ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 4, Issue 2, February 2019

A Survey On Secure Data Aggregation In Wireless Sensor Networks

[1] Volga A Mohanan
[1] Karunya Institute Of Technology And Sciences
Coimbatore,India

Abstract: ***A wireless sensor network is a collection of spatially distributed sensor nodes for monitoring physical environmental conditions such as pressure, temperature or humidity. To decrease the energy consumption and to increase the lifetime of wireless sensor network a mechanism called data aggregation is introduced. Data aggregation is a process of aggregating the data from different sensor nodes so as to reduce the transmission overhead. However, this data aggregation creates new security challenges. In this paper, we are doing a survey on existing secure data aggregation protocols.***

Keywords: Data aggregation, wireless sensor network, privacy homomorphism.

I. INTRODUCTION

Wireless Sensor Network is a collection of sensors deployed in a physical environment in order to gather sensed data. This data is then transmitted to a base station for further processing. Wireless Sensor Network has many applications in the area of military, agriculture, disaster management, and healthcare. Sensor nodes are limited in cost, battery control, size, and memory. Since the distribution of sensor nodes in WSN is dense, there is a chance for overlapping sensing ranges among neighboring sensor nodes. This leads to data redundancy and transmission of the same data leads to an increase in the amount of data transmission which again leads to more energy consumption. One of the solutions to this problem is data aggregation. Data aggregation is the process of combining data from different sensor node using aggregation functions like min, max, average, and sum. The data aggregation mechanism can eliminate the data redundancy in the transmitted data, can reduce energy consumption and thus increase the network lifetime.

Based on the topology used for aggregation the data aggregation protocols are divided into two types. They are cluster-based data aggregation protocols and tree-based data aggregation protocols. In cluster-based data aggregation protocols, the cluster head performs the data aggregation whereas in tree-based data aggregation protocols the intermediate nodes will perform data aggregation

In wireless sensor networks, the benefit of data aggregation rises if the intermediate sensor nodes do data aggregation when data are being forwarded to the base station. However, this data aggregation operation improves energy utilization and bandwidth it may adversely affect accuracy rate, fault-tolerance, delay and security. Moreover, it is a challenging task to provide data authentication since the data aggregation results in alteration of sensed data. Since it is not possible to sacrifice security for data aggregation, there proposed different security protocols. The security protocols prefer to send sensed data in an encrypted format and will be decrypted by the base station. On the other hand, data aggregation protocols prefer plain data to implement data aggregation so that energy consumption can be reduced. So there emerges a strong conflict between data aggregation and security protocols. In order to achieve security, the data aggregation and security protocols must be designed together. In this paper, we are comparing different existing data aggregation protocols.

II. Security Requirements Of Wireless Sensor Networks

Unlike Traditional network, the WSN have different security issues that should be explored. Here present essential security requirements of wireless sensor networks.

2.1 Data confidentiality

Privacy of the data is most important. So in order to maintain the privacy, the data aggregation is done over the encrypted data. Thus the sensitive information can be protected from the unauthorized entities.Data integrity Data integrity ensures that the message being transferred is never corrupted by malicious nodes.

2.2 Data Authentication

Authentication enables verification of the peer node it is communicating with, so as to eliminate the nodes with a false identity. By secure authentication, it is possible to identify maliciously injected or spoofed packets.

2.3 Availability

The Availability determines whether a node can use the resources and it assures whether the network is available for communication. It guarantees the survivability of network services against Denial-of-Service (dos) attack.

III. Security Requirements of Wireless Sensor Networks

Unlike Traditional network, the WSN have different security issues that should be explored. Here present essential security requirements of wireless sensor networks.

3.1 Hop-By-Hop Encrypted Data Aggregation

In this, the sensor node will encrypt the data and will send the encrypted data to the aggregator node, and then the aggregator node will decrypt the data and performs aggregation over this decrypted data. After that, it will encrypt the aggregation result again. At last the sink node will get the final encrypted result and decrypts it. Here because of the decryption of sensor data in the aggregator node, the aggregator nodes are vulnerable to attack.

3.2 End-To-End Encrypted Data Aggregation

Here the aggregator node aggregates the encrypted sensor readings without decrypting them. So this method assures an end to end privacy between nodes.

IV. Literature Survey

Currently, there are some existing works for secure data aggregation. Out of that some of the protocols only addresses data confidentiality like End to End secure data aggregation protocols. In this, the security is assured by applying the aggregation function directly to the encrypted data. Some of the protocols under End to End secure data aggregation protocols includes CDAP, SEDA, RCDA, and Sen-SDA

Ozdemir [3] has proposed the CDAP protocol to facilitate the aggregation process and to obtain a safe end to end transmission between the base station and the nodes of the network. This model use privacy homomorphism to provide end to end data protection and also to operate directly on cipher texts while providing a secure data aggregation process. The protocol is applied to a heterogeneous WSN where powerful nodes called aggnodes are utilized.

