Perspective Study on Recoverable Concealed Data Aggregation in WSNs

John Major. J, Shajin Prince

Abstract— In Wireless Sensor Networks, Traditional Aggregation Schemes were used to aggregate the ciphertext without decryption. Since it causes problems such as aggregation constraint and failure of data integrity, a new technique called Recoverable Concealed Data Aggregation was introduced. Here in this scheme, the base station can recover all the sensing data even these data has been aggregated. Such a property is called as 'recoverable'. Also it suits well for both homogeneous and heterogeneous wireless sensor networks. In this paper, a comprehensive overview of all the supportive aggregation mechanisms was discussed briefly.

Keywords- data aggregation, wireless sensor networks, privacy homomorphism encryption.

I. INTRODUCTION

Wireless Sensor Networks (WSN) has been widely deployed in many applications, e.g., health care, military field surveillance, accident report, environment monitor etc. A WSN is composed of a large number of sensors which conspire with each other. Each sensor exposes a target within its radio range, performs simple computations, and interacts with other sensors. Normally, sensors are liable in communication, battery power, and computation capability; hence, reducing the power consumption is a severe concern for a WSN. Just a while ago, a practical solution called data aggregation [1], [2], [3] was introduced. The original concept is to aggregate multiple sense data by performing algebraic or statistical operations such as multiplication, addition, median, maximum, minimum, and mean of a data set, etc. Generally, data aggregation is achieved by cluster heads if the whole network is divided into several groups known as clusters. For example, in military terrain, sensors are used to fix radiation or chemical pollution. The base station (sink) may require the maximum value of all sensing data to trigger the immediate response; hence, each cluster head selects the maximum value of numerous sensing data of its cluster members and sends the result to the base station. Certainly, the communication cost is reduced since only aggregated results reach the base station. Unfortunately, an adversary has the ability to capture cluster heads. It would cause the adjustment of the whole cluster; consequently, several schemes, such as ESPDA [4] and SRDA [5], have been proposed. However, these schemes restrict the data type of aggregation or cause extra transmission on high. Further, an adversary can quiet obtain the sensing data of its cluster members after capturing a cluster head. To solve above problems completely, two ideas are used in recent research [6], [7], [8]. First, data are encrypted during show. Second, cluster heads directly aggregate encrypted data without decryption. A well-known access named Concealed Data Aggregation (CDA) [6] has been proposed based on these two ideas. CDA contribute both end-to-end encryption and in-networking processing in WSN. Since CDA applies privacy homomorphism (PH) encryption with additive homomorphism, cluster heads are adapted of executing addition operations on encrypted numeric data. Next, a few PH-based data aggregation schemes [7], [8] have been designed to achieve higher security levels.

In this paper, we introduce a concept named Recoverable Concealed Data Aggregation (RCDA). In RCDA, a base station can recover each sensing data generate by all sensors even if these data have been aggregated by cluster heads (aggregators).Also the perspective study of various supportive schemes for aggregation were discussed in this paper.

II. TERMINOLOGIES

A. Privacy Homomorphism Encryption

Privacy homomorphisms (PHs) are encryption transformations that allow direct computation on encrypted data. Well-Known secure PHs allows addition and multiplication to be carried out on encrypted data, but do not provide computation of inverses.

B. Wireless Sensor Networks

A WSN is composed of a large number of sensors which collaborates with each other. Each sensor identifies a target within its radio range, achieves simple computations, and communicates with other sensors.

C. Network Model

A WSN is controlled by a base station (BS). A BS has large bandwidth, sufficient memory, strong computing capability, and stable power to support the cryptographic and routing requirements of the whole WSN. Besides the BS, sensors (SNs) are also deployed to sense and gather responsible results for the BS. Typical SNs are small and low cost; hence, SNs are defined on storage, computation, and communication capability.

D. RCDA Scheme

RCDA scheme can be defined as follows. A base station can recover each sensing data generated by all sensors even if these data have been aggregated by cluster heads (aggregators).

