www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 3 March, 2014 Page No. 4017-4021

Recoverable Concealed Data Aggregation with Multiple Applications in WSN

[1]M.Amrutha, [2]M.Kamarajan

[1]R.V.S College of Engineering & Technology, Dindigul, amru.mecse20@gmail.com

[2]R.V.S College of Enigeering & Technology, Dindigul.

***Abstract*—Recently several data aggregation techniques based on symmetric key encryption mechanism have been proposed on wireless sensor networks (WSNs). These types of data aggregation methods result better security compared with the traditional aggregation mechanisms. In this proposed Recoverable Concealed Data Aggregation approach, Cluster Head (CH) can directly aggregate the cipher texts of an individual nodes present on that particular cluster. Based on symmetric schemes, the provider can conduct aggregation queries without decryption. Here, a Concealed Data Aggregation (CDA) technique is extended with the symmetric key encryption. Also, the clustering strategy is presented to divide the sensor nodes into multiple clusters. Cipher Block Chaining (CBC) algorithm is used to encrypt the sequence of bits into a single block or unit. The proposed scheme has three contributions. First, it is designed for a multiple application environment. The base station retrieves the application-specific data from the aggregated cipher texts. Next, it mitigates the impact of compromising attacks in single application environments. Finally, it degrades the attacks from unauthorized aggregations. The result shows that the proposed Recoverable Concealed Data Aggregation with Multiple Applications (RCDA-MA) performs better than the existing CDAMA system.**

***Index Terms*—Base Station, Ciphertext, Block Chaining (CBC), Concealed Data Aggregation (CDA), Data Aggregation, Wireless Sensor Networks (WSNs), and Symmetric key encryption**

I. Introduction

THE Wireless Sensor Network consists of thousands of spatially distributed autonomous sensors to monitor physical or environmental conditions like temperature, sound, pressure etc. Depending on the purpose of each application, sensor nodes are customized to read the various types of data. Also, sensor nodes are restricted by the resources due to the limited computational power and low battery power. To provide better energy utilization cluster based WSN have been proposed. The sensor nodes are divided into a number of clusters. For each cluster, one CH is elected to aggregate the result from the other sensor nodes present in the same cluster. Further, the CH forwards the data to the base station (BS) based on the usual routing paths. A data aggregation technique is one of the data mining techniques which have been widely used in many domains. The goal of the data mining techniques is to extract information from a data set and transform it into an understandable structure for further usage. Data aggregation is a type of data and information mining process. In terms of wireless sensor network, there avail two different solutions from existing works, given as Concealed Data Aggregation (CDA) and Multiple-Application (MA). CDA is an improved version of the in-network aggregation (INA), which is contrast to the classic hop-by-hop (HBH) ensure the end-to-end security, i.e. the encrypted values do not need to be decrypted for the aggregation. Instead the aggregation is performed with the encrypted values and only the receiver can decrypt the result.

Message aggregation can reduce communication overhead considerably, but message aggregation makes security more complex. Each intermediate node can change forge or discard messages or simply transmit false aggregation values, so one compromised node can able to significantly alter the final aggregation value. So the encryption process is needed to encrypt the message using a unique key shared between each device and the base station. Since, each intermediate node desires to know the received messages to perform the aggregation. The simplest ciphers are known as symmetric-key ciphers. Communicating parties share a common private key which is used to transform the message from plain text to cipher text. The cipher text is communicated to the other party, and then the process is reversed using the same private key. The primary obstacle in making private key symmetric ciphers useful is distribution of private keys.

In this paper, Recoverable Concealed Data Aggregation technique is proposed among multiple applications. The CDA techniques are exposed to attackers due to the lack of security mechanisms. In this proposed method each message is encrypted with the symmetric key. The sensor nodes send the secure data to the base station. The base station communicates to the individual user without decrypting the message; it yields to high-level secure transmission. The cipher texts from different applications are aggregated into one cipher text. Also clustering strategy is presented to ensure the energy consumption among the sensor nodes.

The rest of the paper is organized as follows. Section II presents a description about the previous research which is relevant to the concealed data aggregation techniques and security mechanism used on data aggregation. Section III involves the detailed description about the proposed method. Section IV presents the performance analysis. This paper concludes in Section V.

