IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. VII (Feb. 2014), PP 60-64
www.iosrjournals.org

Enhancing Data Security in WSN using Symmetric Key Algorithm

[1]U. Sathya Rekha, [2]Mrs P. Hemalatha
PG Student, Dept of CSE, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India.
Assistant Professor, Dept of CSE, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India.

Abstract: *Data aggregation is implemented in wireless sensor networks to reduce data redundancy and to summarize relevant and necessary information without requiring all pieces of the data and to reduce large amount of data transmission. Homomorphic public encryption is the proposed scheme designed for multi-application environment. The base station extracts application-specific data from aggregated cipher texts, and compromised attacks in single application environments, and to degrade damage from unauthorized aggregations. To enhancing a new approach as symmetric key algorithm used where the keys for encryption and decryption are done in same shared secret. These keys are used to provide security in data aggregation and separate the cipher text when it stored and retrieve from database. In Database As a Service (DAS) model, the client has to secure their database. The attacker cannot change the data because it is dynamically created.*

Keywords: *Aggregation, Homomorphic public Encryption, Symmetric Key, Database Asa Service, Attacker, Cipher text*

I. Introduction

Wireless Sensor Networks (WSNs), consist of thousands of sensor nodes (SN) that gather data from deployed environments and it is used in plenty of rich applications, 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. The aggregators collect data from a subset of the network and aggregate the data and aggregate function. Aggregation reduces the amount of network traffic which helps to reduce energy consumption on sensor nodes in WSN, the aggregators in a secure data aggregation scenario need to decrypt the encrypted data to perform aggregation. Girao et al [4] proposes an additive and multiplicative homomorphic encryption that allows aggregation of encrypted data and it is secure and efficient.Concealed data aggregation(CDA) schemes that are based on the homomorphic characteristics of a privacy homomorphism(PH) enable end-to-end encryption in wireless sensor networks. CDA requires that a key be distributed to a subgroup of nodes that form a reverse-multicast routable region in the WSN. This key enables the nodes to perform end-to-end encryption where the corruption of one node, or a subset of nodes. The CDA approach significantly reduces the energy consumption at aggregator nodes since no encryption and decryption is performed.

Concealed Data Aggregation in Multiple Applications (CDAMA) is the scheme that provides Concealed Data Aggregation (CDA) between multiple groups. CDAMA having two limitations when it aggregate multiple applications that shared in WSN can reduce the system cost and improve system flexibility such as

- CDA requirements provide solutions to maintain data privacy and reduce the communication overheads; corresponding cipher text must be aggregated.
- Aggregation of multi-application is still hard even if aggregation of cipher texts is possible, because the decryption cannot extract application-specific aggregated result from a mixed cipher text.

A. Characteristics of CDAMA are as follows:

- Designed for multiple applications in WSN. In this characteristic, cipher text of different applications can't aggregate together.
- In CDAMA, cipher text of different applications aggregate into a single cipher text.
- Designed for single application WSNs and it mitigates the impact of compromising SN through the construction of multiple groups.
- Designed for secure counting. The base station does not know how many messages are aggregated from the decrypted aggregated result.

CDAMA having several issues including efficient implementation, cipher text length and curve selection. First operations in CDAMA are based on scalar multiplication on elliptic curve points, skills which accelerate scalar multiplications that can enhance the performance of CDAMA. Secondly the length of cipher texts isalso defined because of deciding the lowest bound of cipher text length for sufficient security.

B. CDAMA Requirements:

CDAMA requires bandwidth, security, Data integrity, authentication [4][8].

a) *Bandwidth:* The bandwidth overhead attributed to sending ciphertexts should not require the transmission of large amounts of additional data.
b) *Provable Security:* The security level of the encryption scheme should be measurable and it should be based upon the commonly agreed hardness of a mathematical problem to be provably computationally secure.
c) *Data Integrity:*Data integrity ensures the receiver that the received data is not altered in transit by an adversary. Integrity can be implemented to ensure that information is not altered in any unexpected way.
d) *Authentication:* It is necessary that the interface defined between the user, the system and the admin has to provide authentication. In a sensor network, an adversary can inject the messages and the authentication techniques can verify the identity of data using symmetric key. The privacy homomorphic encryption functions only one-way authentication of sensor data at the base station only.
e) *Authorization:*Data authorization specifies access rights to resources and is strongly related to access control. Access control should prevent unauthorized users from participating in network resources.

