Indian Journal of Science and Technology, *Vol 10(4), DOI: 10.17485/ijst/2017/v10i4/110668, January 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Implementing Privacy Homomorphism in Data Aggregation for Wireless Sensor Networks

Y. Sandeep* and Mohammed Ali Hussain

Department of Electronics and Computer Engineering, KL University, Vijayawada - 522502, Andhra Pradesh, India; ysreddy.210@outlook.com, dralihussain@kluniversity.in

Abstract

Objective: To design and implement a methodology to achieve privacy and security of data in Wireless Sensor Network (WSN) through malleability resilient concealed data aggregation protocol. **Analysis:** The aim of concealed collection of data in WSN is to provide privacy preservation of the data at both Intermediate Nodes (IN) and at Base Stations (BS) while aiding in-network data aggregation. The data aggregation which can be executed using privacy homomorphism at both INs and BS and is naturally malleable as the encrypted data was processed at INs without decrypting. Hence it is dreadful challenge to recognize constraints like point-to-point privacy and integrity in carrying out the aggregation. **Methodology:** In this paper, for protecting against passive and active adversaries in the network we propose a malleability resilient concealed data aggregation protocol. The proposed protocol protects the data from the opposing targets like privacy at both IN and at base station, point-to-point integrity, point-to-point privacy, replay protection, and aggregation. **Findings/ Improvements:** The major contribution of the proposed scheme verifies freshness of the data before performing encrypted data at INs as well as at BS. It also protects the data from the insider attacks as well as the outside. Thus, the protocol improves the privacy homomorphism of the data and verification of data freshness continuously at INs and also at BS.

Keywords: Concealed Data Aggregation, Malleable, Privacy Homomorphism, Point-to-Point Privacy, Point-to-Point Integrity, Secure Data Aggregation, Wireless Sensor Networks

1. Introduction

Wireless sensor networks which may also known as actuators which helps to supervisor physical and environmental conditions mainly temperature, pressure, sound, etc., these information are been successfully sends to the base station. The WSN are constructed of "nodes" and these are bi-directional in nature. Each sensor node consists a radio transceiver with an antenna, a micro controller, and energy source (battery). Simple star network and multi hop mesh network is used in WSN.

Energy is the most specific circumstance that has to be considered which has a serious effect on the WSN life time. Radio frequency performance in the network consumes more energy than instructions of the CPU. Several methods have been prospective to improvise the energy efficiency of WSN[1,2]. Hence to improve the energy efficiency users need to reduce the traffic communication and it has been crucial. One of the methods used to reduce traffic communication i.e., "Data Aggregation (DA)"[3,4]. The main objective of DA is to scale down the traffic where security and privacy features add additional communication traffic to the network. In-network processing readings of the senor nodes at the INs are collected and forward the aggregate results to the BS.

Secure DA mainly focuses on two objectives, 1) Data Aggregation and 2) Security. Security of DA in the network can be classified based on either hop-by-hop or point-to-point. Hop-by-hop secure DA contemplate that INs are realistic because these INs decrypt sensor raw readings; aggregate and encrypt the readings and forward them to the BS. This intermediate node becomes problematic if they are compromised, although the hop-by-hop is applicable. The aggregated data can be revealed

**Author for correspondence*

to the antagonist by the compromised intermediate nodes and it may lead to the catastrophic effect on the activity of WSNs in an unfriendly environment. Only outside antagonist are considered by the hop-by-hop message authentication, whereas there exist many malicious INs which can successfully modify the readings of the sensor without being detected. Hence, the privacy of sensor readings must established by the user at INs becomes a paramount security object in data centric networks. Point-to-point secure DA which can know in another way by concealed DA which helps to protect the sensor reading privacy while implementing and executing data collection[4,5].

Privacy homomorphism is another form of encryption of data that allow computation is carried out based on cipher text[6,7]. It can access the encrypted data at INs without any need of decrypting them. Privacy homomorphism helps in protecting the sensor readings from the passive antagonist, and it may be responsible to active antagonist[8]. Algorithms which can execute privacy homomorphism are naturally malleable. Any secret information is not required by the aggregator node to aggregate the data packets, and in middle any mischievous node can also has a chance to inject false data packets into the channel to pervert correct data packets. In data-centric networks, information is assumed to be modified at each hop, whereas the traditional mechanism used to ensures integrity of data that is, data cannot be modified when it is being transferred from leaf node to the BS.

