International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 01 | Apr-2015 www.irjet.net p-ISSN: 2395-0072

Structureless Efficient Data Aggregation and Data Integrity in Sensor Network

Mrs. Kavita Sunchu[1], Prof. Dhainje Prakash[2]

[1]M.E. Student, Computer Science and Engineering, Shriram Institute of technology, Maharashtra, India
[2]Professor, Computer Science and Engineering, Shriram Institute of technology, Maharashtra, India

---

Abstract - ***Recently, several data aggregation schemes based on privacy homomorphism encryption have been proposed and investigated on wireless sensor networks. These data aggregation techniques provide higher security compared with traditional aggregation since cluster heads (aggregator) can directly aggregate the cipher texts without decryption; consequently, transmission overhead. Data aggregation protocol can reduce the communication cost, so the life time of sensor network is extended. The structure based has the overhead in dynamic scenarios for any event based application. The goal of our work is to design techniques and protocol that is structure free and ensure data integrity and aggregation with low transmission overhead and transmission cost. Experiment results demonstrate that the transmission overhead is still reduced even if on sensing data. Further, the design has been generalized and adopted in wireless sensor networks.***

Keywords *-Privacy Homomorphism encryption, Sensor Networks, Data Integrity, Data Aggregation, Structure less.*

1. INTRODUCTION

In sensor networks, the communication cost is often higher than the computation cost. For calculating the communication cost, in-network data aggregation is considered an effective technique [3]. The inherent redundancy in preprocessing data collected from the sensors can often be removed by in-network data aggregation. In addition, such operations are also useful for extracting application specific information from preprocessing data. To conserve energy for a longer network lifetime, it is different for the network to support high incidence in network data aggregation [1]. Sensor networks have emerged as a popular research area with the advances in the sensor technology and reductions in the cost of sensor hardware. Usually sensor networks contain a huge amount of nodes and provide the global view of the phenomena observed from monitored area by combining the local measurements of separate nodes. A wireless sensor network is a combine network in which both nodes perform their sensing task and if required, acts as relay for converting the data of other nodes. The main traffic flow in a wireless sensor network is from the sensor nodes to the base station [2]. Optionally, an interest can be flooded from the user to the sensor nodes in the region of interest. Nodes can also communicate locally with each other for sensing tasks, cluster formation and scheduling active/sleep times of nodes. These networks provide long-lived and autonomous systems for environmental monitoring in military operations and life sciences, tracking vehicles or animals, airport surveillance, telemedicine and smart home applications. The transmission limit of the sensor radio is short and data rate is low due to the limited energy supply of the nodes based on battery technology [3]. Radio saves considerable energy as compared to other functional units in sensor network architecture; therefore it is crucial to prevent redundant transmissions and collisions. Data storage is another limiting factor which should be kept in mind during protocol design for wireless sensor networks. While hardware technology save energy such as sleep/idle modes for the radio and memory modules with separate power controls for each module, if the algorithms and protocols developed for sensor networks do not consider these features, the energy savings achieved will not reach the full extent. The amount of data generated by sensor nodes can be huge due to the large number of nodes in the network [8]. Consider the fact that, relay nodes in the network have the same capacity with the sensor nodes, relaying overhead on these nodes should be mitigated as much as possible. Redundant packets which carry information about the same event with other packets can be eliminated on their way to the base station. The data aggregation paradigm is essential for the lifetime of the network due to the reduced number of broadcast and collisions. Security in data communication is another important issue to be considered while designing wireless sensor networks, as wireless sensor networks may be deployed in hostile areas such as battlefields. Therefore, data aggregation protocols should work with the data communication security protocols, as any collision

© 2015, IRJET.NET- All Rights Reserved

between these protocols might create problems in network security. In the above PH-based schemes, the base station receives only the aggregated results [8]. However, it brings two problems. First, the usage of aggregation functions is constrained. For example, these techniques only permits cluster heads to perform additional operations on cipher texts sent by sensors; therefore, they are ineffective if the base station desires to query the maximum value of all sensing data. Second, the base station cannot verify the integrity and authenticity of each sensing data [8]. These problems seem to be solved if the base station can receive all sensing data rather than aggregated results, but this method is in direct contradiction to the concept of data aggregation—that the base station obtains only aggregated results. Thus, we attempt to design an approach that allows the base station to receive all sensing data but still reduce burden on transmission.