C. Types of Attacks:

CDAMA faces several types of attacks[8], they are as follows;

a) Ciphertext Analysis:The most basic attack is the analysis of encrypted packet; the adversary wants to obtain information only by interpreting cipher texts. In WSNs with a scarce domain of values, the attack can very efficiently result in a deduction of the plaintexts.

b) KnownPlaintextAttack: The adversary tries to determine secret information with the additional knowledge of plaintexts.With known plaintext and corresponding cipher text, it is the aim of theadversary either to reveal the secret key or at least to gather additional information that can be exploited to deduct malicious cipher texts or decrypt other messages.

c) Malleability: Malleability is simply variation of the attack that would generate the cipher text that is correct.

*d) ForgePackets:*An adversary doesn't need to modify existing data, if she is able to create correctly encoded cipher text with a specific content. The attacker could substitute the packets of sensed value that the forge done. A PH scheme that is resistant to maliciously forged packets must not allow any third party to create properly encoded messages at least not without being able to detect the interference during decryption.

II. Related Work

In WSN,sensor data must be encrypted with a single key to perform concealed data aggregation sensor nodes in the network must share a common key and use it for encryption. Using a single symmetric key in the network is not secure as an adversary can fake the aggregated results through compromising only a sensor node.

Symmetric key based privacy homomorphism is shown to be insecure for chosen plaintext attacks for some specific parameter settingsas dropping or forging messages and transmitting false data. Witness nodes of data aggregators alsoaggregate data and compute MACs to help verify the correctness of the aggregators' data at base station because the data validation is performed at base station, the transmission of false data and MACs up to base station affect adversely the utilization of sensor network resources.

Due to their high computational overhead, asymmetric key homomorphic encryption algorithms are not feasible for sensor nodes. The privacy homomorphic encryption algorithm introduced by Domingo[3] Ferrer is symmetric key based. The concealed data aggregation algorithm that is proposed which employs Domingo[3] Ferrer's privacy homomorphic encryption algorithm.

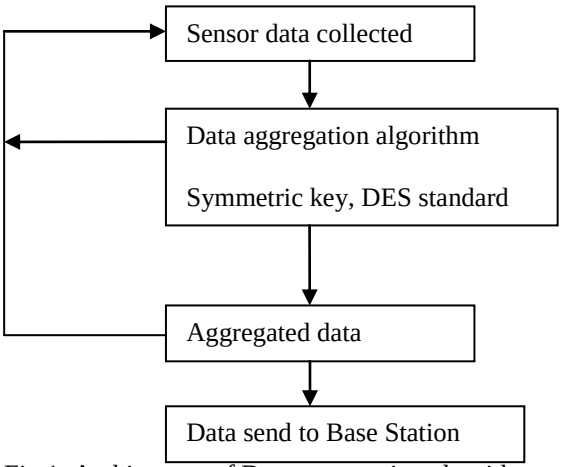

Fig 1. Architecture of Data aggregation algorithm

However in order to aggregate the data of the all network, the proposed scheme must uses a secret key known by all sensor nodes which leads to provide effective security to data. If a sensor node is compromised, it can decrypt data of any sensor node which is encrypted by the secret key.

Dolev Yao threat model [6], the attacker can capture a sensor node and acquire all information stored within it. Should the attacker capture a subset of sensor nodes, the probability that captured nodes are from the same region is higher than if the captured nodes are equally distributed over the WSN.

Okamota and Uchiyama [9] proposed a public-key cryptosystem with homomorphic properties, which is proven to be as secure.

Castellucciaetal. [3] Presented an efficient aggregation of encrypted data in wireless sensor networks which is also based on additively homomorphic features of the encryption scheme based on an extension of the onetime pad technique. This approach uses different keys per sensor at the cost of mandatory transmitting the sensor ID list of the involved monitoring nodes.