Another vital security aspect that is to be considered in WSNs is replay protection. As sensor readings can be aggregated, at INs the data freshness verification becomes more compulsory[9]. A counter or a nonce is used by hop-by-hop secure DA protocol to provide replay protection. Sensor readings remain encrypted at INs in point-to-point secure DA where replay protection cannot be adopted directly. So, malicious INs also a challenging task against hop-by-hop replays protection. So, before processing the encrypted data there is a need to verify the data freshness and it becomes more vital objective.

In this paper, for protecting privacy of the data and integrity of sensor readings we prospective (MRPCDA). The integrity verification cannot be provided both at INs and also at the BS by using single authentication mechanism. For verifying the integrity of the data at INs and at also at BS we may use different and separate primitives. The prospective protocol provides protection against outside antagonist by using a symmetric-key based MAC[10] for integrity at layer-wise across active inside antagonist by using holomorphic MAC[10] for protecting the network. The prospective protocol can also provide protection from active and passive antagonist. The point-to-point privacy and integrity in reverse multicast traffic when there exist some adversaries can also be achieved by the prospective protocol. Moreover, the major contribution of the prospective solution is that the data freshness is verified before performing encrypted data at Ins along with BS. Thus, the protocol improves the privacy homomorphism of the data and verification of data freshness continuously at INs and also at BS.

2. Extant Method

In[11] approached a solution malleability resilient premium concealed data aggregation (MRPCDA) which verifies sensor readings integrity at BS. This approach provides point-to-point integrity and only data is protected from outside antagonist and abort to detect tempered data packets which are present inside antagonist. In extension, integrity verification is done only at the BS and maliciously injected information packets should forwarded to BS for verification of integrity. So, energy of the sensor node depletes due to redundant communication.

3. Prospective protocol

In[12] introduces the requirement for encrypted data and the way to resolve that data encryption employing cryptography and is can also be termed as privacy homomorphism. Without encrypting the data using privacy homomorphism the data can be processed in a raw form. Data encryption can perform additive and multiplicative operations over encrypting the data in the network. Ɗs' represents the encryption function and Ɗs" represents the corresponding decryption function. In usage of symmetric keys based cryptosystems the keys which are generated are identical s'=s". Where as in usage of public key based cryptosystems the generated keys are not identical.

$$\varepsilon s'(p1) \oplus \varepsilon s'(p2) = \varepsilon s'(p1 \otimes p2) \quad (1)$$

as shown in eq. 1 the operands used for generating keys for encryption process may not have any brunt on the decrypting the data. The operator used in Domingo-Ferrer's cryptosystems remains the same where as in the case of Paillieretal.'s it can be different.

$Ds'(\varepsilon s'(p1) + \varepsilon s'(p2)) \bmod Q = Ds'(\varepsilon s'(p1+p2)) \bmod Q$ (2)

$Ds''(\varepsilon s'(p1) \times \varepsilon s'(p2)) \bmod Q^2 = Ds''(\varepsilon s'(p1+p2)) \bmod Q$ (3)

Equation 2 represents the symmetric-key cryptosystems which requires the same key "s'" for both encryption and decryption process where as in Eq.3 , asymmetric- key based cryptosystems requires "s'" for encrypting the data and "s''" for decrypting the data. The elliptic curve cryptosystem is based on public key which can incorporate additive privacy homomorphism[13]. This scheme is used to protect the privacy of the data in the network while the Homomorphic MAC can be utilized to crosscheck the authenticity and originality of aggregated cipher text.

Concealed DA naturally uses malleably privacy homomorphism which makes it possible for sensor readings to be accessible to the attackers in the network. The privacy homomorphism helping aggregating the cipher texts in the genuine aggregator nodes also includes helping in modifying the cipher texts by maliciousant agonist. Therefore, it is necessary to ensure the integrity of the sensor readings before processing them to INs and point-to-point integrity verification need some conditions to be fulfilled. 1) Each IN has to authenticate and ensure the integrity of aggregated, original readings which are handed over to its child nodes. 2) The verification of aggregated sensor data is the authentic portrayal of original sensor readings that should be ensured by the base station.

The fulfilment of discussed constraints not only conserve the purity of the readings but it also assists in downsizing the additional communication traffic by detecting the malicious packets which are near to their sources. Conservative secure DA algorithm provides integrity verification either at the INs or at the BS and there is a need to ensure the integrity either at the IN or at the BS. Single/One-Way authentication scheme cannot ensure the integrity at IN as well as BS. So, to provide integrity we use pair wise symmetric keys at INs and homomorphic MAC at the BS as to provide integrity.

