ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Cryptography Based Data Aggregation Scheme for Data Integrity Analysis in Wireless Sensor Networks

R. Kaleeswari, M.N.Karuppusamy

PG Student, Sri Subramanya College of Engineering and Technology, Palani, Tamilnadu, India[1]

Research scholar, Sri Subramanya College of Engineering and Technology, Palani, Tamilnadu, India[2]

ABSTRACT: Several data aggregation schemes based on homomorphism encryption have been proposed and investigated on wireless sensor networks. These data aggregation schemes provide better security since cluster heads (aggregator) can directly aggregate the cipher texts without decryption. However, the base station only retrieves the aggregated result, not individual data, which causes two problems. First, the base station cannot retrieve the maximum value of all sensing data. Second, the base station cannot confirm data integrity and authenticity to each sensing sample. However, these schemes are not satisfy multi-application environments. These schemes become insecure in case some sensor nodes are compromised. To overcome these problem in our design, the base station can recover all sensing data even these data has been aggregated. This property is called "recoverable". The proposed scheme has three contributions. First, it is designed for a multi-application environment. The base station extracts application-specific data from aggregated cipher texts. Next, it mitigates the impact of compromising attacks in single application environments. Finally, it degrades the damage from unauthorized aggregations. The design has been adopted on both homogeneous and heterogeneous wireless sensor networks.

KEYWORDS: Data aggregation, Elliptic curve cryptography, homomorphic encryption, Integrity check, wireless sensor networks

I. INTRODUCTION

Wireless sensor networks (WSNs) consist of thousands of sensor nodes (SN) that gather data from deployed environments. Currently, there are plenty of rich applications proposed for WSNs, such as environment monitoring, accident reporting, and military investigation. Depending on the purpose of each application, SN is customized to read different kinds of data (e.g., temperature, light, or smoke). Typically, SN are restricted by the resources due to limited computational power and low battery supply; thus, energy saving technologies must be considered when design the protocols. For better energy utilization, cluster-based WSNs have been proposed. In cluster-based WSNs, SN resident in nearby area would form a cluster and select one among them to be their cluster head (CH). The CH organizes data pieces received from SN into an aggregated result, and then forwards the result to the base station based on regular routing paths.

The proposed scheme, called CDAMA, provides CDA between multiple groups. Basically, CDAMA is a modification from Boneh et al.'s PH scheme. Here, also suppose three practical application scenarios for CDAMA, all of which can be realized by only CDAMA. The first purpose is designed for multi-application WSNs. In practice, SN having different purposes, If apply conventional concealed data aggregation schemes the Cipher texts of different applications cannot be aggregated together; otherwise, the decrypted aggregated result will be incorrect. For instance, compromising a CH will allow adversaries to forge aggregated results as similar as compromising all its cluster members. The only solution is to aggregate the cipher texts of different applications separately. The second purpose is designed for single application WSNs. CDAMA mitigates the impact of compromising SN through the construction of multiple groups. An adversary can forge data only in the compromised groups, not the whole system. The last purpose is designed for secure counting capability. In previous schemes, the base station does not know how many messages are aggregated from the decrypted aggregated result; leaking count knowledge will suffer maliciously selective aggregation and repeated aggregation.

II. RELATED WORK

A. PRIVACY HOMOMORPHIC CRYPTOSYSTEM

Privacy homomorphic encryption (PH) is an encryption scheme with homomorphic property. The homomorphic property implies that algebraic operations on plaintexts can be executed by manipulating the corresponding ciphertexts; for instance, $DK(EK(m1) \otimes EK(m2)) = m1 \oplus m2$, where EK(.) is the encryption with key K, DK(.) is the decryption with key K, and _ and _ denote operations on ciphertexts and plaintexts, respectively. In general, operations $\otimes$ and $\oplus$ can be addition, multiplication, and so on. Similar to conventional encryption schemes, PH schemes are classified to symmetric cryptosystem when the encryption and decryption keys are identical, or asymmetric cryptosystem (also called public key cryptosystem) when the two keys are different. Symmetric PH schemes, such as Domingo-Ferrer scheme or Castelluccia et al.'s scheme, usually are more competitive in terms of efficiency than asymmetric schemes. The most notable asymmetric PH schemes are based on elliptic curve cryptography (ECC). Compared with RSA cryptosystems, ECC provides the same security with a shorter key size and shorter ciphertexts.