Chan et al [7] present the first secure hierarchical data aggregation scheme based on aggregation commit verify, which forces the adversary to commit to its choice of aggregation results and then allow the sensors to verify whether their aggregation contribution is correct or not.

Goldwasser and Micali [7] is to provide data security, goal is to prevent an attacker from gaining information about sensor data.

III. Proposed Work

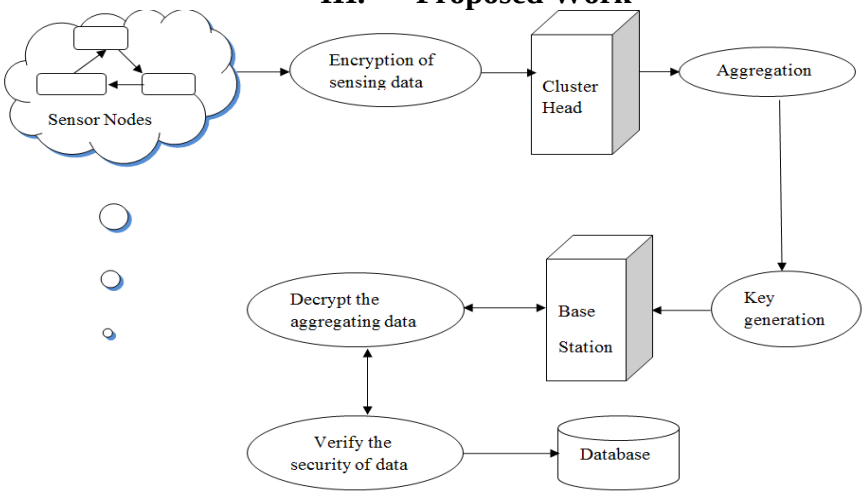

Fig 2. System Architecture

In WSN's, sensor nodes sends the encrypted data that is capable of performing some processing the data to cluster head, CH organizes data pieces received from SN into an aggregated result, and then forwards the result to the base station based on regular routing path. Aggregators would forward the results to the next hop after the aggregation done. In order to perform aggregation, aggregators are used to increase the lifetime, tree-based or cluster networks force the intermediate nodes. Whenever the user needs information for the group or individual it will send to the BS. The base station received the request and split the cipher text. Performing the reverse aggregation the cipher text can decrypt to sends the data for users. The CH sends the result to aggregation, after aggregation done the results must be sends to base station. Base station now can extract the data (cipher text) with decryption and verifies the decrypted data is secured and finally the data must be stored in database repository.An important aspect of encryption scheme for aggregation in WSNs is that the sink node needs to be aware of the encryptors id's such that it can regenerate the correct key stream for decryption purposes. Because WSNs are not always reliable, it cannot be expected that all nodes reply to all requests. There need a mechanism for communicating the id's of the non-responding nodes to the base station.

IV. Implementation

The process is divided into several major tasks such as sensor node and group aggregation, attacker, key generation, data security.

Sensor Node and Group Aggregation

Multi group data can collect which is used to create and separate the node and aggregate it. The aggregate node can analyse the cipher text, and can verify the message in group data from multi group data and

produce the result that must be stored in base station.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 tree-based or cluster networks force the intermediate nodes (a sub tree 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. The source information for data aggregators may originate from public data. Aggregator nodes summarize the datasets in order to provide a higher level view of available data. After aggregation the cipher text is encoded after it has been passed through an encryption. The cipher text is the product or combination of plain text and its encryption.

Attacker

Base station sends data which is aggregate to form a cipher text, when encrypting a group keys and a cipher key to produce a cipher text. Attacker can collect the cipher text, then find whether the data has attacker, attacker is inside the text then analyse the text send back to user if the attacker is not present in cipher text then decrypt the data and send to user. Adversary wants to send the forged messages to cheat the BS even though she does not know the secret key. Attacker is a special type of player, usually one whose role involves aggressive data. A group key is a cryptographic key that is shared between groups of users. Group key are distance by sending them to individual users physically or encrypt individually for each user using either that user's pre distributed private key.