2. RELATED WORK

In this paper Chien-Ming Chen, Yue-Hsun Lin et al [8], introduced a concept named Recoverable Concealed Data Aggregation. In recoverable concealed Data Aggregation, a base station can recover each sensing data generated by all sensors even if these data have been aggregated by cluster heads. With these individual data, two functionalities are provided. First, the base station can verify the integrity and authenticity of all Sensing data. Second, the base station can perform any aggregation functions on them. Then, they propose two recoverable concealed data aggregation schemes named recoverable Concealed Data Aggregation Homogenous and Recoverable Concealed Data Aggregation Heterogeneous WSN respectively, but at the cost of transmission cost i.e. transmitting the sensed data and aggregated data to the base station. The figure 1 shown below gives the idea about the aggregated data and the sensed data to the base station.

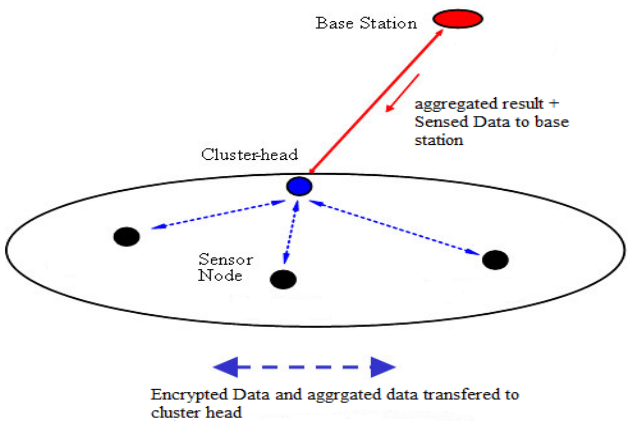

Fig-1: Cluster of sensor nodes and base station broadcasting data.

H. OzgurSanli, SuatOzdemir et al [1], focuses on the work for confidential data exchange in WSNs that supports data aggregation. To knowledge this is the first work proposing a solution for end-to-end encryption under such circumstances. The proposed solution considers positive adversaries. In practice, there are several other security goals that should be accomplished by combining other mechanisms, e.g. authentication of communicating sensors, protects from data integrity, and plausibility of sensed data. The proposals regarding other protection goals in WSNs especially focus on integrity and plausibility of sensed data [1].

2.1. Encrypted Data Aggregation

Our design for data aggregation eliminates redundant sensor readings without using encryption and maintains data secrecy and privacy during transmission [6]. The concealed data aggregation for wireless sensor network with privacy homomorphism is illustrated in figure 2.

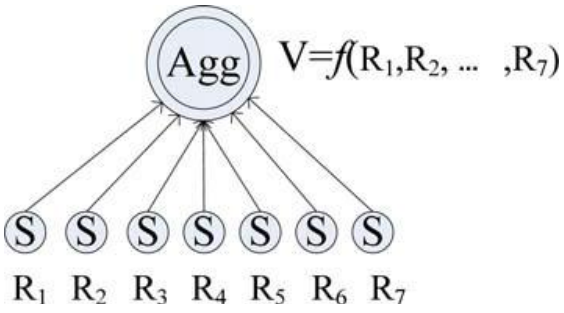

Fig -2: Concealed data aggregation for wireless sensor network with privacy homomorphism.

3. EXISTING SYSTEM.

The existing system is compromised of homogenous environment and heterogeneous environment, the construction of above system is given below

3.1 .Construction of Homogenous System

Homogeneous system is composed of four steps: Setup, Encrypt-Sign, Aggregate, and Verify[8]. The Setup procedure is to prepare and install necessary secrets for the Base Station and each sensor. When a sensor decides to send sensing data to its Cluster Head, it performs Encrypt-Sign and sends the result to the Cluster Head. Once the Cluster Head receives all results from its members, it activates aggregate to aggregate what it received, and then sends the final results (aggregated cipher text and signature) to the Base station. The last procedure is verified. The Base Station first extracts individual sensing data by decrypting the aggregated cipher text. After that, the Base Station verifies the

© 2015, IRJET.NET- All Rights Reserved

authenticity and integrity of the decrypted data based on the corresponding aggregated signature.

3.2 Construction of Heterogeneous System

Here, consider another environment, heterogeneous Wireless sensor network. A concealed data aggregation scheme for heterogeneous Wireless sensor network has been proposed however, their techniques do not provide data integrity and recovery.

3.3 Heterogeneous Scheme

Here, the author tries to fully exploit H-Sensors which have stronger computing capability [8]. Operations on L-Sensors could be switched to H-Sensors.