4. System Architecture

Figure 1 shows the individual sensors nodes can be aggregated into different groups based on the information gathered by specific variables of the nodes for the statistical analysis. Each individual node has its own information like a homomorphic MAC tag, ciphertext tag value, pair wise keys, encryption keys etc., each individual node encrypts the information and it will pass to the parent node or to the next node. In the parent node it decrypts the data using pairwise-keys, homomorphic MAC tags and it refreshes the information, verifies the information and then it decrypts the information and sends it to the next node and this will be continued until the information of all nodes reaches to the base station. Encryption helps in providing the integrity from outside as well as inside antagonist. The information of all the nodes will be updated every second continuously.

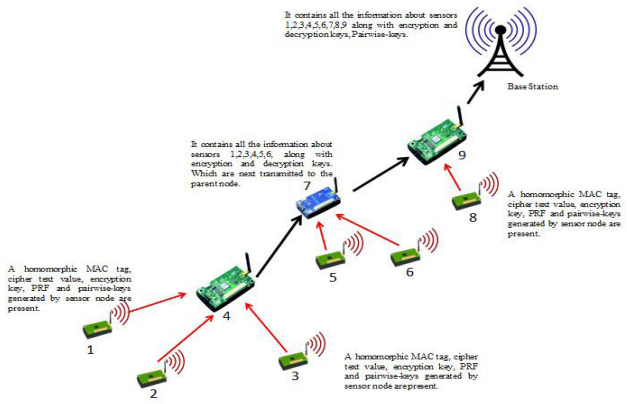

Figure 1. System Architecture.

4.1 Simulation

We implement our prospective system in NS simulator. Figure 2depicts the entire network developed in NS.

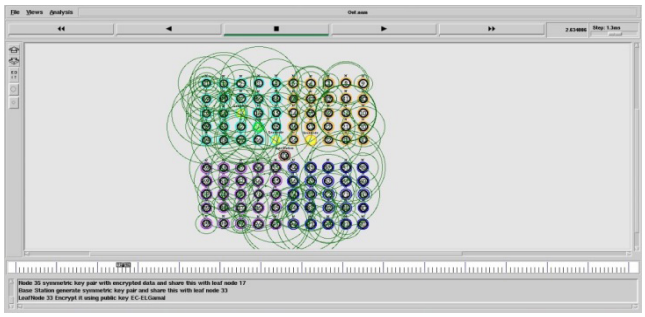

Figure 2. Formation of network.

Figure 2 explains how the sensor nodes forms the network and which node can act as leaf node and which node can be the neighbouring node and which node can be the base station. Figure illustrates how the data can be transferred between the leaf nodes and the neigh-

bour nodes. Plotting of graphs can be simulated between Communication overhead and communication overhead Data aggregation. We've taken two test case simulations in this work. There are three parameters against which we've plotted the graphs. Those three parameters are 'Distance between nodes', 'Bit Transmission rate' and 'Malleable Time'. The two test case plotting's illustrated below.

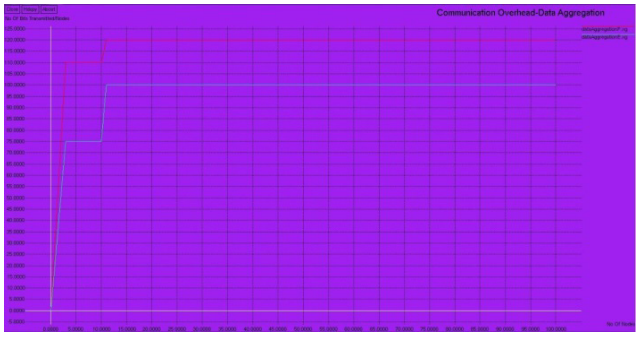

Figure 3. Simulation graph of Communication Overhead Data Aggregation.

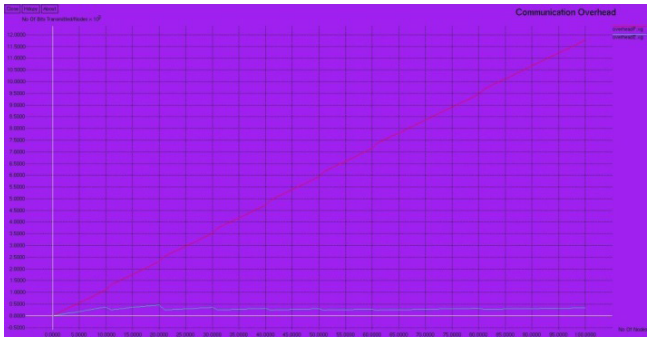

Figure 4. Simulation graph of communication overhead.

