ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering &Technology (IJARCET)
Volume 2, Issue 3, March 2013

A Survey on Data Aggregation Techniques for Wireless Sensor Networks

Kriti Saini **Parveen Kumar** **Jatin Sharma**

Abstract-Wireless Sensor Network is an area of growing interest in which recent advancements in the field of sensing, computing and communication attracted various research efforts. Limitations of sensors involve power consumption, computation as well as communication capability. Data aggregation is one practical solution of constraint of power consumption. Various Data aggregation schemes have been proposed on the basis of privacy homomorphism. Privacy homomorphism allows direct computation on encrypted data. Thus, Data Aggregation helps in reducing transmission overhead as well as better security.

Index Terms—Concealed data aggregation, wireless sensor networks.

I. INTRODUCTION

Wireless Sensor Node (WSN) is a network which consists of small sensor nodes that gather data from the surrounding environment with sensing, computing and communication capabilities. There are various applications in which wireless sensor networks are deployed such as military field Surveillance, environmental monitoring, intrusion detection, habitat monitoring and health care to detect temperature, entity movement, humidity and seismic activity. WSN is also defined as special class of ad hoc wireless network. Wireless sensor network contains thousands of sensor nodes distributed in an environment which detects target within its range, collects data and perform computation on that data. Sensor nodes consist of application specific sensors, simple processor, wireless transceiver and battery. Sensor nodes are deployed with limited amount of power; therefore, a commonly employed technique of data aggregation is used to minimize the transmission overhead.[1] Various data aggregation schemes based on privacy homomorphism also provides security. Privacy homomorphism means Computation performed on the encrypted data without decrypting it.

II. ISSUES IN WIRELESS SENSOR NETWORKS

The major issues that affect wireless sensor network are following: Hardware and Operating system for WSN, Wireless radio communication characteristics, medium access schemes, deployment, localization, synchronization, calibration, network layer, transport layer, data aggregation and data dissemination, database centric and querying, architecture, programming models for sensor networks, middleware, quality of service and security. Main objective of sensor nodes is Data gathering.

Data is sensed periodically by the surrounding environment and process

it before transmitting it to the sink. Number of sensors as well as frequency of reporting the data depends on a particular application. Sensors often generate redundant data and a huge amount of data is collected for processing by the base station.[2] This leads to the Data Aggregation. Some of the design issues in data aggregation include: unreliability of sensors, improving of clustering techniques, improving in-networking aggregation techniques. Main focus is towards energy conservation. Other issues are improving security in data transmission, handling tradeoffs, improving quality of service.

III. CDA: CONCEALED DATA AGGREGATION IN WIRELESS SENSOR NETWORKS

In this paper, Tiny and cheap cost sensors consist of application-specific sensors, a wireless transceiver, simple processor and a battery. Problem of end-to-end encryption of data is introduced. An encryption transformation known as privacy homomorphism that allows encrypted data to be computed without decrypting it. Let P and C denote Plaintexts and Cipher texts respectively. Let K be the key space.

Encryption transformation: E: K x P→C

Decryption transformation: D: K x C→P

PH can be performed additively and multiplicatively.

Additive Homomorphism:

$a+b = D_k(E_k(a)+ E_k(b))$

Multiplicatively Homomorphism: $a \times b = D_k(E_k(a) \times E_k(b))$. RSA is a multiplicative PH.

IV. RCDA: RECOVERABLE CONCEALED DATA AGGREGATION FOR DATA INTEGRITY IN WIRELESS SENSOR NETWORK.

In this paper, RCDA schemes are proposed for two types of WSN i.e homogeneous and heterogeneous WSN. Special feature of this scheme is that the base station can securely recover all sensing data generated by the sensor nodes rather than aggregated results with less transmission overhead. In addition, to ensure the authenticity and integrity, the aggregate signature scheme is integrated. Although integration of signature brings additional cost but still it is affordable for WSN.

V. CDAMA: CONCEALED DATA AGGREGATION FOR MULTIPLE APPLICATIONS IN WIRELESS SENSOR NETWORK.

CDAMA is the first concealed data aggregation scheme for a multi-application environment. CDAMA is based on the same logic as BGN, which is constructed on a cyclic group of elliptic curve points. BGN is implemented by using two points of different orders; on the other hand, CDAMA is designed by using multiple points, each of which has different order. Through CDAMA,[3] the cipher texts from distinct applications can be aggregated but not mixed. CDAMA is application on WSNs while the number of groups or applications is not large. This scheme provides concealed data aggregation between multiple groups. Basically CDAMA is a modification from Boneh et al.'s PH scheme.