B. CDA BASED ON PH

Conventional hop-by-hop aggregation schemes are insecure because an adversary is able to forge aggregated results such as compromising all the AG's child nodes when he compromises the secret of an AG. To diminish this impact, PH schemes have been applied to WSNs. By PH schemes, SNs encrypt their sensed readings and allow AGs to homomorphically aggregate their ciphertexts without decryption. Therefore, compromising AGs earns no advantage of forging aggregated results. Westhoff et al. and Girao et al. proposed CDA based on symmetric PH to facilitate the aggregation of encrypted data. n these schemes, because all SN in a network only share a common key for encryption , an adversary can forge the aggregated results by simply compromising one SN.. In each transmission, individual SN generates a temporary key from a pseudo random number generator (PRNG) and adds its messages with the key under modulation. And the BS decrypts the ciphertext received by modular subtraction with all the temporal keys. If an adversary tries to forge aggregated results, he must compromise all SNs. However, their scheme cannot prevent the adversary from injecting forged data packets into the legitimate data flow.

III. SYSTEM MODEL

Here, we state two models for further uses, aggregation model and attack model. The aggregation model defines how aggregation works; the attack model defines what kinds of attacks a secure data aggregation scheme should protect from.

A. AGGREGATION MODEL

In WSNs, SN collect information from deployed environments and forward the information back to base station (BS) via multihop transmission based on a tree or a cluster topology. The accumulated transmission carries large energy cost for intermediate nodes. To increase the lifetime, tree-based or cluster networks force the intermediate nodes (a subtree node or a cluster head) to perform aggregation, i.e., to be aggregators (AG). After aggregation done, AGs would forward the results to the next hop. In general, the data can be aggregated via algebraic operations (e.g., addition or multiplication) or statistical operations (e.g., median, minimum, maximum, or mean). For example, an AG can simply forward the sum of numerical data received instead of forwarding all data to the next hop.

B.ATTACKER MODEL

First of all, we categorize the adversary's abilities as follows:

1. Adversaries can eavesdrop on transmission data in a WSN.
2. Adversaries can send forged data to any entities in a WSN (e.g., SN, AG, or BS).
3. Adversaries can compromise secrets in SNs or AGs through capturing them.

Second, we define the following attacks to qualify the security strength of a CDA scheme. Part of these attacks refers to Peter et al.'s analysis. Based on adversary's abilities and purposes, we further classify these attacks into three categories. In the first category A, an adversary wants to deduce the secret key (i.e., decrypting arbitrary ciphertexts).

Category A consists of four attacks that are commonly used in qualifying an encryption scheme. In practice, the first two attacks are feasible in WSNs. Here, we use them to qualify the underlying homomorphic encryption schemes. In category B, an adversary wants to send the forged messages to cheat the BS even though she does not know the secret key. This category consists of two attacking scenarios based on specific features deriving from PH schemes. The last category C consists of three attacks and considers the impact of node compromising attacks. The first attack is the case of compromising an AG, and the last two attacks are cases of compromising an SN. We discuss them separately because they store different secrets in the PH schemes.

IV. OUR PROPOSED SCHEME

A. Main Idea

The main goal of our framework is to check the integrity of data in wireless sensor networks. In this system, introduce a concept named Recoverable Concealed Data Aggregation. A base station can recover each sensing data generated by all sensors even if these data have been aggregated by cluster heads. Here two functionalities are provided. First, the base station can verify the integrity and authenticity of all sensing data. Second, the base station can perform and aggregation functions on them. Then, propose two RCDA schemes named RCDA-HOMO and RCDA-HETE for WSN.. In the security analysis, demonstrate that the proposed schemes are secure under our attack model. Through experiments, show that the performance of our design reasonable and affordable.

