ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st& 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

A Novel Approach for Rectification of Data Aggregation for Multiple Applications in Wireless Sensor Networks

Subanivedhi N K[1], Rekha M[2]

[1]ME, Dept of CSE, Vel Tech Multi Tech Engineering College, Avadi, Chennai, India.

[2]Asst Professor, Dept of Computer Science and Engineering, Vel Tech Multi Tech Engineering College, Avadi, Chennai.

Abstract- For wireless sensor networks, large amount of transmission is decreased by a data aggregation scheme. To conceal communication during data aggregation homomorphic encryptions have been applied. Adversaries are not able to compromise the aggregators because they work on the encrypted data. But this does not satisfy multi-application environment because decrypting ciphertexts from different application will be incorrect. This scheme is insecure if sensor nodes are compromised. The base station does not have knowledge of aggregated result. An extended new concealed data aggregation scheme from the existing homomorphic public encryption scheme is proposed. This is built for multi-application environment. By CDAMA (Concealed Data Aggregation Scheme for Multiple Application), the ciphertexts from different application can be encapsulated into only one ciphertexts. The base station obtains application related data from single aggregated ciphertexts. It also reduces the settlement of single application environment attacks. It reduces the damage caused by unauthorized aggregations. It is also planned for secure counting capability. In this proposed system, ECDAMA (Enhanced Concealed Data Aggregation Scheme for Multiple Application) is designed to mitigate the impact of compromising a single aggregator by storing the replica of main aggregator in sub aggregator and to discover an alternate route to the base station is performed.

Keywords- homomorphic public encryption, data aggregation, ciphertexts, secure counting capability.

I.INTRODUCTION

A wireless sensor network composed of number of sensor networks that are deployed to gather data from the environment. The various factors such as fault tolerance, network topology, hardware constraints, power constraints have to be considered during the design of the protocol. In order to minimize the power consumption, cluster based wireless sensor network have been considered. In cluster based architecture, sensor nodes in nearby region group together to form cluster and one of the node is elected as a cluster head. The cluster head aggregate the data collected from the sensor node into one data. So that number of data packet routed to the base station is reduced.

Even though data aggregation consumes less transmission power, it is prone to number of attacks. If the cluster head is compromised at some point of time then it is possible to forge the entire aggregated result. In order to overcome this problem, number of studies such as the delay aggregation [14], SIA (Secure Information Aggregation) [15], ESPDA (Energy-Efficient Secure Pattern Based Data Aggregation) [7], and SRDA (Secure Reference-based Data Aggregation) [12], have been proposed.

The one another approach to solve the problem of compromising an cluster head is to encrypt the data at sensor node itself. The cluster head are not have capable of encrypting the data thus forgering the cluster head does not again any advantage. Girao et al. [11] proposed concealed data aggregation (CDA) utilizes the privacy homomorphism encryption (PH) to assist aggregation in encrypted data. By leveraging the additive and multiplicative homomorphism properties, cluster head are able to execute algebraic operations on encrypted numeric data. In addition, he extended the ElGamal PH encryption to construct theirs.

CDAMA (Concealed Data Aggregation scheme for Multiple Applications) is an extension of Boneh et al.'s [13] PH scheme. It is designed for an multiple application wireless sensor environment. Sensor nodes with different application can be deployed in same environment. In convention data aggregation scheme [9], [10], [11], [12], [14], the decryption of aggregated ciphertext of different application is erroneous. The key to this problem is to aggregate the ciphertext of different application independently. This has significant impact in communication cost. With CDAMA, ciphertext of several application are encapsulated into an single ciphertext. Thus base station can extract application related plaintext using corresponding secret key. CDAMA reduce the impact of compromising sensor node through the construction of multiple groups. An opponent can forge data only in the compromised groups, not the entire system. It is also having the knowledge of secure counting. That is base station

has the information about number of data aggregated. In this proposed work, A ECDAMA Scheme is extended to address the problem of main aggregator failure by incorporating the encrypted replica of main aggregator.

