IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Multiple Sensor Application using Secure Data Aggregation

Shanthi.G.S[1], Chandrakala.K.R.S[2]

[1, 2]**Department of Computer Science and Engineering, Sriram Engineering College ,Perumalpattu – 602 024**

Abstract

Wireless sensor networks are become increasingly popular in many spheres of life. One major application scenario for a Wireless sensor networks is to monitor environmental data and transmit it to a Base station. A new type of scheme called, concealed data aggregation scheme extended from homomorphic encryption technique is to detect and block the risk of physical attacks. It support multi application environment .Data aggregation reduces the raw data transmission. It provides security enhancement measures (Secure counting) to Prevent hackers from extracting encrypted data or by compromising sensor nodes, aggregators to cheat the base station and collapse the entire environment (i.e. whole process). And also mitigates the impact and reduces the damages to an acceptable condition.

Index Terms—*Concealed data aggregation, elliptic curve cryptography, homomorphic encryption, 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 is restricted by the resources due to limited computational power and low battery supply; thus, energy saving technologies must be considered when we 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. Generally, aggregative operations are algebraic, such as the addition or multiplication of received data, or statistical operation.

Although data aggregation could significantly reduce transmission, it is vulnerable to some attacks. For instance, compromising a CH will allow adversaries to forge aggregated results as similar as compromising all its cluster members. To solve this problem, several studies, such as the delay aggregation, SIA, ESPDA , and SRDA, have been proposed.

An alternative approach for this problem is to aggregate encrypted messages directly from SN, thereby avoiding the forgery of aggregated result. Since CHs are not capable of encrypting messages, compromising a CH earns nothing in forging aggregated results. Based on this concept, Wu et al.gave the proposal to allow CHs to classify encrypted data without decrypting them. Following this concept, Westhoff et al. And Girao et al. proposed concealed data aggregation (CDA) supporting richer operations on aggregation. Unlike Wu et al.'s work, CDA utilizes the privacy homomorphism encryption (PH) to facilitate aggregation in encrypted data. By leveraging the additive and multiplicative homomorphism properties, CHs are able to execute algebraic operations on encrypted numeric data. Further, Mykletun et al. adopted several public-key-based

PH encryptions to construct their systems. In similar fashion, Girao et al. extended the ElGamal PH encryption to construct theirs.

In this paper, the proposed scheme, called CDAMA, provides CDA between multiple groups. Basically, CDA-MA is a modification from Boneh et al.'s PH scheme. Here, we also suppose three practical application scenarios for CDAMA, all of which can be realized by only CDAMA.

The first scenario is designed for multi-application WSNs. In practice, SN having different purposes, e.g., smoke alarms and thermometer sensors may be deployed in

The same environment. If we apply conventional concealed data aggregation schemes the ciphertexts of different applications cannot be aggregated together; otherwise, the decrypted aggregated result will be incorrect. The only solution is to aggregate the ciphertexts of different applications separately. As a result, the transmission cost grows as the number of the applications increases. By CDAMA, the ciphertexts from different applications can be encapsulated into "only" one ciphertext. Conversely, the base station can extract application-specific plaintexts via the corresponding secret keys.

The second scenario is designed for single application WSNs. Compared with conventional schemes 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 scenario 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. In CDAMA, the base station exactly knows the number of messages aggregated to avoid above attacks.

II. 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. WSN Setup Model

Fig. 1 explains the Wireless Sensor CDAMA Architecture. The WSN environments are designed by designing base station, Aggregators and multiple sensors. Initially base station is created there is only one base station, There is only one Main aggregator will be created, more than one aggregators will be created based on the environment, for each aggregator, aggregator id will be generated for secure data communication. This aggregator information will be populated in main aggregator.

Multiple sensors will be created, for each sensor will have a sensor id for secure transmission of data, and sensor got the aggregator information from Main aggregator, and then chooses an aggregator, for multiple sensors will have one Aggregator and multiple sensors. The communications between them also have to establish. Group Public and Private Key established that keys are known by Application sensors and Basestation.