E. Overhead

Overhead is any combination of excess or indirect memory, computation time, bandwidth, or other resources that are required to attain a particular goal. It is a special case of handling overhead.

Manuscript received on February, 2013.

Mr. J. John Major, Electronics and Communication Engineering, Karunya University, Coimbatore, India.

Prof. Shajin Prince, Electronics and Communication Engineering, Karunya University, Coimbatore, India.

F. Homogeneous and Heterogeneous WSNs

A homogeneous sensor network consists of duplicate nodes, while a hetero- geneous sensor network consists of two or more types of nodes (organized into hierarchical clusters).

G. Mykletun et al.'s Encryption Scheme

It is a concealed data aggregation scheme based on the elliptic curve El-Gamal (EC-EG) cryptosystem. It can be expressed by four procedures: key generation (KeyGen), encryption (Enc), aggregation (Agg), and decryption (Dec).

H. Boneh et al.'s Signature Scheme

It is an aggregate signature scheme which merges a set of distinct signatures into one aggregated signature. The scheme consists of five procedures: key generation (KeyGen), signing (Sign), verifying (Verify), aggregation (Agg), and verifying aggregated signature (Agg-Verify).

III. VARIOUS METHODOLOGIES FOR AN DATA AGGREGATION

There are various methodologies under the wireless sensor networks for providing secure data aggregation and to improve the efficiency. Few such methodologies are discussed here.

A. LEACH (Low Energy Adaptive Clustering Hierarchy) Protocol

LEACH Goals for Topology Control looks at ways to deal with networks that are dense by reducing transmission power, deciding which links to use, turning some nodes off.

LEACH - a clustering-based protocol that utilizes randomized rotation of local cluster base stations (cluster-heads) to evenly distribute the energy load among the sensors in the network. Data aggregation reduces amount of information to be sent to base station; large reduction in energy dissipation as computation is much cheaper than communication.

It can achieve as much as a factor of 8 in reduction in energy dissipation compared with conventional routing protocol. Conventional protocols may not be optimal for static sensor networks - direct communication, multi-hop routing, and static clustering.

B. HEED Protocol

HEED was designed to select different cluster heads in a field according to the amount of energy that is distributed in relation to a neighboring node. There are for primary goals are as follows. (1) Prolonging network life-time by istributing energy consumption, (2) Terminating the clustering process within a constant number of iterations/steps, (3) minimizing control overhead, (4) producing well distributed cluster heads.

The advantages of HEED protocols are the distribution of energy extends the lifetime of the nodes within the network thus stabilizing the neighboring node, does not require special node capabilities, such as location-awareness, Does not make assumptions about node distribution, Operates correctly even when nodes are not synchronized.

C. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001. AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It calls 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds. To provide security, AES uses four types of transformations: permutation, substitution, mixing, and key-adding.

D. Forward-Secure Sequential Aggregate MAC Scheme

To ensure forward security and to minimize resource consumption, the Forward-Secure Sequential Aggregate authentication Schemes have been introduced. It can be used to authenticate multiple messages when public (transferrable) verification is not required. If public (transferrable) verification is required we need an FssAgg signature scheme to check the authenticity of data records. The advantages can be MAC based scheme is highly efficient and both key exposure will be there along with good storage efficiency.

E. Hierarchical Trust Management Protocol

The objective of the anomaly detection steps is to provide an efficient and effective methodology of our hierarchical trust management addressing the problem of Trust formation, Trust aggregation, and Trust composition. The hierarchical trust management protocol maintains two levels of trust: SN-level trust and CH-level trust. These two levels of peer-to-peer trust evaluation process consider four different trust components described earlier: intimacy, honesty, energy, and unselfishness.

F. Trusted agent

The goal is to encrypt a message so that it cannot be decrypted by any person or third party not even the sender anticipation of a pre determined amount of time has passed. Here comes the action of a trusted agent and its functioning.

A Trusted Agent is a member of your organization who manages ECA Certificate enrolments [8]. The Trusted Agent ensures that your enrolment information is valid and accurate, which enables issuance of your ECA Certificate. Usually the Trusted Agent also assumes the role of the notary by notarizing the Subscriber Enrolment Form. We can efficiently enable timed release crypto.