II.RELATED WORKS

This section overviews pervious work on concealing the data and performing aggregation on the data. Lingxuan Hu and David Evans [14] proposed delayed aggregation and delayed authentication. Delayed aggregation delays aggregation of data for an single hop instead of immediate aggregation at sensor node. Delayed authentication delays the authentication for some period of time. Therefore it is resilient to intruders device and single device key compromise.

Bartosz et al.,[15] proposed Aggregate-Commit-Prove method that allow aggregator to aggregate the data collected from node, commit and prove that it uses the data collected from the sensor nodes. Hasan Cam, Suat Ozdemir, Prashant Nair and Ozgur San ali[7] proposed sleep-active mode coordination that allows to identity overlapping sensing range of some node to switch off. Thus it avoids duplicate transmission and saves energy.

Girao et al.,[9] proposed Privacy Homomorphism technique that allows to perform algebraic or statistical operation on encrypted data. Wu et al.,[13] proposed that classifier has set of keywords and they match these keyword against the received encrypted message. Based on the resultant, it forwards the data.

Perrig et al.,d[18] designed and developed SNEP (Secure Network Encryption Protocol) protocol to provide data confidentiality, data freshness, data authentication with minimal overhead.

III.PROPOSED SYSTEM

Sensor nodes having different purposes are deployed an environment. Sensor nodes senses the value and encrypt these values using group key generated by the base station. Sensor nodes are responsible for forwarding the data to the sub aggregator. Sub aggregator aggregate the ciphertext of similar application and forwards to the main-aggregator. Main aggregator encapsulate the ciphertext of the different application into single ciphertext and routes to the base station. Base station can extract the application specific plaintext using the corresponding secret key. In this proposed system the problem of failure of the whole wireless sensor network with respect to main aggregator is eliminated by enhancing the ECDAMA scheme. The replica of main aggregator software is stored in the sub aggregator. If someone tries to compromise the main aggregator it sends error message to the sub aggregator and disconnects itself from base station. The sub aggregator now performs task of both sub aggregator and main aggregator as well as finds an alternate route to the base station.

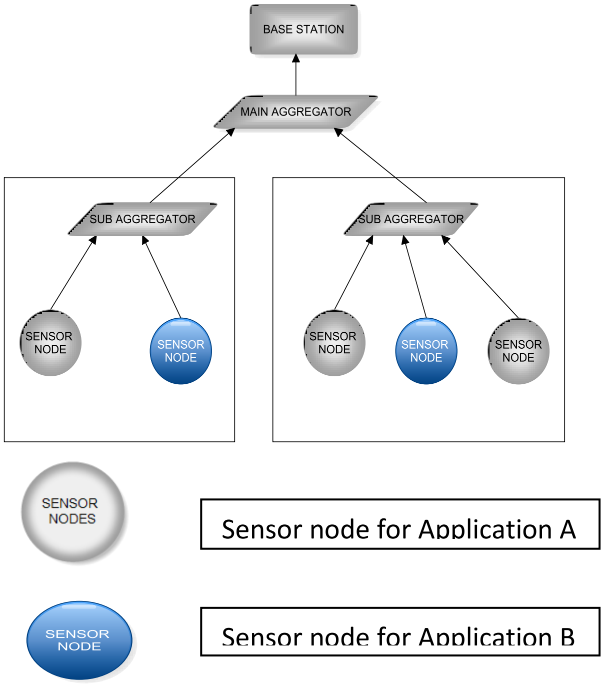

Fig 3.1 Architecture diagram

IV.METHODOLOGY

A.PRIVACY HOMOMORPHISM

Privacy homomorphism is an encryption scheme that has a homomorphic property. Privacy homomorphisms allows to map set of operations on cleartext to the set of operations on the ciphertext. $D_k(E_k(m_1)*E_k(m_2))=m_1+m_2$, where $E_k()$ is the encryption with the key k, $D_k()$ is the decryption with the key k, * and + denote the operations on the plaintext and ciphertexts. The Privacy homomorphic scheme can be classified as symmetric crytosystem where similar key is used for encryption and decryption. This scheme is considered to be more secure when an ciphertext space is larger then an cleartext space.

