construction, all the collected data is placed at the leaves of the tree, and the aggregator computes a binary hash tree starting from the leaf nodes: each internal node in the hash tree is computed as the hash value of the concatenation of the two child nodes. The root of the tree is called the commitment of the collected data. This scheme provides resistance against a special type of attack called stealthy attacks aggregate manipulation where the attacker's goal is to make the user accept false aggregation results without revealing its presence to the user. Protocol consists of three node categories: a home server, a base station, and sensor nodes. SIA assumes that each sensor has a unique identifier and shares a separate secret cryptographic key with both the home server and the aggregator. The keys enable message authentication and encryption if data confidentiality is required. home server and base station can use a mechanism, such as µTESLA [6] to broadcast authentic messages. SIA consists of three parts: collecting data from sensors and locally computing the aggregation result, committing to the collected data, and reporting the aggregation result while proving the correctness of the result. SIA offers data integrity, authentication, data freshness, and confidentiality (if required).

Mahimkar et al [7] proposed SecureDEV protocol which is similar to SIA and ESA except that elliptic curve cryptography is used for encryption purposes. Moreover, SecureDAV improves the data integrity vulnerability by signing the aggregated data. SecureDAV is a clustered approach where all sensor nodes within a cluster share a secret cluster key. Each sensor node is able to generate a partial signature over the aggregated data. Each data aggregator aggregates its cluster data and broadcasts the aggregated data to its cluster. Each sensor node in the cluster compares its data with the aggregated data broadcasted by the data aggregator. A sensor node partially signs the aggregated data if and only if the difference between its data and aggregated data is less than a certain value (threshold). Finally, the data aggregator combines the partial signatures to form a full signature of the aggregated data and sends it to the base station. SecureDAV provides data confidentiality, data integrity, and source authentication. The drawbacks of this scheme are, high communication costs for data validation, and supports only AVG aggregation function.

Witness based Data Aggregation scheme is proposed by Du et al [8] this scheme assures the validation of the data sent from an aggregator node to the base station. In order to prove the validity of the aggregated result, the aggregator node has to provide proofs from several witnesses. A witness is one who also performs data aggregation like the aggregator node, but does not forward its result to the base station. Instead, each witness computes the message authentication code (MAC) of the result and then sends it to the aggregator node which must forward the proofs to the base station. WDA offers only integrity property to the data aggregation security and this is required to send multiple copies similar to the original aggregated result, to the aggregator point. Thus, the aggregator point must forward these reports as well as the aggregated result to the base station. Since the aggregator point is fixed and responsible to handle so much traffic, the aggregator resources will not last long. The proposed protocol offers only integrity property.

Secure Aggregation Tree (SAT) proposed by Wu et al [9] sensor nodes use the cryptographic algorithms only when a cheating activity is detected. Topological constraints are introduced to build a secure aggregation tree (SAT) that facilitates the monitoring of data aggregators. In SAT, any child node is able to listen to the incoming data of its parent node. When the aggregated data of a data aggregator are questionable, a weighted voting scheme is employed to decide whether the data aggregator is properly behaving or is cheating. If the data aggregator is a misbehaving node, then SAT is rebuilt locally so that the misbehaving data aggregator is excluded from the aggregation tree.

Secure and rEliable Data Aggregation protocol (SELDA) proposed by Ozdemir [10] argues that compromised nodes have access to cryptographic keys that are used to secure the aggregation process and therefore cryptographic primitives alone cannot provide a sufficient enough solution to secure data aggregation problem. Depending on this observation SELDA is proposed by author. The basic idea behind SELDA is that sensor nodes observe actions of their neighboring nodes to develop trust levels (trustworthiness) for both the environment and the neighboring nodes. Sensor nodes employ monitoring mechanisms to detect node availability, sensing and routing, misbehavior of their neighbors. These misbehaviors are quantified as trust levels using Beta distribution function. Sensor nodes exchange their trust levels with neighboring nodes to form a web of trust that allows them to determine secure and reliable paths to data aggregators. Moreover, to improve the reliability of the aggregated data, data aggregators weigh sensor data they receive using the web of trust. One important property of SELDA is that, due to the monitoring mechanisms in use, it can detect if a data aggregator is under DoS attack. The simulation results show that SELDA increases the reliability of the aggregated data at the expense of a tolerable communication overhead. The authors improved the main idea of SELDA by introducing functional reputation concept where each functional reputation value is computed over sensor node actions with respect to that function. Hence, security of data aggregation process is ensured by selecting trusted data aggregators using aggregation functional reputation and by weighting sensor data using sensing functional reputation. The simulation results show that functional reputation is more effective than general reputation when evaluating the trustworthiness of a sensor node [11].

