ENHANCING END-TO-END CONFIDENTIALITY IN WIRELESS SENSOR NETWORKS

[1]S.P.Kavya, [2]M.Kalimuthu, [3]M.Nandhini

[1,2,3] Assistant Professor, Department of Information Technology
SNS College of Technology, Coimbatore, Tamil Nadu, India
[1]kavyaspcbe@gmail.com,
[2]mkmuthu73@gmail.com
[3]nandhinim24@gmail.com

Abstract :A wireless sensor network (WSN) is a collection of a large number of sensor nodes and few sink nodes that have limited computation, communication and power resources. Data aggregation is used to reduce the amount of data transmission and increases the lifetime of sensors. Data aggregation is the process of combining the raw data from one or more sensor nodes and performs operations as min, max, count, sum, avg etc[1]. The sensor nodes are often deployed in hostile environment so the aggregated result should be protected from the various types of attacks in order to achieve the data integrity, data confidentiality and authentication. The various approaches given for the secure data aggregation is classified into two groups: secure data aggregation on unencrypted data and secure data aggregation on encrypted data. The project is to propose a secure data aggregation on encrypted data by using additive homomorphic encryption scheme and digital signature.

Keywords - *Data aggregation, Encryption, Decryption, Integrity, confidentiality, authentication, security*.

1. INTRODUCTION

A WSN is a network of devices and nodes, which can sense the environment and communicate the information gathered from the monitored field (e.g., an area or volume) through wireless links. The data is forwarded through multiple hops to a sink (sometimes denoted as controller or monitor) that can use it locally or is connected to other networks (e.g., the Internet) through a gateway. The nodes can be stationary or moving. A wireless sensor network (WSN) consists of number of distributed autonomous sensors to monitor the environmental conditions, such as temperature, sound, motion or pollutants and to cooperatively send their data through the network to a base server. The more modern networks are bi-directional in nature. The wireless sensor networks are existing in many applications like military, industrial and consumer applications, area monitoring and control, health monitoring for machines, and so on [5].

As sensor networks become wide-spread in different environments, security issues become a central concern, especially in mission-critical tasks. To protect information from the various types of attacks in order to achieve the data integrity-confidentiality and authentication, secure data aggregation is introduced.

1.1 Importance of Security in WSN

The sensor nodes can be easily attacked due to resource constrained nature and the broadcast nature of query. The sensor nodes are exposed to physical attacks because it is deployed in an open environment and managed remotely. Due to these reasons sensor data and the physical node need to be secured. The aggregation

data in sensor network needs more security because if it is disturbed the entire aggregated data that is captured in a particular period of time will be lost and it cannot be reclaimed in emergency situation[5]. The security properties like confidentiality, integrity, and availability and data freshness should be satisfied to the aggregate data.

1.2 Secure Data Aggregation

In order to save resources and energy, data must be aggregated to avoid overwhelming amounts of traffic in the network. Aggregation is the process of performing some operation on the data sensed by sensor nodes and reports the aggregated data to a central node, called sink.When data is transmitted with aggregation it enhances the lifetime of sensor and reduces the energy consumption by eliminating the redundancy. The sensor nodes are often deployed in hostile environment so the aggregated result should be protected from the various types of attacks in order to achieve the security issues[6]. The various approaches given for the secure data aggregation is classified into two groups i) Secure data aggregation on unencrypted data means the aggregator node decrypts, performs aggregation, encrypts and forward to the base station. So it leads to key compromise problems in aggregator node. ii) Secure data aggregation on encrypted means the aggregator node performs aggregation on encrypted data and forward to the base station. So it is more secured than former one.

2 . Related Works

In Secure data aggregation scheme(SDAP) [3] for clustered wireless sensor networks, the encrypted sensor readings are transmitted to the cluster head with MAC and the cluster head process the encrypted data without decryption. For the readings have the same value and come from different sensor nodes, the cluster head remains the node's identifiers in data aggregation process to provide the information for global data distribution. Except providing data privacy protection, the scheme had better performances in resilient against active attack, node compromise attack and DoS attack.