II. Related Work

This section deals with the works related to the Data Aggregation techniques and the security mechnasims used for secure transmission. *Chien-Ming et al* proposed a recoverable concealed data aggregation technique for data integrity. The system provides better secure transmission between the base station and the individual user [1]. *Westhoff et al* presented a Malleability Resilient Concealed Data Aggregation (MR-CDA). This approach combines homomorphic MACs with additively homomorphic encryption tachniques. It helps to detect the outside attackers which maliciously add resp inject encrypted data to an aggregated encrypted data format [2]. *Ozdemir et al* designed a hierarchial concealed data aggregation protocol that allows the aggregation of data packets that are encrypted with different encryption keys. During the decryption, the base station was able to classify the encrypted and aggregated data based on the encryption keys. An eliptic curve cryptography based homomorphic encryption algorithm was presented to offer data integrity and confidentiality along with the hierarchial data aggregation [3].

Yue-Hsun et al proposed a sorting scheme on ciphertexts without decryption; where ciphertexts were generated by Elliptic Curve Eigamal encryption. This method preserves assitive homomorphic property of the Curve Eigamal encryption [4]. *Huang et al* proposed a secure encrypted data aggregation method. This method eliminates the redundant sensor readings without using encryption and privacy during transmission. This technique was resilient to known-plaintext attacks, chosen-plaintext attacks, ciphertext-only attacks and man-in-the middle attacks [5]. *Dezfouli et al* proposed a protocol for concealed data aggregation. Here, the network was divided into virtual cells. Nodes within each cell produce a shared key to send and receive the concealed data with each other [6]. *Roy et al* proposed an aggregation framework which combines multipath routing schemes with supplicate insensitive algorithms to accurately compute the aggregate messages. Also, a light weight verification algorithm was presented. Here, the base station can determine if the computed aggregate includes any false contribution [7].

Applebaum et al proposed a privacy-preserving data aggregation among a large number of participants. Here, scalability and efficiency was achieved through a 'semi-centralized architecture that divides responsibility between a proxy and a database. The cryptographic protocol protects the privacy of both the participants and the keywords [8]. *Li et al* proposed an energy efficient and high accuracy scheme for secure data aggregation. The accurate data aggregation was achieved without releasing private sensor readings and without introducing significant overhead on the battery-limited sensors [9]. *Chu et al* proposed a Receiver-Bounded Online/Offline Identity-based Encryption (RB-OOIBE). The encryption process was splitted into two parts. One is offline part, where all heavy computations were done without the knowledge of the receiver's identity and the plaintext message. Another one is the online stage, where only light computations such as modular operation and symmetric key encryption were required combined with the receiver's identity and the plaintext message. Each offline ciphertext can be reused for the same receiver [10]. *Rasmi et al* presented a paired cipher text public key system based on RSA. This method incorporates two hard mathematical problems like discrete logarithms and factoring to provide secure transmission [11].

Peng et al proposed an index structure that supports cipher text indexing and retrieval. It allows full-text search on the encrypted documents in multiple formats without decryption [12]. *Hohenberger et al* proposed a method for craeting chosen ciphertext secure encryption. The focal point of this method was discovering a new abstarction called Detectable Chosen Ciphertext Security (DCCA) [13].*Agrawal et al* presented a detailed study of most of the symmetric encryption techniques with their advantage and limitations [14]. *Li et al* proposed a lightweight scheme for secure sensor association a key management in Body Area Networks (BAN). A different kind of secret keys was generated on demand after deployment. The Group Device Pairing (GDP) supports batch deployment of sensor nodes to save setup time. This system does not depend on any additional hardware devices and it was based on symmetric key cryptography [15].

III. RCDA-MA: Recoverable Concealed Data Aggregation with Multiple Applications

The proposed system called RCDA-MA, which provides Recoverable Concealed Data Aggregation between multiple groups. The clustering network aggregates the data and forwarding to the base station. An adversary can deduce the key from only the encrypted messages. RCDA-MA realizes the aggregation query in Database, which is a trusted service provider. To secure the database a symmetric key scheme is used. The cipher texts for the entire transmission are implemented by using two points of different orders. So, the effect of one point can be removed by multiplying the aggregated ciphertext with the order of the point and then the scalar of other point can be obtained. The proposed model provides secure communication and data transmission from Base Station to individual users.

The following sections are briefly addressing the delivery of group public keys to sensor nodes with security criteria's.

A. Setup Phase

The entire network is divided into clusters; each cluster has one CH to aggregate the outcome of the other nodes present in the corresponding cluster. There are two approaches are incorporated to set up the sensor nodes for key distribution: One is Key Pre-distribution and the other one are Key Post-distributive.