Computation cost on L-Sensors is switched to H-Sensors, so Encrypt, Aggregate, and Verify [8]. In the Setup procedure, necessary secrets are loaded to each H-Sensor and L-Sensor. Intracluster Encrypt procedure involves when L-Sensors desire to send their sensing data to the corresponding H-Sensor. In the Intercluster Encrypt procedure, each H-Sensor aggregates the received data and then encrypts and signs the aggregated result. In addition, if an H-Sensor receives cipher texts and signatures from other H-Sensors on its routing path, it activates the Aggregate procedure. Finally, the Verify procedure ensures the authenticity and integrity of each aggregated result.

3.4 Disadvantages

1. Transmission cost is more since only aggregated results and the sensed data reach the base station. It would cause the compromise of the whole cluster.
2. These schemes restrict the data type of aggregation or cause extra transmission overhead.
3. An adversary can still obtain the sensing data of its cluster members after capturing a cluster head.

Symbol	Description
BS	Base Station
CH	Cluster Head
Homo	Homomorphism
Hete	Heterogeneous
L-Sensor	Low End Sensor
H-Sensor	High End Sensor
SN	Sensor Node

Table 2: Notation Used in Homogenous System and heterogeneous System

4. PROPOSED SYSTEM.

In addition, H-Sensors can be designed to be tamper-resistant, so we may allow H-Sensors to store the partial secret information if required. With these considerations,

We introduce a concept named Structureless efficient data aggregation and data integrity in sensor network. In this, a base station can recover each sensing data generated by all sensors even if these data have been aggregated by cluster procedures: Setup, Intracluster Encrypt, and Intercluster heads with transmission overhead and cost is reduced. With these individual data, two functionalities are provided. First, the base station can verify the integrity and authenticity of all sensing data. Second, the base station can perform any aggregation functions on them. Then, we propose Structure free technique that verifies the results of data aggregation and integrity in WSN respectively. In the security and scalability analysis, we demonstrate that the proposed schemes are secure under any attack model. Through experiments, we show that the performance of our design is reasonable and affordable [9].

4.1 Advantages

1. Random sampling technique that enables aggregation queries to not only detects malicious sensors, but also to tolerate them.
2. Mykletun et al. a data aggregation scheme based on addition homomorphism public-key encryption. It seems more secure since every sensor stores only public key.
3. Castelluccia et al. a new PH-based aggregation scheme to overcome this security problem by generating a temporal key for each transmission.

5. SECURITY AND SCALABILITY ANALYSIS

5.1 Unsafe aggregation

In these proposals, intermediate nodes decrypt messages before aggregating them. Since intermediate nodes see the data they are aggregating, they can compute any mathematical function on them[11]. However, when an intermediate node is compromised, the confidentiality of messages traversing that node becomes compromised too. Therefore, this kind of schemes only offers protection against external attackers eavesdropping transmitted messages.

5.2 Many-to-one security without scalability

Consider the following trivial, non-scalable protocol:
(1) Each leaf *Ui*encrypts its data under a symmetric key *SKi*shared with the base station (root). Then, *Ui*sends the result to its parent (intermediate node).
(2) Internal nodes aggregate the received values by combination.
(3) The base station receives a combination of encrypted values from the leaves. Then, it decrypts them and computes the desired value. This trivial solution provides privacy and authentication, and it can easily offer integrity if some redundancy is added. Besides, after decryption, the

© 2015, IRJET.NET- All Rights Reserved

base station can compute any mathematical function on the received data. The main shortcoming of this solution is that it is a lossless approach instead of a lossy approach. This situation implies that the base station receives a final message with $O(n)$ length, n being the number of leaves of the tree. This cost does not scale well for large values of n. The figure 2 shown below illustrates the security versus scalability trade-off between sensor sending the data and aggregated results to the base station, in which the sensed data encrypted the results is shown in above analysis and when encryption is done then our approach is more secure and scalable and hence the both the transmission cost and transmission overhead is reduced. Nevertheless it could be structure less.

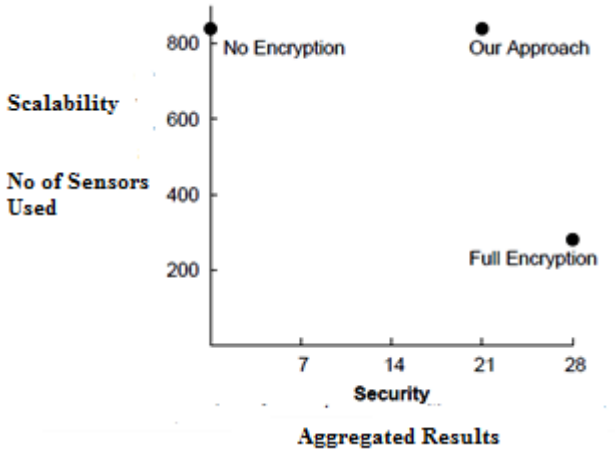

Fig -3: Scalability and security Trade off.