Huang et al. [5] have proposed this protocol to eliminate redundant sensor readings without encryption and to maintain data confidentiality during their transmission. The proposed protocol ensures data security and confidentiality. An aggregation mechanism is proposed to maintain data confidentiality and secrecy that is the sensor nodes encrypt data before transmitting to the aggregation node. Thus the data remains undisclosed to the aggregation node.

Chen et al. [8] proposed RCDA to ensure data integrity and authenticity. Normally in other protocols, the base station cannot recover the aggregated data but in this model, the base station can recover all the sensed data for verifying data integrity even if they are aggregated.

Shim [9] proposed Sen-SDA Sen-SDA is a secure data aggregation mechanism based on the combination of the homomorphic encryption scheme (HE), EC-El Gamal, an identity-based signature scheme (IBS), for finding invalid signatures a batch verification technique with binary quick search (BQS) is also introduced. The proposed homomorphic encryption scheme is combined with a signature scheme to ensure a high degree of security. Since the homomorphic encryption reduces the use of aggregation function, this leads to the reduction of the aggregation accuracy also.

Hong Zhong et al [17] proposed an efficient and secure recoverable data aggregation scheme for heterogeneous wireless sensor networks by combining homomorphic encryption technology with a signature scheme. In this model, the base station can

recover the original sensing data and thus the base station can identify the origin and validity of messages received. However, the recoverable sensing data approach is very inefficient for large-sized messages.

Other secure data aggregation protocols like DAA and IPHCDA removes the data redundancy and preserve additional energy consumption. Suat Ozdemir [6] proposed Integration of False Data Detection with Data Aggregation and Confidential Transmission in Wireless Sensor Networks. This model presents a data aggregation and authentication protocol (DAA) to detects any false data injected into compromised nodes and the detected false data are not forwarded beyond the next data aggregator on the path. DAA can reduce the amount of transmitted data by up to 60%.

Suat Ozdemir and Yang Xiao [7] proposed a integrity protecting hierarchical concealed data aggregation for wireless sensor networks. This model allows the aggregation of data packets that are encrypted with different encryption keys and provides integrity protection for the aggregated data. IPHCDA protocol Employs a privacy homomorphic encryption scheme and message authentication codes (MAC) and this protocol allow hierarchical aggregation of encrypted sensor data while providing confidentiality and integrity.

The secure access control is very important for data aggregation, particularly for sensitive applications. The aggregation accuracy with access control could save energy and improve the quality of service. Qiang Zhou et al [13] proposed a secure-enhanced data aggregation based on ECC in Wireless Sensor Networks. Elliptic Curve Cryptography (SEDA-ECC) is based on the principles of privacy homomorphic encryption (PH) and divide-and-conquer. SEDA-ECC includes six phases such as Key Generation Phase, Aggregation Tree disjoint phase, encryption phase, aggregation phase, decryption Phase and data integrity check phase. SEDA-ECC protocol can achieve the highest security level on the aggregated result.

The resource limitations of sensor nodes make symmetric key cryptography a better choice to employ as compared to asymmetric key cryptography. Therefore many researchers proposed data aggregation using symmetric key cryptographic protocols such as ESPDA and SAT. Hasan Cam et al [1] proposed an energy-efficient secure pattern-based data aggregation for wireless sensor networks (ESPDA).The ESPDA avoids the transmission of redundant data from the sensor nodes to the cluster-head. Here the cluster-heads are not required to examine the data received from the sensor nodes, instead, the cluster-heads compare the pattern codes received from the sensor nodes and decide on which sensor nodes the sensor data need to be transmitted.

Kui Wu et al [2] proposed a secure data aggregation without persistent cryptographic operations in wireless sensor networks. A secure aggregation tree (SAT) is proposed to detect and prevent cheating. In this model, the security is based on cheating detection instead of persistent data authentication.SAT includes three phases. The first phase is to build a SAT and monitor the behavior of each aggregation sensor node. In the second phase, a weighted voting scheme is proposed when the aggregated values are in doubt. If a misbehaving node is detected, a local recovery scheme is presented to re-build SAT by excluding that node in the third phase.SAT can reduce energy consumption and more importantly can save the CPU resource.