1) Key Pre-distribution

The necessary keys and functions are preloaded into the sensor nodes and cluster heads (CH). Each node is assigned with a symmetric key. So that, they can work correctly after being spread out over a geographical region.

2) Key Post-distribution

The sensor nodes are capable of nothing about keys, before the sensor node deployment. The sensor node loads only the key shared with the Base Station prior to their deployment such as individual key and the master secret key. Once these nodes are deployed, they can run to elect the CHs and construct the clusters. After that, the Base Station sends the corresponding symmetric keys, encrypted by the pre-shared keys to sensor nodes and CHs.

Data transmission among clusters on the entire network need to follow the following steps:

1. Using a symmetric key algorithm, each node is assigned to group key or public key.
2. Users or nodes generated the message and send it to the CH for that particular cluster.
3. Verify the public key for all the data.
4. The data will be processed for the encryption phase.
5. All the message/data are encrypted using public key.
6. All the encrypted messages are combined to get a single Ciphertext key, which is stored in the database.

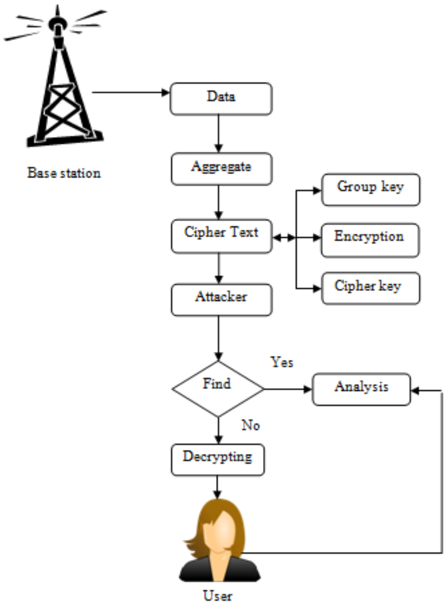

Fig.1.Secure Transmission from Base Station to the user

Symmetric Key Algorithm Steps

```
DESCryptoServiceProvider key = new
DESCryptoServiceProvider();
        byte[] buffer;
            // Create a memory stream.
            MemoryStream ms = new MemoryStream();
            // Create a CryptoStream using the memory stream and
                the CSP DES key
            CryptoStream crypstream = new CryptoStream(ms,
key.CreateEncryptor(), CryptoStreamMode.Write);
            // Create a StreamWriter to write a string
                to the stream.
            StreamWriter sw = new StreamWriter(crypstream);
            // Write the strText to the stream.
            sw.WriteLine(strText);
            // Close the StreamWriter and CryptoStream.
            sw.Close();
            crypstream.Close();
            // Get an array of bytes that representsthe memory
                stream
            byte[] buffer = ms.ToArray();
            // Close the memory stream.
            ms.Close();
            // Return the encrypted byte array.
            return buffer;
```

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plain text will encrypt to different ciphertext in a stream cipher. Stream ciphers come in several flavors but two are worth mentioning here. Self-synchronizing stream ciphers calculate each bit in the key stream as a function of the previous n bits in the key stream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit key stream it is. Synchronous stream ciphers generate the key stream in a fashion independent of the message stream but by using the same key stream generation function at sender and receiver.

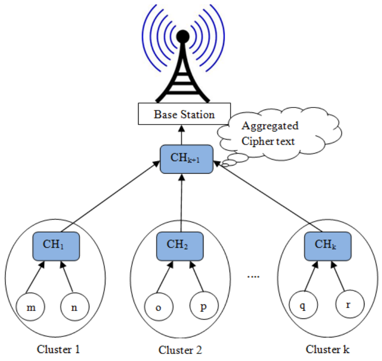

Fig.2. Example of Ciphertext aggregation

B. Cipher Block Chaining

Cipher block chaining (CBC) is a mode of operation for a block cipher (one in which a sequence of bits is encrypted as a single unit or block with a cipher key applied to the entire block). Fig.3. depicts the CBC mode encryption and decryption process.