Data Aggregation and Authentication protocol (DAA) proposed by H. cam et al [12] integrates false data detection with data aggregation and confidentiality. To support data aggregation along with false data detection, a monitoring algorithm is proposed. Using this monitoring algorithm, the monitoring nodes of every data aggregator also conduct data aggregation and compute the corresponding small-size message authentication codes for data verification at their pair mates. To support confidential data transmission, the sensor nodes between two consecutive data aggregators verify the data integrity on the encrypted data rather than the plain data. Each data packet is appended with two full-size message authentication codes, each consisting of T + 1 small-size message authentication codes. Performance analysis shows that DAA detects any false data injected by up to T compromised nodes, and that the detected false data are not forwarded beyond the next data aggregator on the path. Despite that false data detection and data confidentiality increase the communication overhead, simulation results show that DAA can still reduce the amount of transmitted data by up to 60% with the help of data aggregation and early detection and dropping of false data.

All of the secure aggregation protocols discussed above use actual sensor data for aggregation and hence require decryption of sensor data at aggregators. So it is more power consuming and resource utilization is high. So depending on security requirements and sensor network architecture, this schemes may be used or not.

ESDPA [13] and SRDA [14] do not need actual data and therefore they are able to integrate security and data aggregation seamlessly. Energy efficient and Secure Pattern based Data Aggregation (ESPDA) protocol Proposed by H. Cam et al [13] considers both data aggregation and security concepts together in cluster-based wireless sensor networks. ESPDA is the first protocol to consider data aggregation techniques without compromising security. ESPDA uses pattern codes to perform data aggregation. The pattern codes are representative data items that are extracted from the actual data in such a way that every pattern code has certain characteristics of the corresponding actual data. The extraction process may vary depending on the type of the actual data. For example, when the actual data are images of human beings sensed by the surveillance sensors, the key parameter values for the face and body recognition are considered as the representative data depending on the application requirements. When a sensor node consists of multiple sensing units, the pattern codes of the sensor node are obtained by combining the pattern codes of the individual sensing units. Instead of transmitting the whole sensed data, sensor nodes first generate and then send the pattern codes to cluster heads. Cluster heads determine the distinct pattern codes and then request only one sensor node to send the actual data for each distinct pattern code. This approach makes ESPDA both energy and bandwidth efficient. ESPDA is also secure because cluster heads do not need to decrypt the data for data aggregation and no encryption/decryption key is broadcast.

Secure Reference-Based Data Aggregation (SRDA) protocol proposed by H.O. Sanli et al [14] sends only the difference between sensed data and the reference value (called differential value) instead of raw data. Deference value is taken as the average value of previous sensor readings. In SRDA scheme, each sensor computes the differential data, encrypts it, and then sends it to the cluster-head. As an example, let $105^{o}F$ denote the temperature measurement of a sensor node. If $100^{o}F$ is considered as reference temperature by the cluster head, the sensor node can send only the difference (i.e., $5^{o}F$) of the current measurement from the reference value in the transmission. Consequently, differential aggregation has great potential to reduce the amount of data to be transmitted from sensor nodes to cluster heads. The downside of ESPDA [13] and SRDA [14] is that they do not allow intermediate nodes to perform data aggregation. That is, sensor data can be aggregated only at the immediate data aggregator which significantly limits the benefit of data aggregation. Following section gives brief overview of the data aggregation protocols that do not require decryption of sensor data but also allow intermediate nodes to perform data aggregation.

6. SDA USING ENCRYPTED SENSOR DATA

By using traditional symmetric key cryptography algorithms, it is not possible to achieve end-to-end confidentiality and in-network data aggregation together. If the application of symmetric key based cryptography algorithms is combined with data aggregation, then the messages must be encrypted hop by-hop. This means that, to perform data aggregation, intermediate nodes have to decrypt each received message, then aggregate the messages according to the corresponding aggregation function, and finally encrypt the aggregation result before forwarding it. Clearly, this is not an energy efficient way of performing secure data aggregation and it may result in considerable delay. In addition, this process requires neighboring data aggregators to share secret keys for decryption and encryption. In order to achieve end-to-end data confidentiality and data aggregation together without sharing secret key among data aggregators, privacy homomorphism cryptography has been used.