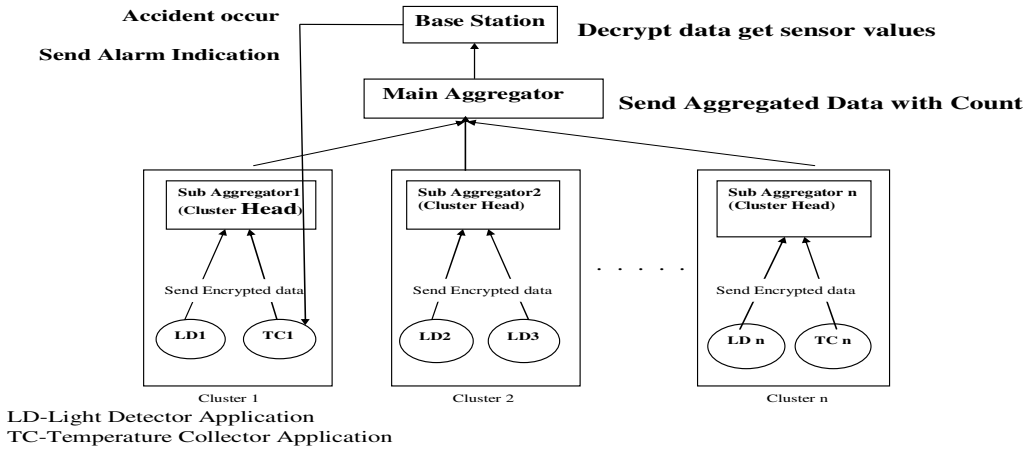

Fig 1. Wireless Sensor CDAMA Architecture

B. Aggregation Model

In WSNs, SN collect information from deployed environ-ments 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.

C. Attack 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.

A1. Ciphertext only attack. An adversary can deduce the key from only the encrypted messages.

A2. Known plaintext attack. Given some samples of plaintext and their ciphertext, an adversary can deduce the key or decrypt any ciphertext.

A3. Chosen plaintext attack. Given some samples of chosen plaintext and their ciphertext, an adversary can deduce the key or decrypt any ciphertext.

A4. Chosen ciphertext attack. Given some samples of chosen ciphertext and their plaintext, an adversary can deduce the key or decrypt any ciphertext she has not chosen before. The model is CCA1, also called lunchtime attacks [16].

B1. Unauthorized aggregation. An adversary can aggregate sniffed ciphertexts into forged but format-valid ciphertexts.

B2. Malleability. An adversary can alter the content of a ciphertext.[1]

C1. B1/B2 under compromised AG. When an adversary captures an AG and compromises its secret, she can use it to launch B2/B3 attacks with higher probability of success.

C2.Unauthorized decryption under compromised SN. When an adversary captures an SN and compromises its secret, she can decrypt not only the ciphertexts from that SN but also the ciphertexts from the other remaining SNs. Asymmetric schemes can defend against unauthorized decryption under compromised secrets because knowing the public key is useless for decryption.

III. CDAMA

A. CDAMA (k = 2) Construction

Assume that all SNs are divided into two groups, GA and GB. CDAMA contains four procedures: Key generation, encryption, aggregation, and decryption, listing in Fig. 2. As we can see, CDAMA (k = 2) is implemented by using three points P;Q, and H whose orders are q1; q2, and q3,respectively. The scalars of the first two points carry the aggregated messages in GA and GB, respectively, and the scalar of the third point carries randomness for security. As shown in the DEC functions, by multiplying the aggregated Ciphertext with q2q3 (i.e., the SK in GA), the scalar of the point P carrying the aggregated message in GA can be obtained. Similarly, by multiplying the aggregated ciphertext with q1q3 (i.e., the SK in GB), the scalar of the point Qcarrying the aggregated message in GB can be obtained. In this way, the encryptions of messages of two groups can be aggregated to a single ciphertext, but the aggregated message of each group can be obtained by decrypting the ciphertext with the corresponding SK.Considering deployment, the private keys should be kept secret and only known by the BS. SNs in the same group share the same public key and no other entities outside the group know the group public key. How to securely deliver the public keys to different groups of SNs will be discussed later in Section 4.4. Another major change is the decryption procedure. By performing individual decryption, the BS extracts individual aggregated results of different groups from an aggregated ciphertext.

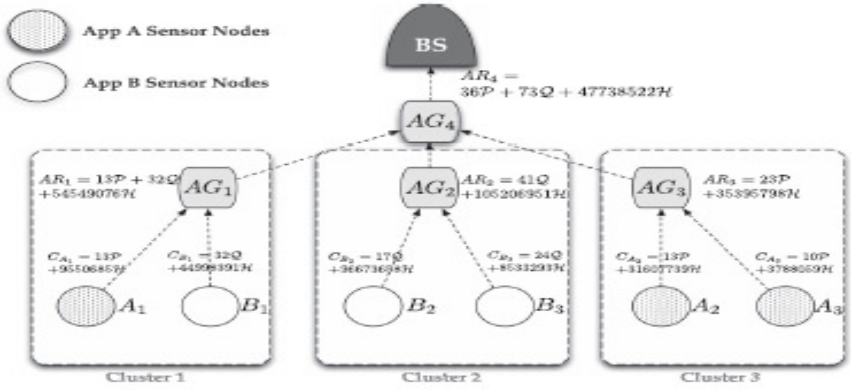

Fig. 3. A concrete example of CDAMA ($k = 2$).