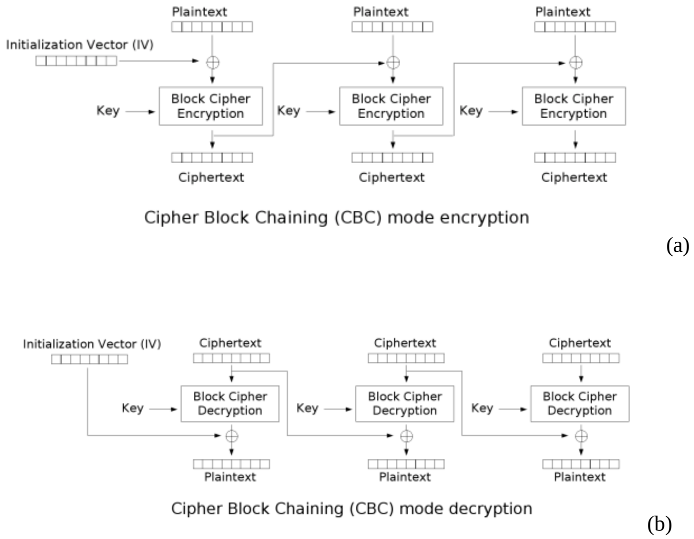

Fig.3. Cipher Block Chaining mode operations

Step 1: CBC converts the data and keys into binary. Then, use five bits for each number in this example - just enough to cover the alphabet. The six remaining binary numbers (27-32) represent the characters '0' through '5'. Here is the binary equivalent of our plaintext and key:

Plaintext: 10011 00111 00100 00001 10100 00010 01010 10010 10011 01110 01111 10010 00111 00100 10001 00100
Key: 11000 00100 00000 00111

Step 2 :

The next step is to break the plaintext into some larger (12 bit) blocks and remove whitespace from the key:

Plaintext: 100110011100 100000011010 000010010101 001010011011 100111110010 001110010010 00100100
Key: 11000001000000000111

Cipher block chaining uses an initialization vector (IV) of a certain length. One of its key individuality is that it uses a chaining mechanism that causes the decryption of a block of ciphertext to depend on all the proceeding cipher text blocks. As a result, the entire validity of all preceding blocks is contained in the immediately previous ciphertext block. A single bit error occurred in the ciphertext block affects the decryption of all the successive blocks. Rearrangement of the order of the ciphertext blocks causes decryption to become corrupted. Identical ciphertext blocks only result if the same plaintext block is encrypted using both the same key and the initialization vector. It has the advantage over the Electronic Code Book mode in that the XOR'ing process hides plaintext patterns. Ideally, the initialization vector should be different for any two messages encrypted with the same key.

C. *Abstraction of RCDA-MA*

The prototype of observation uses different generators to construct different key pairs for clusters. The cipher text from different applications can be aggregated together, but they are not mixed. The ciphertext can be integrated into a single ciphertext and transmitted to the Base station. The Base Station does not decrypt the aggregated ciphertext for security reasons. An individual user can send the request to the Base Station to retrieve the message/data. The Base Station forwards the ciphertext for that particular user. Later, the user decrypts the message individually.

The main drawback of asymmetric CDA schemes is that the CH can manipulate aggregated results without encryption capability. The CH can able to increase the value of the aggregated result of aggregating the same ciphertext of sensed reading repeatedly, or decrease the value of selective aggregation. Since, the Base Station does not know the exact number of ciphertext aggregated. To avoid this problem, the proposed RCDA-MA provides secure counting for multiple applications. The Base Station exactly knows how many sensed readings are aggregated while it receives the final output.

IV. Performance Analysis

This section presents the performance evaluation of the proposed Recoverable Concelaed Data Aggregation system. The performance is evaluated based on the following measures:

A. *Aggregation accuracy*

The accuracy metric is defined as the ratio between the collected summations by the data aggregation scheme used and the real summation of all the individual sensor nodes. Fig.3 illustrates the accuracy of RCDA-MA and CDAMA with respect to different time intervals.

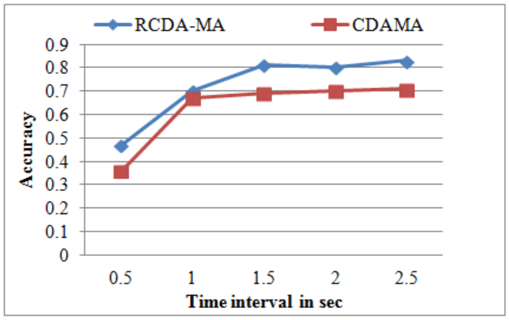

Fig.4.Accuracy of RCD-MA and CDAMA

In fig.4 it is observed that the accuracy increases as the time interval increases. The proposed RCDA-MA system results better accuracy than the existing CDAMA system. Hence, the chance of collisions occurring is also reduced.

B. *Energy Consumption*

It is the measure of energy utilized to transmit the message/data throughout the network. The clustering strategy tends to reduce the amount of energy consumption during transmission. The result is evaluated for before aggregation and after the aggregation of the encrypted message. Fig.5. shows that the aggregated cost takes lesser energy than the encrypted cost.