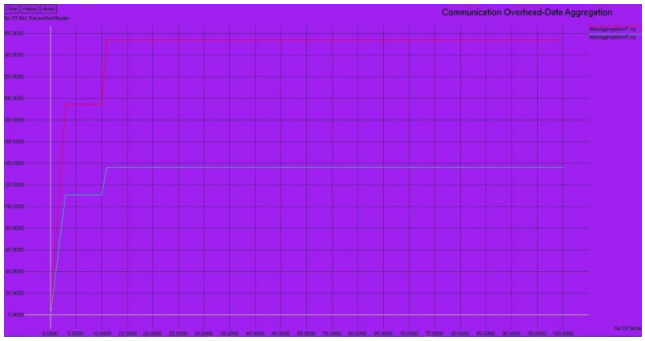

Figure 5. Simulation graph of Communication Overhead Data Aggregation.

Figure 3 and Figure 4 represents the graph between the communication overhead and the communication overhead data aggregation. It also represents the comparison between the existing system and also the prospective system. The parameter values for the network are taken as Distance between nodes is 110,Bit transmission rate is 10 and malleable time is 10.

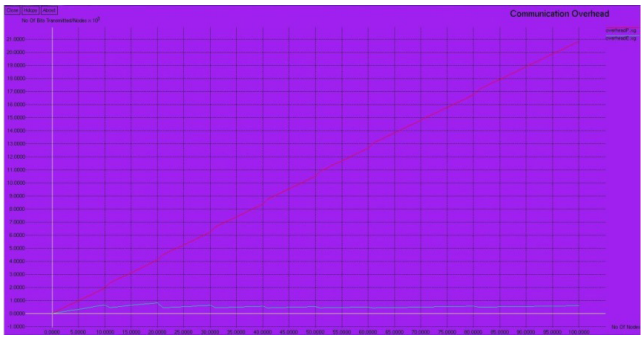

Figure 6. Simulation graph of communication overhead.

Figure 5 and Figure 6 represents the communication overhead and the communication overhead data aggregation. These two figures depict the plotting for another parameter test case values. In this case, Distance between nodes is 195, Bit transmission rate is 98 and malleable time is 59.

5. Security Analysis

In WSN security is one of the most important factors to be considered. Adverse and neglected distribution, in an inaccurate communication channel, inadequacy of environmental protection makes WSNs exposed to huge variety of different attacks. We are discussing different types of antagonist models present and their ability to cast various attacks on the data.

5.1 Antagonist Model

In WSNs attacks classified into two types namely, passive and active attackers.

5.1.1 Passive Attacks

Are also known as network attacks where the system is monitored continuously and scanned for any open ports available for susceptibility. The main aim is to get the information about the target and there is no chance of data modification in this attack. Passive attackers may also figure out the traffic patterns as attackers may disturb the routing. The exposure of passive attackers will be more in wireless communication when compared with the wired communication. These passive attacks are fur-

ther classified into two types namely, active surveillance and passive surveillance.

5.1.2 Active Attack

Is a method in a network where the changes can be done to the data or data en route to the target by the hacker. In message modification the hacker alter address of the header to different destination or the hacker can modify the data present in it and modified data can be sending to the target. Generally, denial of service attack accomplished by hacker by amazing the more traffic to the target than it can handle, where large number of compromised systems attacks to a particular target.

6. Cryptographic Attacks and Antivenin

6.1 Malleability

In WSN's, cryptographic algorithm possess different property in which malleability is one undesirable among them. Any cryptosystem which can support privacy homomorphism in WSN is naturally malleable. That is, cryptosystems allows the attacker to modify the context of a message of encrypted data without the need of decrypting the message or without knowing the knowledge of secret keys. In order to process the encrypted data there won't be a need of any secret key. Hence, any of the malicious nodes present in the network can execute the operations which are executed by the normal nodes and it is vital to prevent those malicious nodes. In this paper, dual authentication mechanism is mainly used for safeguard against malicious antagonist. The prospective protocol may not help in preventing the malicious antagonist in DA but it can be able to detect those malicious antagonist and can able to delete those maliciously aggregated information at the immediate hop. The encryption using a pairwise-key ensures the shielding in opposition to unauthorized DA in the nodes by inside and outside antagonist.

6.2 Node Capture Attack

Node Capture Attack is an important aspect in WSNs, and these cannot be completely reduced and it can only be accomplished by means of a robust authentication mechanism. The implemented algorithm encrypts the sensor data using the EC-ELGamal cryptosystems and these can also be decrypted at the BS only and privacy of the sensor data at the INs are achieved. The prospective protocol uses a pairwise secret keys to encrypt a homomorphic MAC tags which establish the integrity of the data from the outside as well as inside antagonist. Compromised intermediate node in the network can also perform malicious aggregation of the data into original using genuine keys and these can be distinguishing easily at the urgent next hop.