Concealed Data Aggregation (CDA) proposed by D westhoff et al [14] uses an additive and multiplicative homomorphic encryption scheme that allows the aggregator to aggregate encrypted data. End-to-end encryption solutions for convergecast traffic in wireless sensor networks that support in-network processing at forwarding intermediate nodes is known as Concealed Data Aggregation (CDA) [18]. Sensor nodes share a common symmetric key with the base station that is kept hidden from intermediate aggregators. The major contribution of this work is the provision of end-to-end encryption for reverse multicast traffic between the sensors and the base station. Data aggregators carry out aggregation functions that are applied to cipher texts (encrypted data). This provides the advantage that intermediate aggregators do not have to carry out costly decryption and encryption operations. Therefore, data aggregators do not have to store a sensitive cryptographic key which ensures an unrestricted aggregator node election process for each epoch during the wireless sensor network's lifetime. CDA is light weight protocol which is providing only confidentiality.

Castelluccia et al [15] proposed (EDA) an efficient aggregation of encrypted data in wireless sensor networks based on homomorphic encryption. This approach uses different keys per sensor node at the cost of mandatory transmission of the sensor ID list of the encrypting nodes. This allows an aggregator to execute the aggregation function and aggregate the encrypted data that are received from its children with no need for decryption and to recover the original messages. It uses a modular addition instead of the Exclusive-OR operation that is found in the stream ciphers. Thus, even if an aggregator is being compromised, original messages can not be revealed by an attacker.

S. Ozdemir [16] proposed data aggregation protocol, called CDAP which takes advantage of asymmetric key based privacy homomorphic cryptography to achieve end-to-end data confidentiality and data aggregation together. Asymmetric cryptography based privacy homomorphism incurs high computational overhead which cannot be afforded by regular sensor nodes with scarce resources. To solve this problem, CDAP protocol employs a set of resource-rich sensor nodes, called aggregator nodes (AGGNODEs), for privacy homomorphic encryption and aggregation of the encrypted data. In CDAP, after the network deployment each AGGNODE establishes pair-wise keys with its neighboring nodes so that neighboring nodes can send their sensor readings securely. In data collection phase of CDAP, each AGGNODE queries its neighboring nodes. Each neighboring node encrypts its data (using RC5 algorithm) sends the encrypted data to its AGGNODE. The AGGNODE decrypts all the data received from its neighbors, aggregates them, and encrypts the aggregated data using the privacy homomorphic encryption algorithm. Once the data are encrypted with the privacy homomorphic encryption algorithm, only the base station can decrypt them using its private key.

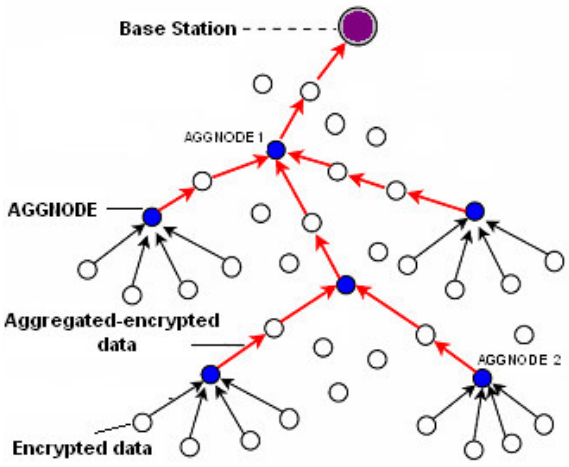

Fig. 3: Concealed data aggregation protocol

Due to homomorphic property, intermediate AGGNODEs can aggregate those encrypted data during data forwarding. Therefore, the data collected by sensor nodes are aggregated by AGGNODEs as they travel towards the base station. The base station decrypts the final aggregated data using its private key. An illustrative example of data aggregation in CDAP is given in Figure 3. Due to the computational overhead of privacy homomorphic encryption algorithms, in CDAP, only AGGNODEs are allowed to encrypt and aggregate the collected data using privacy homomorphic algorithms. Therefore, during the initial data collection phase of the protocol CDAP, sensor nodes use symmetric key algorithms for encryption. Due to the symmetric encryption, a compromised AGGNODE may disclose the secrecy of its neighboring nodes' data or inject false data into the data. However, the authors argue that the effect of this attack is local, and hence, it can be tolerated.

