ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 9(3), DOI: 10.17485/ijst/2016/v9i3/75971, January, 2016 ISSN (Online) : 0974-5645

Efficient Sensing of Data when Aggregated with Integrity and Authenticity

G. S. Raj, M. Thanjaivadivel, M. Viswanathan* and N. Bindhu

Vel Tech University, Chennai - 600062, Tamil Nadu, India; gsraj1982@gmail.com, thanjaivadivel@gmail.com, viswamtech19@gmail.com, bindhu2424@gmail.com

Abstract

Background/Objectives: The main objective of this paper is to gather and aggregate data in an efficient manner so that network lifetime is enhanced. Enhanced mechanisms for end-to-end encryption from the sensors to the sink, also termed converge cast traffic, address the concern of reducing both the energy consumption at the sensor nodes and the effect of physical attacks on the nodes. Concealed Data Aggregation provides a good balance between energy-efficiency and security while still allowing data to be processed at the nodes. **Methods/Statistical analysis:** In this paper, we first outline and discuss the formation of cluster nodes. In these each sensor node is controlled by the Cluster Head (CH) which in turn is controlled by a Base Station (BS). Then, an integrity and authenticity has been enhanced using Mykletun encryption scheme. **Findings:** To recover, the above issues a novel methodology has been proposed, which provides maximize data integrity and authenticity using Concealed Data Aggregation (CDA). This leads to reduce the transmission overhead and improves the overall lifetime of WSN. **Applications/Improvements:** We propose a novel approach using homomorphic encryption, Mykletun KeyGen and Boneh Signature Scheme to achieve confidentiality, integrity and availability for secure data aggregation in wireless sensor networks.

Keywords: Base Station (BS), Cluster Head (CH), Concealed Data Aggregation (CDA), Privacy Homomorphism (PH), Sensor Nodes (SNs) ,Wireless Sensor Networks (WSN)

1. Introduction

Wierless Sensor Network (WSN) has several constrains like battery power, memory, communication, bandwidh, computation speed etc. Therefore, reducing the power consumption is a challenging issue in WSN for more than a decade. To imporove the power life, a solution called data aggregation has been implemented here[1].

Normally, the process of grouping the node in a sensor networks is known as clusters. The data aggregation is a process of combining and compressing the data belonging in to a single cluster with the help of Cluster Heads (CHs)[2].

Each CHs senses maximum node in a network and send the results to the base station, which leads to reduce the communication cost, Since, only the aggregated results reach the base station. The main aim of data aggregation is to gathered, searched, processed and presented in summarized form and to utilize the energy in an efficient manner[2].

Many issues in the process of clustering in WSN includes about:

- How many clusters should be formed?
- How many nodes should be taken in to a single cluster? and
- How to select the CHs?

To find the solutions for the above problem, First, the data are encrypted before transmission. Followed by CHs aggregate encrypted data w/o encryption.To save the overall energy, sensed data are consolidated and aggregated on its way to the final destinaton[3].

The Concealed Data Aggregation (CDA) provides in-networking processing and end-to-end encryption.The CDA schemes are based on Privacy Homomorphism (PH) encryption. PH make use of additive homomorphism to support additive operation on encrypted data[4]. On the other hand Multiplicative Homomorphism (MH) allows multiple operations on the ciphertext. Multiplicative homomorphism uses RSA Cryptosytem

* Author for correspondence

scheme. To achieve the aggregate scheme either addive or multiplicative hohmorphism can be used but both are not at the same time[5].

However PH schemes used for only to collect the aggregated result. The problem faced in PH Schemes is constrained in usage of aggregated result and the BS doesn't verify authenticity and integrity of each sensing data. "Homomorphic" is an adjective which describes a property of an encryption scheme[6]. In simple terms, is the ability to perform computations on the ciphertext without decrypting it first. The popular but wildly insecure cipher scheme is partially homomorphic, specifically with respect to the concatenation operation[7].

Later, Mykletun sign. proposed a scheme not only for ciphertext but also signature. By verfying the aggregated signature can ensure the data integrity of each plaintext[8].

2. Implementation and Modules Description

2.1 Formation of Nodes and Clusters

In this module, we implement a formation of nodes and cluster in Wireless Sensor Networks (WSNs). In the Figure 1 we design wireless environment and the sensor nodes are deployed in this environment. Based upon our assumption we have to form a Sensor Nodes (SNs) and wireless environment. In wireless environment location based all SNs are connected in a cluster like form. A CHs sense maximum node in a network and send the results to the base station. The CH is controlled by each cluster[9-10]. All sensor nodes connected via Intermediate Node. Finally, the Cluster Head (CH) is controlled by a Base Station (BS).