Secure aggregation is required when an attacker may capture secret data as sensor networks are vulnerable. Symmetric key cryptography algorithms are possible to achieving the secured data.

Key Generation

Cluster Head can aggregate the data sent by a sensor after aggregation the Cluster Head can generate a key added to the aggregated data, after aggregation finally the data are sent to base station. Key generation is the process of generating keys for cryptosystem. A key is used to encrypt or decrypt whatever data is being encrypted or decrypted. Key Generator objects are reusable, i.e., after a key has been generated, the same Key Generator object can be re-used to generate further keys. There are two ways to generate a key: in an algorithm-independent manner, and in an algorithm-specific manner. The only difference between the two is the initialization of the object.

Data Security

Initially the base station can verifies the key from the aggregated data sent by the Cluster Head, after verifying the keys the base station can decrypt the aggregated data. Data security is used to protecting a database from destructive forces or unwanted actions of unauthorized users.

Input: User data, Aggregation
Output: Secured data
Begin
Step1: Sensor nodes send different kinds of data.
Step2: Cluster head organizes data pieces received from SN into an aggregated result
Step 3:Forwards the result to the base station based on regular routing paths.
Step 4: Cluster head receives the data, appends its own ID#, and then sends them to the higher- level cluster head or the base station.
Step 5: If there is no need for a new session key then check if there is any incoming data from the cluster heads.
Step 6: Process the decrypted data and obtain the message sent by the sensor nodes**.**
Step 7: Decides whether to request to all sensor nodes for retransmission of data.
End

TABLE I. NOTATIONS

Notations	**Descriptions**
CDA	Concealed Data Aggregation
SN	Sensor Node
WSN	Wireless Sensor Networks
CH	Cluster Head
PH	Privacy Homomorphism
AG	Aggregators
BS	Base Station

Fig 3. Notation Table

The above table shows the notations used in this paper.

V. Conclusion and Future Work

CDAMA is the first multi-application environment; the cipher texts from distinct applications can be aggregated, but not mixed, and in single-application environment, CDAMA is still moresecure than other CDA and finally mitigates the impacts and reduces damage from a compromising attacks occur in WSNs. Thus CDAMA provide secure counting, and the base station would know the exact number of messages aggregated.

In future, CDAMA can be applied to realize aggregation query in Database-As-a-Service (DAS) model. By using symmetric key aggregating multiple applications can provide more security to all the data aggregated. In DAS model, a client stores her database on an untrusted service provider and the client has to secure their database through PH schemes because PH schemes keep utilizable properties than standard ciphers.

Symmetric Key can be implemented in base station when an attacker trying to change the data. In Base station, symmetric keys are used to conceal the encrypted data whatever sends to server, DES cryptosystem act as a buffer when sending and receiving the data from users. Thus the DES cryptosystem in symmetric key are used to aggregate multiple audios, videos in future.

References

[1] A. Liu and P. Ning, (2008) "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," Proc. Int'l Conf. Information Processing in Sensor Networks (IPSN'08), pp.245-256.

[2] C. Castelluccia, E. Mykletun, and G. Tsudik, (2005) "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.

[3] D. Westhoff, J. Girao, and M. Acharya, (2006) "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.

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

[5] H. Sanli, S. Ozdemir, and H. Cam, (2004) "SRDA: Secure Reference-based Data Aggregation Protocol for Wireless Sensor Networks," Proc. IEEE 60th Vehicular Technology Conf. (VTC'04-Fall), vol.7.

[6] L. Oliveira, D. Aranha, E. Morais, F. Daguano, J. Lopez, and R. Dahab, (2007) "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.

[7] R. Min and A. Chandrakasan, (2001) "Energy-Efficient Communication for Ad-Hoc Wireless Sensor Networks," Proc. Conf. Record of the 35thAsilomar Conf. Signals, Systems and Computers, vol.1.

[8] S. Peter, D. Westhoff, and C. Castelluccia, (2010) "A Survey on the Encryption of Convergecast-Traffic with In-Network Processing," IEEE Trans. Dependable and Secure Computing, vol.7, no.1, pp.20-34.

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

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