G. Digital Signatures & Authentication Protocols

The most important development from the work on public-key cryptography is the digital signature. Message authentication shields two parties who exchange messages from any third party. But, it attack the two parties against each other. A digital signature is alike to the handwritten signature, and serves a set of security capabilities that would be difficult to implement in any other way. It has the following properties:

(1) It is essential to verify the author and the date and time of the signature, (2) It need to authenticate the contents at the time of the signature, (3) It conditions be verifiable by third parties, to tracing disputes.

Authentication Protocols are used to convince parties of each other's identity and to exchange session keys. They can be one-way or mutual. Central to the issues of authenticated key exchange are two issues: confidentiality and timeliness.

To avoid masquerade and to limit compromise of session keys, crucial identification and session key information must be communicated in encrypted form. This desires the prior existence of secret or public keys that can be used for this purpose. The second problem, timeliness, is important because of the threat of message replays.

H. Secure logging

It investigates the idea of immutability in the context of forward secure sequential aggregate authentication to provide finer grained verification.

The need for secure logging is well-understood by the security professionals, including both safeguard and practitioners. The ability to quickly verify all (or some) log entries is important to any application employing secure logging techniques.

IV. COMPARISON OF VARIOUS METHODOLOGIES

S.No	TITLE	OBJECTIVE	TECHNIQUE	MERITS	DEMERITS
1	Energy-Efficient Secure Pattern Based Data Aggregation for WSNs	To prevent the redundant data transmission from sensor nodes to cluster-heads by using ESPDA and the use of NOVSF Block-Hopping technique improves the security by randomly changing the mapping of data blocks to NOVSF time slots.	1. Energy-Efficient Secure Pattern based Data Aggregation. 2. NOVSF Block-Hopping technique.	1. Redundancy rate increases, ESPDA bandwidth occupancy decreases 2. NOVSF Block-Hopping technique that provides data communication security	1. Symmetric keys used in the security algorithms are not transmitted
2	Secure Reference-Based Data Aggregation Protocol for WSNs	To enhance the bandwidth usage and energy utilization by minimizing the transfer of redundant data. To reduce the number of bits transmitted, SRDA desires sensor nodes to send differential data instead of raw sensed data.	1.Secure Reference-Based Data Aggregation Protocol 2.A key distribution scheme with deployment estimation and applied an Aggregation Specific Security technique	1. Deployment estimation and not performing any online key distribution 2. SRDA yields significant savings in the energy consumption while preserving the data security.	1. Use of key distribution function is constraint factors.
3	Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks	To support the reverse multicast traffic to one particular destination in a multihop manner.	1. Conceals sensed data end-to-end by encryption 2. Efficient and flexible in-network data aggregation.	1. Increase the robustness and reliability of the connected backbone. 2.Limits an attacker's gain	1. Security approaches are not acceptable in WSNs where nodes can easily be corrupted
4	Efficient Aggregation of Encrypted Data in WSNs	To perform a simple and provably secure additively homomorphic stream cipher which allows efficient aggregation of encrypted data.	1. New homomorphic encryption Scheme	1. The influence of compromising a sensor is actually reduced	1. Rekeying operations for each sensor cause this scheme to be impractical. 2. A synchronization mechanism should be provided.