B.CONCEALED DATA AGGREGATION

Conventional aggregation scheme allows any intermediate node to be forged thus they are considered to be insecure. PH scheme allows to perform aggregation operation on the ciphertext without decryption and they are more secure. The compromising any intermediate node gains no advantage. Girao et al [11] extended privacy homomorphic scheme to construct an aggregation in which all share a same key thus compromising any intermediate node will be able to forge. To solve this problem, each node share unique key in beginning of the transmission. By this forging a single node have no effect on it.

C.ECDAMA

ECDAMA comprises of key generation, aggregation, and decryption processes. For ease we consider two user groups ie (k=2). Consider three points P, Q, H and theirs orders are q_1, q_2 and q_3. The scalar of the two points carry aggregated message in a GA and GB and last point is used to carry random number for security. The aggregated ciphertext is multiplied by their order to get the aggregated message. The ciphertext from different applications are aggregated however they are not mixed. The message of each group can be obtained by simply decrypting the ciphertext with their private keys.

Pseudo code for key generation:

```
Step 1: Based on the security parameter $\tau$, compute the values of $(q_1,q_2,q_3,E)$. E denote set of the elliptic curve points that forms a cyclic group. $ord(E) = n$ and $n=q_1q_2q_3$, such that $q_1$, $q_2$, $q_3$ are large prime numbers and length of $q_1$, $q_2$, $q_3$ are of same.
Step 2: Select three generators $G_1$, $G_2$, $G_3$ in such a way that $ord(G_1) = ord(G_2) = ord(G_3) = n$.
Step 3: Calculate point $H = q_1q_2*G_3$ and $ord(H) = q_3$.
Step 4: Select parameter T as the maximum plaintext boundary wherever Pollard's method is feasible. Compute the values of $T_A$ and $T_B$ based on the number of sensors in an application.
Step 5: Calculate $P = q_2q_3 * G_1$, $ord(P) = q_3$. The output $G_A$'s group public key $PK_A$ and $PK_A$ as (n, E, P, H, $T_A$).
Step 6: Similarly calculate $Q = q_1q_3 * G_2$, $ord(Q) = q_2$. The output $G_B$'s group public key $PK_B$ and $PK_B$ as (n, E, P, H, $T_B$).
Step 7: Output $G_A$'s group private key $SK_A$ as $(q_2q_3)$ and $G_B$'s group private key $SK_B$ as (q1q3).
```

Pseudocode for message encryption in G_A:

```
Step 1: Check if message belongs to $\{0,...,T_A\}$.
Step 2: Select R in such a way that $\{0,...,n-1\}$.
Step 3: Produce the ciphertext C using the formula $M*P+R*H$.
Step 4: Generate C.
```

Pseudocode for message encryption in G_B:

```
Step 1: Check if message belongs to $\{0,...,T_B\}$.
Step 2: Select R in such a way that $\{0,...,n-1\}$.
Step 3: Produce the ciphertext C using the formula $M*Q+R*H$.
Step 4: Generate C.
```

Pseudocode for message aggregation on two ciphertext C_1 and C_2:

```
Step 1: Calculate the value of aggregated ciphertext $C'$ as $C_1+C_2$; $C'$ as $(\sum M_i)*P+(\sum M_j)*Q+ (\sum R_i)*H$.
    $\sum M_i$ denotes the aggregated result of $G_A$.
    $\sum M_j$ denotes the aggregated result of $G_B$.
    $\sum R_i$ denotes the aggregated randomness of both the groups.
Step 2: Generate $C'$.
```

Pseudocode for message decryption in G_A:

```
Step 1: Calculate M as $\sum M_i = \log_{P'}(q_2q_3*C)$. While $P'$
        is $q_2q_3*P$.
Step 2: Generate M.
```

Pseudocode for message decryption in G_A:

```
Step 1: Calculate M as $\sum M_j = \log_{Q'}(q_1q_3*C)$. While $Q'$
        is $q_2q_3*Q$.
Step 2: Generate M.
```

The function of main aggregator is to encapsulate the ciphertext of different application into an single ciphertext. The replica of main aggregator is stored in sub aggregator. When an main aggregator is overwritten by an opponent, it sends error message to sub aggregator and disconnect itself from base station. Now the elected sub aggregator performs the task of both main aggregator and sub aggregator. The sub aggregator also finds an alternate path to route the packet.