ARCHITECTURE

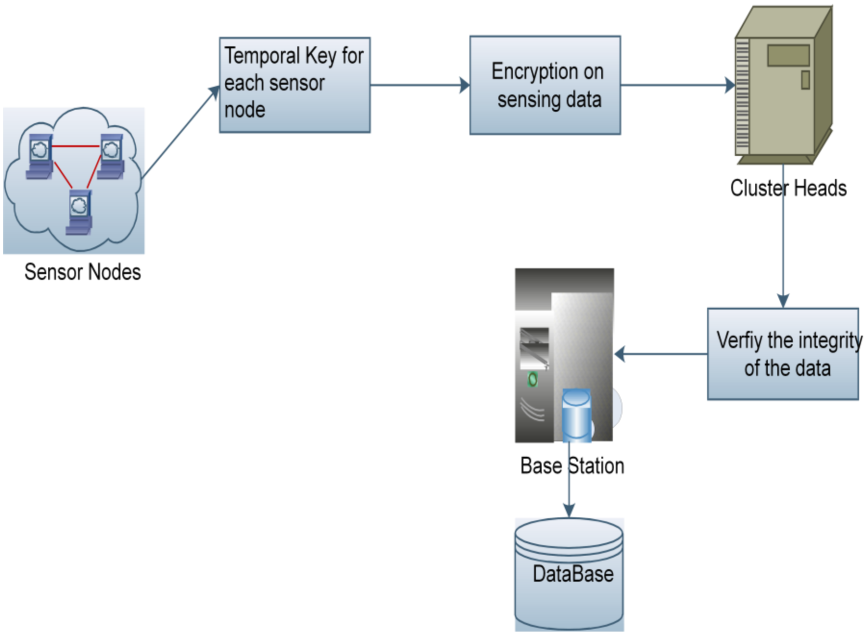
Temporal Key for each sensor node
Encryption on sensing data
Cluster Heads
Sensor Nodes
Verfiy the integrity of the data
Base Station
DataBase

Fig 1 The proposed framework for Data Integrity analysis in wireless sensor networks

The proposed scheme, called CDAMA, provides CDA between multiple groups. Basically, CDAMA is a modification from Boneh et al.'s PH scheme. Here, also suppose three practical application scenarios for CDAMA, all of which can be realized by only CDAMA. The first purpose is designed for multi-application WSNs. In practice, SN having different purposes, If apply conventional concealed data aggregation schemes the Cipher texts of different applications cannot be aggregated together; otherwise, the decrypted aggregated result will be incorrect. The only solution is to aggregate the cipher texts of different applications separately. The second purpose is designed for single application WSNs. CDAMA mitigates the impact of compromising SN through the construction of multiple groups. An adversary can forge data only in the compromised groups, not the whole system

V.CDAMA

BGN is implemented by using two points of different orders so that the effect of one point can be removed by multiplying the aggregated ciphertext with the order of the point, and then the scalar of the other point can be obtained. Based on the same logic of BGN, CDAMA is designed by using multiple points, each of which has different order. We can obtain one scalar of the specific point through removing the effects of remaining points (i.e., multiplying the aggregated ciphertext with the product of the orders of the remaining points). The security of CDAMA and BGN are based on the hardness assumption of subgroup decision problem, whereas CDAMA requires more precise secure analysis for parameter selections.

A. Generalization of CDAMA

CDAMA (k ¼ 2) can be generalized to CDAMA (k > 2). The paradigm of generalization uses different generators to construct different key pairs for groups. The generalized CDAMA is for security reasons, the order of E should be large enough. Therefore, when k becomes large, the length of ciphertext will also expand. For multi-application WSNs, the SNs belonging to one specific application are assigned the same group public key. Under CDAMA, the ciphertexts from different applications can be aggregated together, but they are not mixed. The ciphertexts can be integrated into a ciphertext and transmitted to the BS. The BS then individually decrypts the aggregated ciphertext to extract the aggregated value of each application.