Anthonis et al [4] proposed cryptographic protocols to fight sinkhole attacks on tree-based routing in wireless sensor networks. Two cryptographic protocols models are introduced RESIST-1 and RESIST-0. RESIST-1 prevents a malicious node from modifying its advertised distance to the sink by more than one hop and RESIST-0 is a Complex reconfiguration protocol. The main goal of both protocols is to provide continuous operation by improving resilience against, rather than detection of these attacks. The cryptographic protocols are used for improving resilience against sinkhole attacks in wsns.

The homomorphic encryption and Message Authentication Codes (MAC) were introduced(Othman et al [12]) to improve the authentication and integrity for secure data aggregation in wsns. However, the MAC only attempted to handle the message-authentication problem without addressing other security constraints such as confidentiality. In addition, communication and computational overheads were not properly handled, which could lead to additional energy consumption (Ramotsoela et al [15]).

Another homomorphic encryption based mechanism was proposed by Prathima et al [16] for secure data aggregation for multiple queries in wireless sensor networks. The authenticated query propagation combined with homomorphic encryption provide secure data aggregation at low energy consumption. However, this method enforces all nodes to be authenticated and hence incurs a small delay.

Some mechanisms (Sankardas et al [14], Othman et al [10], Rezvani et al [11]) have been proposed to address confidentiality and overcome the problem of false sub-aggregate values contributed by bargained sensor nodes. However, the existing approaches handle the confidentiality or energy efficiency but do not address the accuracy and communication overhead during the secure data aggregation operation.

V. Conclusion

An extensive literature survey is presented by summarizing various secure data aggregation protocols. This paper mainly focus on end to end encrypted data aggregation scheme which is based on privacy homomorphism. Because privacy homomorphism allow aggregation on encrypted data. The end to end encrypted data aggregation scheme ensures more security than compared to Hop byhop Encrypted Data aggregation.

References

1. Hasan Cam, Suat Ozdemira, Prashant Nairb, Devasenapathy Muthuavinashiappana, H.Ozgur Sanlia, (2005) "Energy-efficient secure pattern based data aggregation for wireless sensor networks," Computer Communications 29 446–455.
2. Kui Wu: Dennis Dreef, Bo Sun, and Yang Xiao,(2006) "Secure Data Aggregation without Persistent Cryptographic Operations in Wireless Sensor Networks", IEEE
3. Ozdemir, (2007) "Concealed Data Aggregation in Heterogeneous Sensor Networks using Privacy Homomorphism" © I EEE.
4. Anthonis Papadimitriou, Fabrice Le Fessant, Aline Carneiro Viana, Cigdem Sengul, (2009) "Cryptographic Protocols to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Networks," © I EEE.
5. Shih-I Huang ,Shiuhpyng Shieh ,J. D. Tygar, (2009) "Secure encrypted-data aggregation for wireless sensor networks," In Wireless Networks, pp. 915-927.
6. Suat Ozdemir, and Hasan Çam, (2010) "Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks," IEEE, VOL. 18, NO. 3.
7. Suat Ozdemir ,Yang Xiao, (2011) "Integrity protecting hierarchical concealed data aggregation for wireless sensor networks," Computer Networks 55 (2011) 1735–1746
8. Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin, and Hung-Min Sun,(2012) "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks," IEEE VOL. 23, NO. 4
9. Kyung-Ah Shim and Cheol-Min Park,(2007) "A Secure Data Aggregation Scheme based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks," IEEE VOL. 6, NO. 1
10. Abdelbasset Trad and Habib Youssef,(2013) "Secure and energy-efficient data aggregation for wireless sensor networks," Int. J. Mobile Network Design and Innovation, Vol. 5, No. 1
11. Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino,and Sanjay Jha,(2013) "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks," IEEE
12. Soufiene Ben Othman, Abdelbasset Trad, Habib Youssef and Hani Alzaid,(2013) "Secure Data Aggregation with MAC Authentication in Wireless Sensor Networks," IEEE
13. Qiang Zhou, Geng Yang and Liwen He (2014) "A Secure-Enhanced Data Aggregation Based on ECC in Wireless Sensor Networks," Sensors, 14, 6701-6721.
14.] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia,(2014) "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact," IEEE VOL. 9, NO. 4.
15. T.D. Ramotsoela and G.P. Hancke,(2015) "Data Aggregation Using Homomorphic Encryption in Wireless Sensor Networks," © IEEE.
16. E. G Prathima,T. Shiv Prakash, K. R. Venugopal, S. S. Iyengar and L. M. Patnaik,(2016) "SDAMQ: Secure Data Aggregation for Multiple Queries in Wireless Sensor Networks," Procedia Computer Science 89 (2016) 283 – 292.