D.CONCRETE EXAMPLE

Consider a wireless sensor network consising of six sensor nodes, three aggregators and forming two clusters. The public key for sensors belonging to application A is denoted using subset of n, E, P, H, T_A. Similarly, The public key for sensors belonging to application B is denoted using subset of n, E, P, H, T_B. E indicates set of elliptic curve points that form a cyclic group. Points P, Q and H are orders of q_1, q_2, q_3. In order to reduce the complexity, the values of P, Q, H are conveyed to small values. n is the product of q_1, q_2, q_3. Messages from these sensor nodes are encrypted to ciphertexts. After aggregator aggregates the ciphertext, base station receives the final result. Now base station decrypt the aggregated message using corresponding group private key.

E. KEY DISTRIBUTION

The base station is responsible for generating the group public keys and distributing it to the sensor nodes. The key distribution is done based on two methodology. The first method is key predistribution in which sensor node locations are known in prior. Therefore we insert keys and functions into sensor nodes and aggregators.

The second method is Key postdistribution. Here sensor nodes have their keys distributed in their prior location. The key can be of secret key or master key. After sensor nodes are deployed, cluster based protocol is used to elect the aggregator and construct the cluster environment. Now sensor node uses the shared key to encrypt the plaintext.

V. APPLICATION

A.WIRELESS SENSOR NETWORK WITH MULTIPLE APPLICATION

The deployment of sensor nodes with multiple application has significant reduction in organisation cost. It is more flexible. Consider a scenario of monitoring the physical environment of an IT industry where different rooms require different temperature eg : mainframe physical environment require temperature of about 18 to 24 degrees centigrade. Each room has some sensor nodes and aggregator. The main challenge is data privacy and to minimize the communication overhead because, sensor nodes encrypt the sensed values and ciphertexts are aggregated. Aggregating the ciphertext from different application is difficult because, decryption cannot extract exact sensed value. This overhead is reduced by this scheme.

B. SECURE COUNTING

The main drawback in conventional concealed data aggregation scheme is that aggregator can manipulate aggregated result. There is a chance for aggregator to increase or decrease the aggregated value by continuously adding or subtracting value by a fixed number. Base station does not have the knowledge of number of data aggregated. Hence it cannot detect error. This is overcome by providing secure counting. Base station knows number of sensed values aggregated.

VI. RESULTS AND DISCUSSION

The total cost of ECDAMA is very large. Although data aggregation scheme reduce number of data transmitted to base station, sensor nodes takes high cost for encryption and aggregation.

In this wireless sensor network, nodes are classified are leaf nodes, aggregator and base station.
Leaf nodes are deployed to gather information from the environment. Aggregators are similar to cluster head they aggregate the data sent from leaf nodes and sent to the base station. Base station decrypt the ciphertext using the corresponding key. Under ECDAMA scheme, leaf nodes consumes thousand times the energy greater than the conventional aggregation scheme. The aggregator at the level next to sensor node consumes energy ten times larger. The aggregator at next level consumes the energy equal to that of the traditional scheme. As the transmission moves closer to the base station, the energy consumption is reduced.

Scheme	Field size	Aggregation of computation	Communication cost per bit
CDAMA (K=2)	768	22	384
CDAMA (K=3)	1024	39	342
CDAMA (K=4)	1280	62	320
ECDAMA (K=2,3,4)	1015	40	355

Table 6.1 Aggregation Cost of Data Concealment Scheme

The result of field size, aggregation cost, communication cost of CDAMA AND ECDAMA Scheme with varying number of application is shown in the fig 6.1.