B. Key Distribution

In the end of this section, we briefly address how to deliver the group public keys to SNs securely. There are two main approaches. Key predistribution. If we know the locations of deployed SNs, we can preload necessary keys and functions into SNs and AGs so that they can work correctly after being spread out over a geographical region. Key postdistribution. Before SNs are deployed to their geographical region, they are capable of nothing about CDAMA keys. These SNs only load the key shared with the BS prior to their deployment, such as the individual key in LEAP and the master secret key in SPINS. Once these SNs are deployed, they can run the LEACH protocol to elect the AGs and construct clusters. After that, the BS sends the corresponding CDAMA keys, encrypted by the pre shared key, to SNs and AGs.

VI.DETAILS OF THE PROPOSED FRAMEWORK

In our framework, there are multiple sensor nodes, multiple cluster heads, and single base station. The framework is illustrated in Fig. 1.

A. Node Registration

This is the first module; here the sensor nodes are registered by the cluster head. By providing the separate secret key to each sensor node that can be registered to the sensor network.

B. Key Generation

In this module the temporary key generation process will be handled. These temporary keys are used to unlock the documents at the destination. To provide high privacy to the data this temporary keying and rekeying operation will be performed. This key will be shared between source and destination users.

C. Attacker Module

Adversaries can eavesdrop on transmission data in a WSN. Adversaries can send forged data to any entities in a WSN. Adversaries can compromise secrets in SNs or AGs through capturing them.

D. Encryption process

In this module Encryption process for all the data will be done. Before sending the sensed data to the cluster head the encryption process will be taken. The cluster heads will be analyzed and initialized based on the transmission rate of each nodes. Then the encrypted data passed to the cluster heads..

E. Integrity Verification Module

In this module data integrity will be verified. Because when the data passed from sensor nodes to the cluster head any hacker may do any activity on the document to hack. During that time the data are not in the high privacy. It may go with any attacks. So, data integrity will be applied before sending to the base station. Because of the integrity verification can avoid the duplicate details in the database.

VII.CONCLUSION

For a multi-application environment, CDAMA is the first CDA scheme. Through CDAMA, the cipher texts from distinct applications can be aggregated, but not mixed. For a single-application environment, CDAMA is still more secure than other CDA schemes. When compromising attacks occur in WSNs, CDAMA mitigates the impact and reduces the damage to an acceptable condition. Besides the above applications, CDAMA is the first CDA scheme that supports secure counting. The base station would know the exact number of messages aggregated, making selective or repeated aggregation attacks infeasible. Finally, the performance evaluation shows that CDAMA is applicable on WSNs while the number of groups or applications is not large.

REFERENCES

[1] P. Paillier, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," Proc. 17th Int'l Conf. Theory and Application of Cryptographic Techniques, pp. 223-238, 1999.
[2] S. Madden, M.J. Franklin, J.M. Hellerstein, and W. Hong, "TinyPBC: Pairings for Authenticated Identity-Based Non-Interactive Key Distribution in Sensor Networks," Proc. Fifth Symp. Operating Systems Design and Implementation, 2002.
[3] H. Sanli, S. Ozdemir, and H. Cam, "SRDA: Secure Reference-based Data Aggregation Protocol for Wireless Sensor Networks," Proc. IEEE 60th Vehicular Technology Conf. (VTC '04-Fall), vol. 7, 2004.
[4] J.-Y. Chen, G. Pandurangan, and D. Xu, "Robust Computation of Aggregates in Wireless Sensor Networks: Distributed Randomized Algorithms and Analysis," IEEE Trans. Parallel Distributed Systems, vol. 17, no. 9, pp. 987-1000, Sept. 2006.
[5] H. Cam, S. O ¨ zdemir, P. Nair, D. Muthuavinashiappan, and H.O. Sanli, "Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks," Computer Comm., vol. 29, no. 4, pp. 446-455, 2006.
[6] D. Faria and D. Cheriton, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.