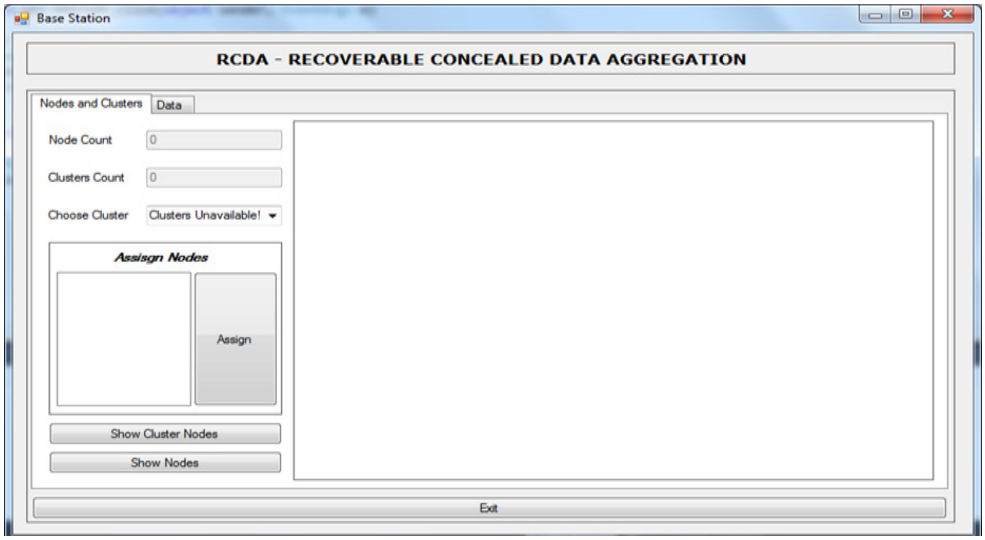

Figure 1. Wireless sensor environment.

2.2 Communicating to Cluster Nodes

In this Figure 2, we have implement the communication way of cluster nodes and data centers. All SNs in a wireless environment may be splitted into many clusters. The CH is controlled by each cluster[11]. All sensor nodes connected via Intermediate Node. Finally, the result of Cluster Head (CH) is maintained by a Base Station (BS). Then BS can retrieves all aggregated data.

2.3 Mykletun Encryption Scheme

In this module, we are going to implement the Mykletun encryption process to generate sending cluster and receiving cluster. All Sensor nodes sense the responsible data are encrypted before transmission in CH. Mykletun et.al proposed the following procedures: KeyGen , Enc, Agg and Decrypt.

2.4 Boneh Signature Scheme

In this module, we implement Boneh aggregate signature scheme, it merges set of distinct signature in to one aggregated aggregated signature based on bilinear map.

The Boneh Signature Scheme consists of following procedures : KeyGen, Sign, Verify, Agg, and Agg-Verify.

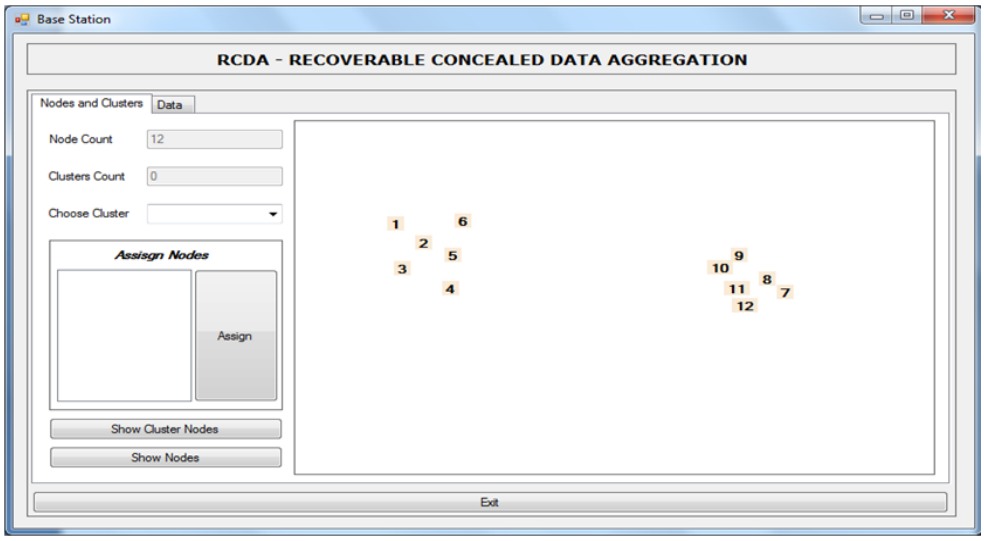

Figure 2. Nodes creation and communicating to cluster nodes.

2.5 Integrating RCDA-HOMO

RCDA-HOMO scheme can be implemented by the following procedures: Setup, Encrypt-Sign, Aggregate, and Verify.