Existing privacy homomorphism based in-network processing protocols can only work for some specific query-based aggregation functions, e.g., sum, average, etc. Hence, instead of privacy homomorphism W zhang et al [17] use digital watermarking and propose an end-to-end confidentiality and authentication that provides inherent support for data aggregation. Basic idea of this work is to modulate authentication information as watermark and superpose this information on the sensory data at the sensor nodes. The watermarked data can be aggregated by the intermediate nodes without incurring any en route checking. In order to check whether the data has been altered by the compromised nodes, upon reception of the sensory data, the data sink is able to authenticate the data by validating the watermark. More specifically, the proposed technique visualizes the sensory data gathered from the whole network at a certain time snapshot as an image, in which every sensor node is viewed as a pixel with its sensory reading representing the pixels intensity. Since senor data is represented as an image digital watermarking can be applied to this image. In order to balance the energy consumption among sensor nodes, a direct spread spectrum sequence (DSSS) based watermarking technique is used. While each sensor node appends a part of the whole watermark into its sensory data, verification of watermark which requires an extensive computational resource is left to the sink. The proposed scheme adopts the existing image compression schemes as the aggregation functions to reduce network load while retaining the desired details of the data. Moreover, using a DSSS based watermarking scheme, the proposed technique is enabled to survive a certain degree of distortion and therefore naturally support data aggregation.

7. ANALYSIS OF SECURE AGGREGATION SCHEMES

Secure aggregation method proposed by Hu et al[3] is hop by hop secure data aggregation protocol which does not provide confidentiality and sensor nodes require buffer to store secrete keys. For WSN this scheme is not suitable because it consumes more power and resources. ESA [4] is improved method but still it consumes more power and resources comparatively. SIA [5] offers data integrity, authentication, data freshness, and confidentiality (if required). It is based on aggregate-commit-prove. SIA is also a hop by hop secure data aggregation protocols. SecureDAV [7] provides data confidentiality, data integrity, and source authentication. However, the scheme incurs high communication overhead on data validation and supports only the average aggregation function. WDA [8] sends multiple copies of the original aggregated result, to the aggregator point. The aggregator point is fixed and responsible to handle so much traffic, the aggregator resources will not last long. The proposed protocol offers only integrity property. SAT [9] uses weighted voting scheme to decide whether the data aggregator is properly behaving or is cheating. If the data aggregator is a misbehaving node, then SAT is rebuilt locally so that the misbehaving data aggregator is excluded from the aggregation tree. In SELDA [10] sensor nodes observe actions of their neighboring nodes to develop trust levels for both the environment and the neighboring nodes. Sensor nodes employ monitoring mechanisms to detect node availability, sensing and routing, misbehaviors of their neighbors. It is hop by hop secure data aggregation protocol. In DAA [11] false data detection and data confidentiality increase the communication overhead. The drawback of ESPDA [12] and SRDA [13] is that they do not allow intermediate nodes to perform data aggregation. That is, sensor data can be aggregated only at the immediate data aggregator which significantly limits the benefit of data aggregation. CDA [14] is based on privacy homomorphism end to end secure data aggregation protocol. This protocol enables intermediate node to perform data aggregations. CDA is light weight Secure Data Aggregation protocol which is only providing confidentiality. The results show that encryption, decryption, and addition operations that are needed to implement Domingo-Ferrers function (PH) are much more expensive compared to those are necessary to perform symmetric key based RC5. This disadvantage is acceptable as CDA advantageously balance the energy consumption. Symmetric key based encryption solutions to perform hop-by-hop data aggregation results in shorter lifetime for data aggregator nodes. Therefore, as data aggregators are the performance bottleneck when maintaining a connected wireless sensor network backbone, it is preferable to employ CDA's asymmetric key based privacy homomorphism to balance the energy consumption of data aggregators. EDA [15] is end to end secure data aggregation scheme and it supports in-network data aggregation. Due to the increased message overhead per monitoring nodes, this approach does not scale well for large sensor networks. Existing secure data aggregation schemes only support limited aggregation function like sum, avg etc. so instead of privacy homomorphism, the authors [17] use digital watermarking and propose an end-to-end confidentiality and authentication that provides inherent support for data aggregation.