B. Algorithm for generalization CDAMA.

KEYGEN (τ): Generate public-private key pairs for group Gi, vi = 1~k

1. Based on security parameter τ ,compute elements, (q1,q2,….,qk+1,E),

   Where E is the set of elliptic curve pints which form a cyclic group;

   Ord (E) = n; n is the product of q1… qk+1 and q1,…., qk+1 are large primes;

   The bit length of q is the same, i.e., |q1| = ….=|qk|= |qk+1|.
2. Randomly pick up K+1 generators, G1….Gk+1 Ɛ E where ord(Gi) = n, vi.
3. Compute point H= (Πi=1 qi) * Gk+1 such that ord(H) = qk+1.
4. Let T be the maximum plaintext boundary where Pollard's ʎ method is feasible.
5. Compute point Pi = (Πi=1, i≠i, qi) * Gi such that ord(Pi) = q1 for i=1,…,k.
6. Output Gi's group public key (PKi): PKi = (n, E, Pi, H, Ti).
7. Output the private key = Ski = (q1, q2,……,qk+1).

ENC(PKi, M): Message encryption in Gi

1. Check if message M Ɛ {0,….,Ti}.
2. Randomly select R Ɛ {0,…..,n-1}.
3. Generate the cipher text C as ; C = M * Pi + R * H where Pi Ɛ PKi.
4. Return C.

AGG(C1, C2): Message aggregation on two cipher texts C1 and C2.

1. Aggregated cipher text C' = C1 + C2 = Σ i=1 (ΣMi) * Pi + (ΣRi) * H,

Where ΣMi represents the aggregated result of group Gi and ΣRi presents the aggregated randomness of all groups.

2. Return C'.

DEC (SKi, C): Message decryption on C for group Gi using private key Ski

1. Compute M =Σ Mi = log G̃i.
2. Return M.

IV. APPLICATIONS

In this section, we propose three applications that are realized by only CDAMA multigroup construction.

A. Multi-Application WSNs

Compared with the multi-application WSNs, the scenario of a single application is more commonly discussed in WSNs. However, the scenario of multiple applications working concurrently is more realistic in most cases. Study [25] indicates that deploying multiple applications in a shared WSN can reduce the system cost and improve system flexibility. The reason is because an SN supports multiple applications and can be assigned to different applications dynamically. For example, UC Berkeley's MICA node is capable of sensing different data, e.g., temperature, light, accelerometer, and magnetometer. For instance, three different kinds of SNs, smoke detectors, temperature collectors, and light detectors, are deployed in the same building. Fig. 5 shows this

typical case. Each room contains an AG and some SNs. A big challenge for the AGs, AG1 to AG4, is to aggregate the sensed readings from the different applications to a mixed aggregated result.

.

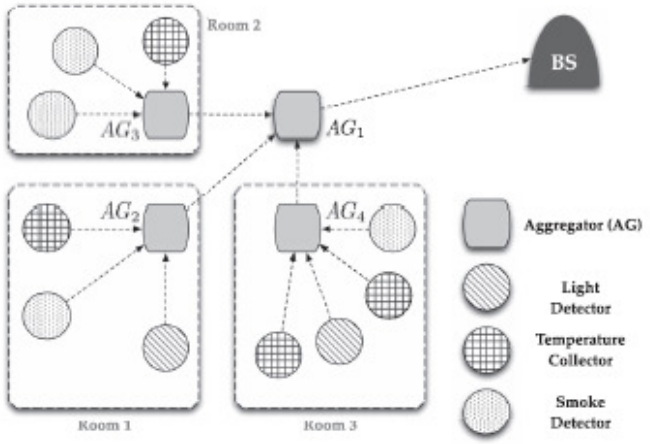

Fig. 5. A multi-application WSN example.

V. CONCLUSIONS AND FUTURE WORK

In the conclusion, for a multi-application environment, CDAMA is still more secure than other CDA schemes. When compromising attacks occur in WSNs, In the future, we wish to apply CDAMA to realize aggregation query in Database-As-a-Service (DAS) model In DAS model, a client stores her database on an untrusted service provider. Therefore, the client has to secure their database.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] R. Min and A. Chandrakasan, “Energy-Efficient Communication for Ad-Hoc Wireless Sensor Networks,” Proc. Conf. Record of the 35th Asilomar Conf. Signals, Systems and Computers, vol. 1, 2001.

[3] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure Information Aggregation in Sensor Networks,” Proc. First Int’l Conf. Embedded Networked Sensor Systems, pp. 255-265, 2003.

[4] A. Perrig, J. Stankovic, and D. Wagner, “Security in Wireless Sensor Networks,” Comm. ACM, vol. 47, no. 6, pp. 53-57, June 2004.

[5] L. Hu and D. Evans, “Secure Aggregation for Wireless Networks,” Proc. Symp. Applications and the Internet Workshops, pp. 384-391, 2003.

[6] 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.

[7] 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.

[8] Y. Wu, D. Ma, T. Li, and R.H. Deng, "Classify Encrypted Data in Wireless Sensor Networks," Proc. IEEE 60th Vehicular Technology Conf., pp. 3236-3239, 2004.