III. CONCLUSION

In this paper, we have proposed structure free aggregation schemes in wireless sensor network which ensures the security and scalability of the aggregated results of the base station. A special feature is that the base station can securely sensing data rather than aggregated results, but the transmission overhead is still acceptable. Moreover, we integrate the aggregate signature scheme 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.

6.REFERENCES

[1] H. OzgurSanli, SuatOzdemir and Hasan Cam, "SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks", Department of Computer Science and Engineering Arizona State University.

[2] HasanÇama,, SuatÖzdemira, PrashantNairb, DevasenapathyMuthuavinashiappana and H. OzgurSanlia ,"Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks", Department of Computer Science and Engineering a, Department of Electrical Engineering Ira A. Fulton School of Engineering, Arizona State University, Tempe, AZ 85287, USA.

[3] KarthikeyanVaidyanathan, Sayantan Sur, SundeepNarravula, PrasunSinha, "Data Aggregation Techinques in Sensor Networks", Technical Report OSU-CISRC-11/04-TR60

[4] Joao Girao , Dirk Westhoff , Markus Schneider "CDA: Concealed Data Aggregation for Reverse Multicast Traffic in Wireless Sensor Networks", NEC Europe Ltd. 69115 Heidelberg, Germany.

[5] M.NesasudhaandM.L.Valarmathi ,"An Energy efficient data transmission in Wireless Sensor Networks", International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009.

[6] HevinRajesh, D. , B. Paramasivan, "Fuzzy Based Secure Data Aggregation Technique in Wireless Sensor Networks", Journal of Computer Science, 2012

[7] Samuel Madden, Michael J. Franklin, and Joseph M. Hellerstein Wei Hong ,"TAG: a Tiny AGgregation Service for Ad-Hoc Sensor Networks", Appearing in 5th Annual Symposium on Operating Systems Design and Implementation (OSDI). December, 2002.

[8] 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.

[9] Jen-Yeu Chen, GopalPandurangan ,DongyanXu , "Robust and Distributed Computation of Aggregates in Wireless Sensor Networks",Computer Science Technical Reports 2004.

[10] Kai-Wei Fan, Sha Liu, and PrasunSinha "Structure-free Data Aggregation in Sensor Networks", Department of Computer Science and Engineering The Ohio State University, Columbus.

[11] Alexandre Viejo, Qianhong Wu, Josep Domingo-Ferrer "Asymmetric Homomorphisms for Secure Aggregation in Heterogeneous Scenarios",Preprint submitted to Elsevier Preprint 8 November 2010.

[12] Bronis R. de Supinski, Rob Fowler, Todd Gamblin, Frank Mueller, PrasunRatn, Martin Schulz ,"An Open Infrastructure for Scalable, Reconfigurable Analysis", International Workshop on Scalable

© 2015, IRJET.NET- All Rights Reserved

Tools for High-End Computing (STHEC), May 16, 2008.

[13] AmitManjhi, AnastassiaAilamaki, Bruce M. Maggs, Todd C. Mowry, Christopher Olston, Anthony Tomasic, "Simultaneous Scalability and Security for Data Intensive Web Applications",ACM.SIGMOD Chicago, Illinois, USA.Copyright 2006.

[14] R. Rajagopalan and P. Varshney, "Data-Aggregation Techniques in Sensor Networks: A Survey," IEEE Comm. Surveys Tutorials, vol. 8, no. 4, pp. 48-63, Oct.-Nov. 2006.

BIBLIOGRAPHIES

Mrs. Kavita Sunchu had B.E from BIGCE ,Solapur University,Solapur. She is a M.E. Student in CSE Departmentof SEIT,Solapur University,She is currently working for her M.E. Research project work under the guidance of Mr. Prakash Dainje.Her area of interest include Network Security,Web Designing.

Prof. Dhainje Prakash Bhagwan had is B.E.(Comp.Engg) from PVG's COET Pune, Pune University and M.B.A (IT) EIILM University and also M.Tech (IT) KSOU. Currently he is pursuing his Ph.D(CSE) from Bundelkhand University, Jhansi and he is currently working as Assistant Professor in CSE Department of SIET college of Engineering, Solpaur.

.

© 2015, IRJET.NET- All Rights Reserved