2.5.1 Setup Processing

It generates key pair for all base station(BS). For each sensor node (SN_i), the BS generates Public key and Private Key (PU_i , PR_i) by using Boneh et.al KeyGen scheme, Where $PU_i = V_i$, Public key of $V_i = X_i * g$ and $PR_i = X_i$, Where X_i is the private key has been randomly selected from finite field (Z_p). The public key generated using Mykletun scheme Key Generation (KeyGen) Where PU = { Y, E, p, G, n}; PR= t; Y=t*G; E is an elliptic curve over a Finite field(Z_p) ; G is an generator on E; n is the order of E; t is an private key randomly from Z_p;

Atlast the Base Station keeps all Public key, Private Key and Hash function are loaded to sensor node (SN_i} for all i.

2.5.2 Encrypt-Sign

While sensor node sends the sensed data to CH, it first encode the data and aggregate to specific form. The main purpose of encrypting the data, then SN_i encrypts by PU_i and signs by PR_i. Then the final result send to CH[11-12]. The steps involved in encoding:

- Signature: $\sigma_i = Xi*Hi$, where Xi is belongs to PRi , hi is hash function of origin data
- Cipher text: Ci = (PRi,σi) = (Ki*G, Mi + K i*Y)
- At the send , SN_i sends σ_i, C_i to CH

2.5.3 Aggregate

CH collects all n-1 pairs (c_1, $\boldsymbol{\sigma}_1$) to (c_{n-1}, $\boldsymbol{\sigma}_{n-1}$) and it also aggregates signatures and ciphertexts as follow :

- For computes n-1 pairs of aggregated ciphertexts: $C= {}^{n-1}\sum_{i=1} c_i$
- For computes n-1 pairs of aggregated Signatures: $\boldsymbol{\sigma} = {}^{n-1}\sum_{i=1} \sigma_i$
- Atlast both (**C**, **σ**) aggregated result send to BS.

2.5.4 Verify

After receiving the aggregated result from CH, the base satation decrypts the C to obtain the plaintext. Then to ensure the integrity the BS verifies the aggregated signature.

3. Results and Discussion

3.1 Node Creation and Key Generation (KeyGen)

In Figure 3 proposed a CDA scheme based on the ElGamal elliptic curve cryptosystem. When the nodes are

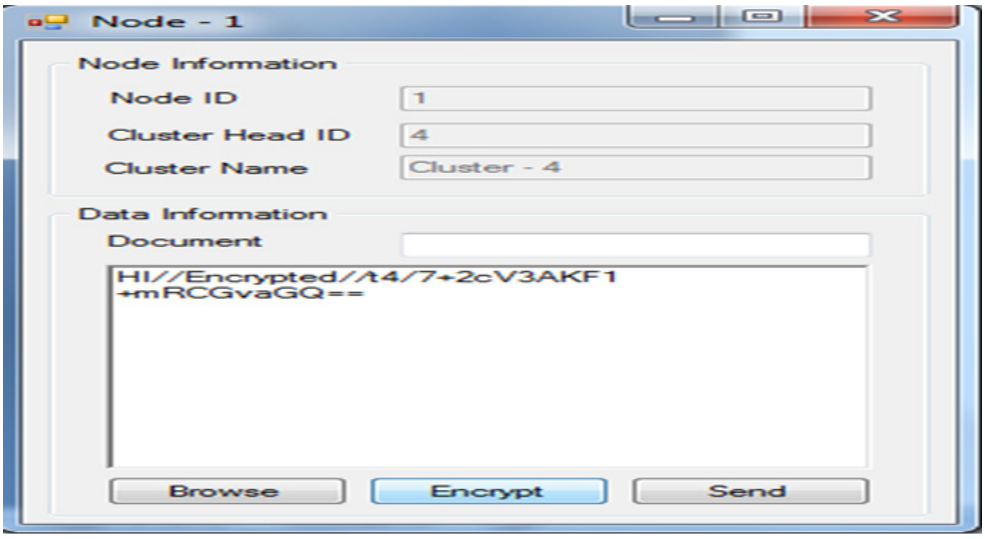

Figure 3. Encrypted Data.

deployed over the target area, the secret keys are used to create the network.

3.2 Encrypt-Sign

In Figure 4 sensor node sends the sensed data to CH, it first encode the data and aggregate to specific form. The main purpose of encrypting the data, then SN_i encrypts by PU_i and signs by PR_i. Then the final result send to CH

3.3 Aggregation (Agg)

The CH collects all n-1 pairs $(c_1, \boldsymbol{\sigma}_1)$ to $(c_{n-1}, \boldsymbol{\sigma}_{n-1})$ and it also aggregates signatures and ciphertexts as follow sec 2.5.3

3.4 Decryption (Dec)

Decryption is the reverse process to Encryption discussed in Section 3.2.