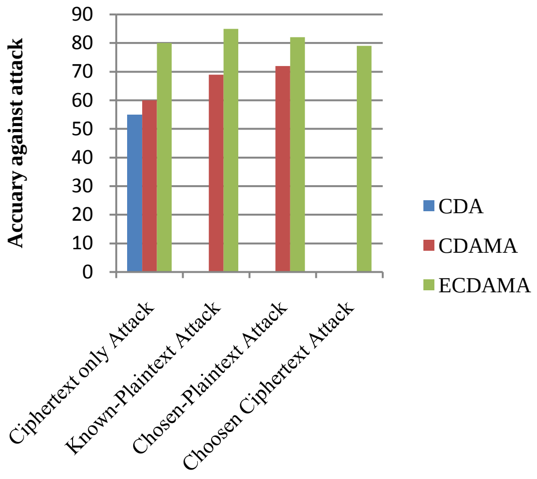

Fig 6.2 Achievement of Security

The ECDAMA scheme shows better accuracy against four types of attacks namely ciphertext only attack, known-ciphertext attack, chosen-plaintext attack, chosen-ciphertext attack. The CDA scheme resist only against ciphertext only attack and CDAMA scheme survive against three attacks namely ciphertext only attack, known-ciphertext attack, chosen-plaintext attack. This is shown in the Fig 6.2.

VII. CONCLUSION

ECDAMA is the concealed data aggregation scheme proposed for an multi-application environment. The ECDAMA under single application environment is found to be more secure then traditional scheme. For multi-application environment, data from different appliction can be aggregated but they are not mixed. The system also reduce the impact of compromising an aggregator. The result also shows that ECDAMA is more applicable to wireless sensor network while number of groups are not large. In future, we hope to apply this scheme to aggregate query in Database-As-a-Service (DAS) model[19].

REFERENCES

[1] Yue-Hsun Lin, Shih-Ying Chang, and Hung- Min Sun, "CDAMA: Concealed Data Aggregation Scheme for Multiple Applications in Wireless Sensor Networks" IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No.7, July 2013.

[2] Kuthadi Venu Madhav, Rajendra.C, and Raja Lakshmi Selvaraj, "A Study of Security Challenges in Wireless Sensor Networks" Journal of Theoretical and Applied Information Technology, 2005 - 2010.

[3] Javier Lopez, Rodrigo Roman, and Cristina Alcaraz, "Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks, " Springer, pp. 289–338, 2009.

[4] L. Oliveira, D. Aranha, E. Morais, F. Daguano, J. Lopez, and R. Dahab, "TinyTate: Computing the Tate Pairing in Resource-Constrained Sensor Nodes," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA '07), pp. 318-323, 2007.

[5] J. Girao, D. Westhoff, E. Mykletun, and T. Araki, "Tinypeds: Tiny Persistent Encrypted Data Storage in Asynchronous Wireless Sensor Networks," Ad Hoc Networks, vol. 5, no. 7, pp. 1073-1089, 2007.

[6] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," ACM Trans. Sensor Networks, vol. 2, no. 4, pp. 500-528, 2006.

[7] 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.

[8] E. Mykletun, J. Girao, and D. Westhoff, "Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Comm. (ICC '06), vol. 5, 2006.

[9] D. Westhoff, J. Girao, and M. Acharya, "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation," IEEE Trans. Mobile Computing, vol. 5, no. 10, pp. 1417-1431, Oct. 2006.

[10] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous '05), pp. 109-117, 2005.

[11] J. Girao, D. Westhoff, M. Schneider, N. Ltd, and G. Heidelberg, "CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Comm. (ICC '05), vol. 5, 2005

[12] 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.

[13] 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.

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

[15] 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.

[16] D. Boneh and H. Shacham, "Fast Variants of RSA," CryptoBytes (RSA Laboratories), vol. 5, pp. 1-9, 2002.

[17] 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.

[18] Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.

[19] B.Iyer, C.Li, and S.Mehrotra, "Executing Sql over Encrypted Data in the Database-Service-Provider Model," Proc. ACM SIGMOD Int'l Conf. Management of Data, pp.216-227,2002.

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