In RCDA data aggregation scheme [9] provide better security compared with traditional aggregation schemes. In traditional scheme like homomorphic encryption scheme the cluster heads (aggregator) can directly aggregate the cipher texts without decryption and consequently transmission overhead is reduced. The base station only retrieves the aggregated result, not individual data, which causes two problems. First, the usage of aggregation functions is less. For example, the base station cannot access the maximum value of all sensing data if the aggregated result is the summation of sensing data. Second, the base station cannot check the data integrity and authenticity via attaching message digests or signatures to each sensing sample. The two drawbacks was overcome in RCDA by using aggregate signature for strong authentication, and all sensing data was recovered by placing the cipher text in proper bit positions, and data is also encrypted by using concealed data aggregation.

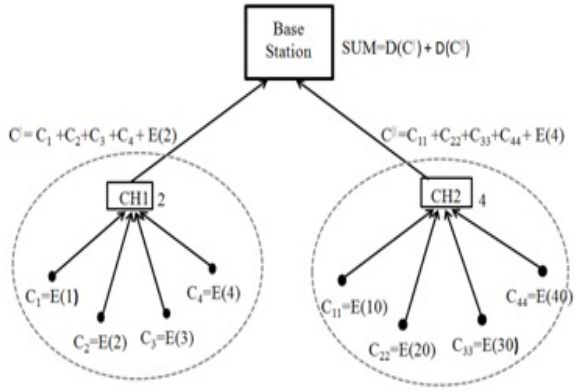


Fig .1. Data Aggregation on Encrypted data

In efficient data aggregation [8] each sensor devices' data transmissions is a energy-consuming tasks, so to increase the lifetime of a WSN it is essential to minimize the number of bits sent by each devices. One well known approach is to aggregate sensor data (e.g., by adding) along the path from sensors to the sink. Aggregation becomes especially challenging if end-to-end privacy between sensors and the sink is required. An simple and provably secure additively homomorphic stream cipher that allows efficient aggregation of encrypted data. The new cipher only uses modular additions (with very small moduli) and is therefore very well suited for CPU-constrained devices. Aggregation based on this cipher text can be used to efficiently compute statistical values such as mean, variance and standard deviation of sensed data, while achieving significant bandwidth gain.

In Fully Homomorphic encryption the modified Encryption can meet multiplicative homomorphism and additive homomorphism and advance security. The brief description of fully homomorphism advanced by Rivest, Adleman and Dertouzos is as follows[2]:

Supposing that S is a set and *S'* is another set with the same cardinality of that of S.

D : S→*S'* is a bijection.

D will be used as decryption function.

S is a Set.

S' is another set with same cardinality.

Plaintext operation

$U= <S;f_1,….,f_k;p_{1,}.....,p_2;s_1,……s_m>$

$f_i : S^{g}{}_i \rightarrow S$ is the function with g_i being the parameter here, and p_i is the predication with h_i being parameter, and s_i is distinguish constant. Inverse operation to U can be descriped as follows[6] :

$C= <S';f_1',….,f_k';p_1',.....,p_2';s_1',……s_m'>$.

In Exact-in network for aggregation with integrity and confidentiality (SIES) scheme ,additive homomorphic encryption was used to encrypt the data and RSA digital signature was also used to check the authenticity and to identify node compromise attack .In addition with this secured share is also used to check the integrity of the data. Both the aggregator and the base station will check the signature and secure share to accept the data ,if it is not valid then the data will be rejected.

i) Setup Phase in SIES

The packet size is considered as 32 bytes long .Base station generates random keys K (known to sink and every source) and k1,k2…. kn (known to sources alone), which is 20 bytes long ,and prime modulous p is 32 bytes long ,lastly data generated by source node mi is considered as 4 bytes long .The keys as (K,k_i,p) is registered at each sources.

Notations:

$K \neq 0$ and $k_i<P$.

m_i->Message,$m_i<P$.

c_i->cipher text

t->time epoch.