5	A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks	To use a novel probabilistic grouping technique to dynamically partition the nodes in a tree topology into multiple logical groups (subtrees) of similar sizes.	1. Principles of divide-and-conquer & commit and attest.	1. Achieve the level of efficiency 2. Assurance of the trustworthiness	1. Drop in the data packets
6	Aggregate and Verifiably Encrypted Signatures from Bilinear Maps	To show that aggregate Signatures give rise to verifiably encrypted signatures. Similar signatures enable the verifier to test that a given ciphertext C is the encryption of a signature on a given message. To support the encrypted signatures are used in contract-signing protocols.	1.Co-GDH Signature Scheme 2. Bilinear Maps	1. Key generation, aggregation, and verification require no interaction.	1.Chances are there to forger the message
7	Concealed Data Aggregation in Heterogeneous Sensor Networks Using Privacy Homomorphism	To reduce data redundancy and to summarize relevant and necessary information without requiring all pieces of the data.	1. Employs Privacy Homomorphism which offers end-to-end concealment of data and ability to operate on ciphertexts.	1. To improve energy efficiency, data aggregation and bandwidth utilization of sensor networks while providing secure communication. 2. Feasible for large heterogeneous wireless sensor networks	1. Computational overhead of privacy homomorphic encryption process is more.
8	Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks	To reduce the energy consumption tied to data transmission in a multi-hop wireless sensor network	1. On addition of homomorphic public key-encryption.	1. Minimize bandwidth overhead and thereby reduce the sensors 'energy consumption, even in the face of compromised nodes.	1. The number of aggregated values is quite high 2. Making the reverse mapping function is costly 3. Size of the cipher text is large

V. CONCLUSION

In this paper, various aggregation schemes related to recoverable data aggregation mechanisms were discussed for both homogeneous and heterogeneous wireless sensor networks. A special feature about the RCDA scheme is that the base station can securely recover all sensing data rather than aggregated results, but the communication overhead is still acceptable. This survey helps us to know more about the aggregation schemes in homogeneous and heterogeneous wireless sensor networks.

REFERENCES

1. 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.
2. S. Madden, M.J. Franklin, J.M. Hellerstein, and W. Hong, “TAG: A Tiny Aggregation Service for Ad-Hoc Sensor Networks,” Proc. Fifth Symp. Operating Systems Design and Implementation, 2002
3. J.-Y. Chen, G. Pandurangan, and D. Xu, “Robust Computation of Aggregates in Wireless Sensor Networks: Distributed Randomized Algorithms and Analysis,” IEEE Trans. Parallel Distributed Systems, vol. 17, no. 9, pp. 987-1000, Sept. 2006.
4. H. C¸ am, S. O ¨ zdemir, P. Nair, D. Muthuavinashiappan, and H. Ozgur Sanli, “Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks,” J. Computer Comm., vol. 29, pp. 446-455, 2006.
5. H. Sanli, S. Ozdemir, and H. Cam, “SRDA: Secure Reference- Based Data Aggregation Protocol for Wireless Sensor Networks,” Proc. IEEE 60th Int’l Conf. Vehicular Technology (VTC ’04-Fall),vol. 7, pp. 4650-4654, Sept. 2004.
6. 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.
7. 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, pp. 109-117, July 2005.
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., vol. 5, pp. 2288-2295, June 2006.
9. H. Chan, A. Perrig, and D. Song, “Secure Hierarchical In-Network Aggregation in Sensor Networks,” Proc. ACM 13th Conf. Computer and Comm. Security, pp. 278-287, 2006.
10. Y. Yang, X. Wang, S. Zhu, and G. Cao, “SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks,” ACM Trans. Information and System Security (TISSEC), vol. 11, no. 4,pp. 1-43, 2008.
11. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,” Proc. 22nd Int’l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 416-432, 2003.
12. S. Ozdemir, “Concealed Data Aggregation in Heterogeneous Sensor Networks Using Privacy Homomorphism,” Proc. IEEE Int’l Conf. Pervasive Services, pp. 165-168, July 2007.
13. 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 computing*, VOL. 23, NO. 4, APRIL 2012

AUTHORS PROFILE

Mr. J. John Major received his B.E degree from Jayaraj Annapackium CSI College of Engineering, Anna University in the year 2011. Currently pursuing his master's degree in communication systems. His area of interest includes Wireless Sensor Networks, Wireless Mess Networks and Antenna Design. Currently working on trust management in Wireless Sensor Networks, to improve the security in wireless Sensor Networks.

Mr. Shajin Prince received his B.E degree from Karunya University in the year 2008. He received his M.tech from Karunya University in the year 2010. Currently working as Assistant Professor in Karunya University. He is also a part time research scholar in Anna University. His research area includes Audio signal processing and Multimedia compression.