8. CONCLUSION

Aggregation of data is very crucial in sensor networks because of the scarcity of energy. Due to the deployment in open environments sensor nodes are vulnerable to number of attacks so aggregation process must be supplemented with strong security support. This paper reviews existing secure aggregation schemes in detail. Secure aggregation needs the bounded security requirements then data aggregation can be correlated with the requirements for the complete solution. End to end secure data aggregation protocols with privacy homomorphism are most suitable for WSNs as there is no compromise with data privacy at intermediate levels. Privacy homomorphism based aggregation seems most promising method for secure aggregation in WSNs as it tries to reduce the energy consumption with provision of data confidentiality. It also increases system flexibility against changing routes. We believe that our paper will encourage other researchers to consider the vital problem of secure information aggregation in sensor networks.

REFERENCE

[1] Suat Ozdemir, Yang Xiao,"Secure data aggregation in wireless sensor networks: A comprehensive overview", Elsevier B.V. *doi:10.1016/j.comnet.2009.02.023,2009*

[2] Hani Alzaid, Ernest Foo, Juan Gonzalez Nieto,"Secure Data Aggregation in Wireless Sensor Network: A Survey", *ACSC2008, Australia, January 2008.*

[3] L. Hu, D. Evans, "Secure aggregation for wireless networks", *SAINT Workshops, IEEE Computer society, pp. 384-395, 2003.*

[4] P. Jadia, A. Mathuria,"Efficient secure aggregation in sensor networks", HiPC, *Vol. 3296 of Lecture Notes in Computer science, Springer, PP. 575-578*

[5] B. Przydatek, D. Song, A. Perrig,"SIA: secure information aggregation in sensor networks", in 'SenSys', *ACM, pp. 255-265, 2003.*

[6] A. Perrig, R. Szewczyk, J.D.Tygar, V.Wen, D.E.Culler,"SPINS: security protocols for sensor networks", *Wireless network 8(5), 521-534.*

[7] A. Mahimkar, T.S. Rappaport,"SecureDAV: a secure data aggregation and verification protocol for wireless sensor networks", *IEEE Global Telecommunications Conference (Globecom), November 29-December 3, Dallas, TX, 2004.*

[8] W. Du, J. Deng, Y.S. Han, P.K. Varshney,"A witness-based approach for data fusion assurance in wireless sensor networks", *IEEE Global Telecommunications Conference (GLOBECOM '03), 2003, pp. 1435-1439.*

[9] K.Wu, D. Dreef, B. Sun, Y. Xiao, "Secure data aggregation without persistent cryptographic operations in wireless sensor networks", *Ad Hoc Networks 5 (1) (2007) 100-111.*

[10] S. Ozdemir,"Secure and reliable data aggregation for wireless sensor networks", *in: H. Ichikawa et al. (Eds.), LNCS 4836, 2007, pp. 102-109.*

[11] H. am, S. Ozdemir,"False data detection and secure data aggregation in wireless sensor networks", *in: Yang Xiao (Ed.), Security in Distributed Grid Mobile and Pervasive Computing, Auerbach Publications, CRC Press, 2007.*

[12] H. am, S. Ozdemir, P. Nair, D. Muthuavinashiappan, H.O. Sanli, "Energy-efficient and secure pattern based data aggregation for wireless sensor networks", *Comput. Commun., Elsevier 29 (4) (2006) 446-455.*

[13] H.O. Sanli, S. Ozdemir, H. am,"SRDA: secure reference-based data aggregation protocol for wireless sensor networks", *in: IEEE VTC Fall Conference, Los Angeles, CA, 26-29 September 2004, pp. 4650-4654.*

[14] D. Westhoff, J. Girao, M. Acharya,"Concealed data aggregation for reverse multicast traffic in sensor networks: encryption key distribution and routing adaptation", *IEEE Trans. Mobile Comput. 5 (10) (2006) 1417-1431.*

[15] C. Castelluccia, E. Mykletun, G. Tsudik,"Efficient aggregation of encrypted data in wireless sensor networks", *in: 'MobQuitous' IEEE Computer Society, PP. 109-117. 2005.*

[16] S. Ozdemir,"Concealed data aggregation in heterogeneous sensor networks using privacy homomorphism", *in: IEEE International Conference on Pervasive Services, Istanbul, Turkey, 2007, pp. 165-168.*

[17] W. Zhang, Y. Liu, S.K. Das, P. De,"Secure data aggregation in wireless sensor networks: a watermark based authentication supportive approach", *Elsevier Pervasive Mobile Comput. 4 (2008) 658-680.*

[18] Steffen Peter, Dirk Westhoff, Claude Castelluccia, "A Survey on the Encryption of Convergecast Traffic with In-Network Processing", *IEEECS Log Number TDSC-0025-0207. Mar.2008.*