$SS_{i,t}$->Secret Share.

ii) Key Generation:

Let key pair be (K,k_i) , k_i-Private key randomly selected from Z_p. K - public Key and K be 4 bytes long and rest be padding bits. Then compute hash on each key using SHA_{256} as follows:

$K_t=HM_{256}(K,t)$

$k_{i,t}= HM_{256}(k_i,t)$

$SS_{i,t}= HM_1(k_i,t)$

In the above, (K,k_i) are 32 bits long and $SS_{i,t}$ be 20 bytes long.

iii) Encryption and Aggregation:

The encryption is defined as

$C_i= \epsilon(m_i,K,k_i,p)=(K\cdot m_i+k_i) \bmod p$.

If the two ciphertexts c1 and c2 corresponding to plaintexts m1 and m2, respectively. Then the Sum value of $m_1 + m_2$ is computed as

$C_1+C_2 = \epsilon(m_1,K,k_1,p)+ \epsilon(m_2,K,k_2,p)$,

$=[K\cdot(m_1+m_2) + (k_1 + k_2)] \bmod p$,

$= \epsilon(m_1+m_2 , K, k_1 + k_2 , p)$.

The ciphertext generated in sensor node is named as partial state record (PSR) .The PSR will have Value (vi,t) and $SS_{i,t}$ and remainng padding bits, along with this the RSA digital signature is also generated and send to the aggregator .The aggregator individually checks the signature and adds the ciphertext as ($C_1+C_2 +C_3$…….C_n)and sends to BS with its own signature as in Fig 1 .

iv) Verification at Base Station:

In base station, the ciphertext and signature are received as

$C' = C_1+C_2 +C_3$…….C_{agg} and RSA signature

$\square' = \square_{agg}$.

The signatures are verified individually at every hops. The base station checks the signature of aggregator and $SS_{i,t}$ as,

$SS_{i,t}= SS_{1,t} +SS_{2,t} +SS_{3,t} +SS_{4,t}$+---------- $+SS_{agg,t}$.

3. Proposed System:

In this system instead of time epoch in SIES scheme the random number is chosen as session key so the guessing of data is not easily possible[1].

Consider the base station broadcasts the query by using RSA digital signature. Assume the packet size is 32 bytes long . The keys are registered as (K,k_1,k_2,p) at each sources.

Notations:

K -> Key known to base station and every sources S , $K \neq 0$.

k_1,k_2-> Session keys

P-> Prime factor.

m_i->Message,m_i<P.

c_i->cipher text

t->time epoch.

$SS_{i,t}$->Secret Share.

N-> random number

3.1 Key Generation:

Let key pair be (K,k_i) , k_i-Private key randomly selected from Z_p. K - public Key and K be 4 bytes long and rest be padding bits. Then compute hash on each key using SHA_{256} as follows:

$K_t=HM_{512}(K,N)$

$k_{i,t}= HM_{512}(k_1,N/2)$

In the above, (K,k_i) are 32 bits long and $SS_{i,t}$ be 20 bytes long.

3.1.2 Encryption and Aggregation

We define encryption as $C_i= \epsilon(m_i,K,k_i,p)=(K+m_i+k_i) \mod p$. Now consider two ciphertexts c_1 and c_2 corresponding to plaintexts m_1 and m_2, respectively. Observe that we can compute the encryption of SUM $m_1 + m_2$ as[1]

$C_1+C_2 = \epsilon(m_1,K,k_1,p)+ \epsilon(m_2,K,k_2,p)$,

$=[K+(m_1+m_2) + (k_{1,t}+ k_{2,t})] \% p$,

$= \epsilon(m_1+m_2 , K, k_{1,t} + k_{2,t} , p)$.

Generate the RSA digital signature as ($\square$), and send these to aggregator as individually. The aggregator checks the RSA digital signature and sends the pair as

{($C_1+C_2 +C_3$…….C_n),($\square_{agg}$)} is to BS.