6.3.Replay attack

In a replay attack the original data transmission is faulty or repeated or delayed data packets in the network using the genuine keys. It can also be triggered by the active inside antagonist along with the outside antagonist. So, pairwise- key is used for encrypting the cipher text-counter pair which establishes protection from the outside antagonist as well as inside antagonist without launching the replay attacks in the network.

6.4 Denial of Service Attacks (DOS)

There are a number of forms of DOS attacks that are present in the WSNs; one of the widely used attacks amongst them is against the non-replenishable deficient energy supply. Due to built-in resource limitations, nodes in the network are exposed to DOS attacks. In this type of attack, the more precious energy of the sensor nodes are tried to be wasted by the antagonist. In addition to it, an antagonist may also target nodes which are near the BS which shows their impact on the overall execution of the sensor network due to the catastrophic impact. The impact of the DOS attack can be reduced by employing the technique of load balancing and also by employing the symmetric-key based cryptosystems.

7. Conclusion

In this paper, we developed a malleability resistant concealed DA methodology. The security against these outside and inside antagonists have an important role in concealed data aggregation because of data aggregation schemes and data encryptions. Our developed system successfully achieves the desired objectives against both outside and inside antagonist. We employed various other homomorphic encryption and homomorphic MAC for executing the encrypted data processing. A collation

of the existing protocols demonstrates efficiency and viability of the developed system on resource restricted devices. We are successfully demonstrating that our developed system achieves the required security pre-requisites while improving the resource consumption in resource restricted networks. Experimental results shows that the developed system assures the prospective privacy objectives while executing aggregation tasks on sensor networks traffic in a more efficient and effective way than the existing methodology.

8. Acknowledgements

The authors are grateful to K L University faculties for constant instructions and support to project. Inputs and suggestions by Embedded Systems and Sensor Networks ESSN of K.L. University are duly acknowledged.

9. References

1. Thiriveni GV, Ramakrishnan M. Distributed Clustering based Energy Efficient Routing Algorithm for Heterogeneous Wireless Sensor Networks. Indian Journal of Science and Technology. 2016; 9(3):1–6.
2. Anastasi G, Conti M, Di Francesco M, Passarella A. Energy conservation in wireless sensor networks: A survey. Ad Hoc Networks. 2009; 7(3):537–68.
3. Fasolo E, Rossi M, Widmer J, Zorzi M. In-network aggregation techniques for wireless sensor networks: A survey. Wireless Communications. 2007; 14(2):70–87.
4. Sasirekha S, Swamynathan S. A Comparative Study and Analysis of Data Aggregation Techniques in WSN. Indian Journal of Science and Technology. 2015; 8(26):1–10.
5. Pandey GK, Singh AP. Energy Conservation and Efficient Data Collection in WSN-ME: A Survey. Indian Journal of Science and Technology. 2015; 8(17):1–11.
6. Saikeerthana R, Umamakeswari A. Secure Data Storage and Data Retrieval in Cloud Storage using Cipher Policy Attribute based Encryption. Indian Journal of Science and Technology. 2015; 8(S9):318–25.
7. Sarath Chandra MS, Raghava Rao K, Hussain MA. An Efficient Scheme for Facilitating Secure Data Sharing in Decentralized Disruption Tolerant Networks. Indian Journal of Science and Technology. 2016; 9(5):1–13.
8. Riverst RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms Foundations of Secure Computation. 1978; 4(11):169–80.
9. Hariharan R, Mahesh C, Prasenna P, Vinoth Kumar R. Enhancing Privacy Preservation in Data Mining using Cluster based Greedy Method in Hierarchical Approach. Indian Journal of Science and Technology. 2016; 9(3):1–8.
10. Agrawal S, Boneh D. Homomorphic MACs: MAC-based integrity for network coding. Proceedings of the 7th International Conference on Applied Cryptography and Network Security, ACNS'09, Lecture Notes in Computer Science. Paris-Rocquencourt: Springer. 2009; 5536. p. 292–305.
11. Westhoff D, Ugus O. Malleability resilient (premium) concealed data aggregation. Proceedings of the 4th IEEE International Workshop on Data Security and Privacy in Wireless Networks, D-SPAN'13. Madrid: IEEE. 2013:1–6
12. Riverst RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms Foundations of Secure Computation. 1978; 4(11):169–80.
13. Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation. 1987; 48(177):203–9.