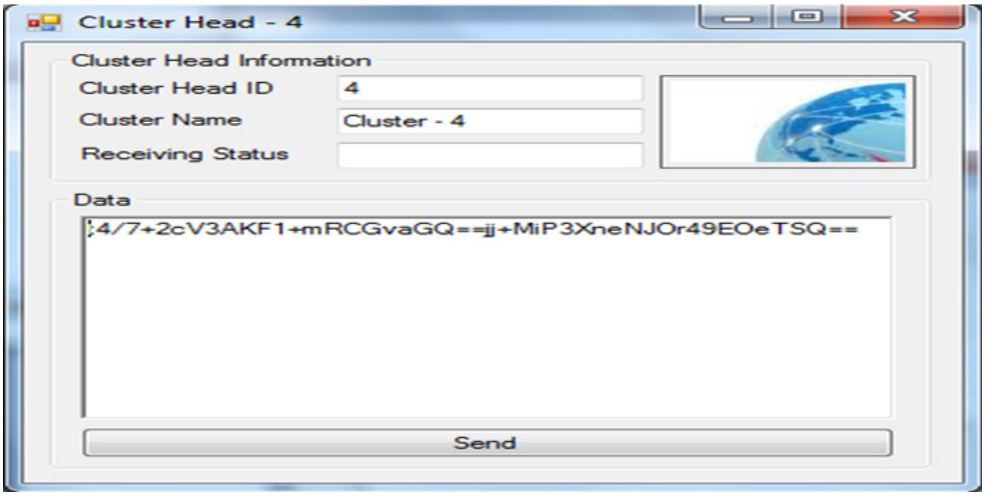

Figure 4. Aggregated Data in cluster head.

4. Conclusion and Future Work

In these paper, We have proposed concealed data aggregation scheme with digital signitature to ensure integrity and confidentiality of data and also we reduced the communication overhead. The problem faced in PH Schemes is constrained in usage of aggregated result and the BS doesn't verify authenticity and integrity of each sensing data and the base station can securely recover all sensing data rather than aggregated results. However, we used the aggregate signature scheme to authenticate and ensure the Intergrity of aggregated data in the implementation. In Future, we will use of hierachical data aggregation approaches for heterogenous sensor network should be undertaken for existing problem. Then we plan to implement these scheme in real environment.

5. References

1. Sun B, Jin X, Kui Wu K , Xiao Y. Integration of secure in-network aggregation and system monitoring for WSN. Proceedings of IEEE Communications Magazine, ICC '07; Glasgow. 2007. p. 1466–71.
2. Ozdemir, S, and Cam, H. Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks. IEEE Transaction on Networking. 2003; 18(3):1900–2.
3. Bista R, Yoo H-K, Chang J-W. A new sensitive data aggregation scheme for protecting integrity in wireless sensor networks. Proceedings of IEEE International conference on Computer and Infomation Technology, CIT; Bradford. 2010. p. 2463–70.
4. Jose J, Manoj Kumar S, Jose J. Energy efficient recoverable concealed data aggregation in wireless sensor networks. International Proceedings of Emerging Trends in Computing, Communication and Nanotechnology, ICE-CCN'13; Tirunelveli. 2013. p. 322–9.
5. Mlaih E, Aly SA. Secure hop-by-hop aggregation of end-to-end concealed data in wireless sensor networks. Proc of IEEE IFOCOM Workshop; Phoenix. 2008. p. 1–6.
6. Mykletun E, Girao J, Westhoff D. Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks. Proc of IEEE International Conference on Communications (ICC'06); Istanbul. 2006. p. 2288–95.
7. Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. Springer - Advances in Crytology- Eurocrypt. Berlin Heidelberg: Springer; 2003. p. 416–32.
8. Kumar V, Madria SK. Secure Hierarchical Data Aggregation in Wireless Sensor Networks: Performance Evaluation and Analysis. 13th International Conference on Mobile Data Management (MDM); Bengaluru, Karnataka. 2012. p. 196–201.
9. Feng H, Li G, Wang G. Efficient Secure In-Network Data Aggregation in Wireless Sensor Networks. 2nd International. Conference. on Netwoerks Security Wireless Communications and Trusted Computing, NSWCTC'10; Wuhan, Hubei. 2010; 1:194–7.
10. Kaur A, Sran SS. Detection of packet-dropping attack in recoverable concealed data aggregation protocol for homogeneous wireless sensor networks. Fifth International Conference on Advanced Computing & Communication Technologies (ACCT); Haryana. 2015. p. 666–70.
11. Bala Krishna M, Vashishta N. Energy efficient data aggregation techniques in wireless sensor networks. 5th International Conference on Computational Intelligence and Communications Network, CICN'13; Mathura. 2013. p. 160–5.
12. Sasi SB, Sivanandam N, Emeritus. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015 Feb; 8(3):216–21.