3.1.3 Verification at Base Station

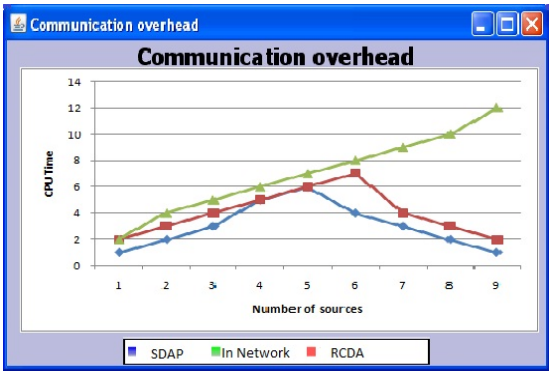
In base station , the ciphertext and signature area received as follows:

$C' = C_1+C_2 +C_3$…….C_{agg} and

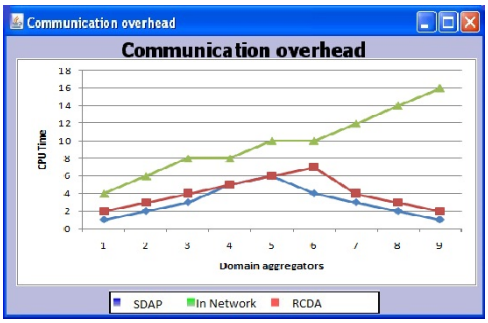
$\square' = \square_{agg}$.

Because the signatures are verified individually at every hops.So finally the aggregators signature is received. And also check $SS_{i,t}$ as,

$SS_{i,t}= SS_{1,t} +SS_{2,t} +SS_{3,t} +SS_{4,t}$+---------- $+SS_{agg,t}$.



(a) Datasets



(b) Aggregation function

Fig. 2. Performance of MAX queries versus S.

5. Conclusion

In this paper the new additive homomorphic encryption is proposed to data aggregation. A special feature is that the base station can securely receive the aggregated data and the transmission overhead is reduced. We integrate the signature scheme with to ensure data authenticity and integrity in the design. Even though signatures bring additional costs, the proposed schemes are still affordable for WSNs after evaluation. Considering a large WSN (over 100 nodes), we also performed simulations on the proposed schemes shown in Fig 2.

6. References

1. Stavros Papadopoulos, Aggelos Kiayias, and Dimitris Papadias "Exact In Network Aggregation with Integrity and Confidentiality" IEEE Transactions On Knowledge And Data Engineering, Vol. 24, No. 10, October 2012.
2. Guangli Xiang,Benzhi Yu, Ping Zhu" A Algorithm of Fully Homomorphic Encryption" 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012).
3. Suat Ozdenir" Concealed Data Aggregation in Heterogeneous Sensor Networks using Privacy Homomorphism" IEEE Conference on Computer Society 2007.
4. JiangHong Guo, JianFeng Ma, XiuQiang Wu" Secure Data Aggregation Scheme for Clustered Wireless Sensor Networks" Seventh International Conference on Computational Intelligence and Security 2011.
5. Kiran Maraiya,Kamal Kant,Nitin Gupta "Wireless Sensor Network :A Review on Data Aggregation" International Journal of Scientific & Engineering Research volume 2,Issue 4,April-2011.
6. Mukesh Kumar Jha,T.P. Sharma "Secure Data aggregation in Wireless Sensor Network: A Survey" International Journal of Engineering Science and Technology (IJEST) ISSN : 0975-5462 ,Vol. 3 No. 3 March 2011.
7. Julia Albath, Sanjay Madria "Secure Hierarchical Data Aggregation in Wireless Sensor Networks" IEEE Communications Society subject matter experts for publication in the WCNC 2009 proceedings.
8. Claude Castelluccia, Einar Mykletun, Gene Tsudik "Efficient Aggregation of encrypted data in Wireless Sensor Networks" Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05) 2005.
9. Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin, and Hung-Min Sun" RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks" IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 4, April 2012.