Three practical application scenarios are considered for CDAMA:

a) First scenario is designed for multi-application WSNs. Practically, sensor nodes with different purposes may be distributed in same environment for example smoke alarms, thermometer sensors both are deployed together. Now, if we apply conventional concealed data aggregation schemes, the cipher texts of different applications cannot be aggregated together because if we do so the decrypted aggregated result will be incorrect. Therefore, Aggregation of cipher texts of different applications should be done separately.
b) Second scenario is designed for single application WSNs. CDAMA uses the construction of multiple groups to lessen the effect of compromising sensor nodes. Any attacker can devise data only in that group that is compromised.
c) Third scenario is designed for secure counting capability. Base station knows exactly how many messages are aggregated.

VI. PUBLIC KEY BASED CRYPTOSCHEMES FOR DATA CONCEALMENT IN WIRELESS SENSOR NETWORK.

Mykletun proposed various Public key Encryption Schemes with the comparison of their costs as well as indication of how practically they can be implemented. He worked on a concealed data aggregation scheme based on elliptic curve Elgamal (EC-EG) cryptosystem. Symbols that are used in this scheme are + and x, where + denote addition and x denote scalar multiplication on elliptic curve points. Four procedures are there in this scheme: a) Key Generation: Generate a key pair of private and public key. b) Encryption: Encrypt message with public key. c) Aggregation: A few aggregation functions are listed which can be computed over enciphered data and recommended which cryptosystem should be used in which application. d) Decryption: Decrypt cipher text with private key.[4]

He showed that their indeed exists a viable public-key cryptosystem candidate for WSNs. This scheme has two applications, Aggregation and Long term data storage. The former involve functions like sum, average, variance, checksum and movement detection. The latter application relies on the fact that data is stored in the nodes for later retrieval when needed. Due to limited storage capability, the amount of values is reduced. Therefore, we can use the concept of Data aggregation to reduce the amount of data stored at the nodes.

Symbols that are used in this scheme are + and x, where + denote addition and x denote scalar multiplication on elliptic curve points. Four procedures are there in this scheme: a) Key Generation: Generate a key pair of private and public key. b) Encryption: Encrypt message with public key. c) Aggregation: A few aggregation functions are listed which can be computed over enciphered data and recommended which cryptosystem should be used in which application. d) Decryption: Decrypt cipher text with private key.

VII. AGGREGATE AND VERIFIABLY ENCRYPTED SIGNATURES FROM BILINEAR MAPS

A concept of aggregated signatures and construction of an efficient aggregate scheme based on bilinear maps is introduced. An aggregate signature is a digital signature that support aggregation means if n signatures are given on n different messages from n users, then to aggregate all these signatures into a short signature will be possible. Aggregate Signatures are helpful in reducing the size of messages in secure routing protocols as well as in reducing the size of certificate chains.[5] Introduction of additional constraint for security purposes, that an aggregate signature is valid only if it is an aggregation of signatures on distinct messages. This scheme includes one additional procedure: Key Generation (KeyGen), Signing (sign), verifying (Verify), aggregation (Agg), verifying aggregated signature (Agg- Verify). Verifiably encrypted signatures can be obtained with the help of aggregated signatures. These signatures are helpful in applications like online contract signing.

VII. REFERENCES:

[1] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar , " *Issues in Wireless Sensor Networks*", Proc. World Congress on Engineering vol.1, London, U.K, 2008.

[2] Joao Girao, Markus Schneider, Dirk Westhoff, " *Issues in Wireless Sensor Networks*", Germany.

[3] Chien-Ming Chen, Yue Hsun Lin, Ya-Ching Lin and Hung-Min Sun, "*RCDA:Recoverable Concealed Data Aggregation*", IEEE Trans. Parallel Systems, vol 23, no.4, Hsinchu, Taiwan, pp727-733, 2011.

[4] 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, Germany, pp. 2288-2295, 2006.

[5] 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.