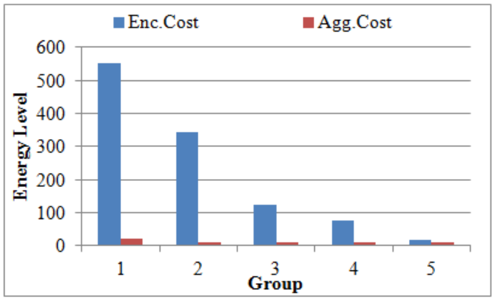

Fig.5. Energy level for encryption cost and aggregated cost

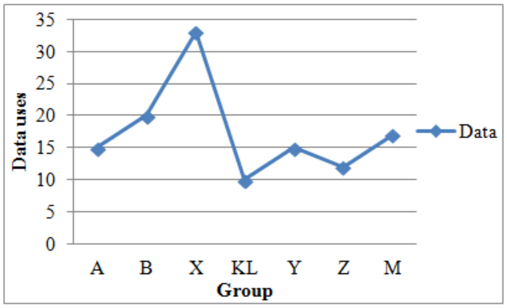

Fig.6. Transmitted data vs Groups

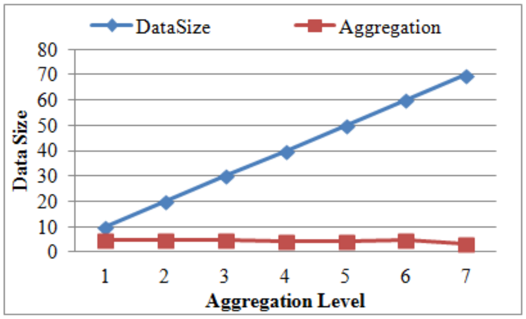

Fig.7. Data size vs Aggregation level

Fig.6 and Fig.7 describes the data transmission with respect to the different clusters and the aggregation level.

Conclusion

The proposed Recoverable Concealed Data Aggregation method is implemented in multiple applications. Generally CDA techniques are exposed to attack due to the lack of security mechanisms. Here, the base station communicates to the individual user without decrypting the message. Hence, it results secure transmission between the Base Station and individual user. Also clustering strategy is presented to ensure the energy consumption among the sensor nodes. The experimental result shows that the proposed RCDA-MA provides better results interms of accuracy, energy level and aggregation level than the existing CDAMA approach. Hence the proposed system results secure communication than the existing system.

In future, this approach is extended with the privacy preserving data aggregation methodology in the networking domain.

References

[1] C. Chien-Ming, L. Yue-Hsun, L. Ya-Ching, and S. Hung-Min, "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, pp. 727-734, 2012.

[2] D. Westhoff and O. Ugus, "Malleability resilient (premium) Concealed Data Aggregation," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a*, 2013, pp. 1-6.

[3] S. Ozdemir and Y. Xiao, "Integrity protecting hierarchical concealed data aggregation for wireless sensor networks," *Computer Networks*, vol. 55, pp. 1735-1746, 2011.

[4] L. Yue-Hsun, H. Bing-Zhe, S. Hung-Min, and C. Yen-Hsueh, "CDS: Concealed data sorting scheme in wireless sensor networks," in *Computer Symposium (ICS), 2010 International*, 2010, pp. 370-375.

[5] S.-I. Huang, S. Shieh, and J. Tygar, "Secure encrypted-data aggregation for wireless sensor networks," *Wireless Networks*, vol. 16, pp. 915-927, 2010.

[6] M. A. Dezfouli, S. Mazraeh, and M. Yektaie, "The New Method of Concealed Data Aggregation in Wireless Sensor: A Case Study," *World Academy of Science, Engineering and Technology*, vol. 60, 2011.

[7] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," *Information Forensics and Security, IEEE Transactions on*, vol. 7, pp. 1040-1052, 2012.

[8] B. Applebaum, H. Ringberg, M. J. Freedman, M. Caesar, and J. Rexford, "Collaborative, privacy-preserving data aggregation at scale," in *Privacy Enhancing Technologies*, 2010, pp. 56-74.

[9] H. Li, K. Lin, and K. Li, "Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks," *Computer Communications*, vol. 34, pp. 591-597, 2011.

[10] C.-K. Chu, J. K. Liu, J. Zhou, F. Bao, and R. H. Deng, "Practical ID-based encryption for wireless sensor network," in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, 2010, pp. 337-340.

[11] P. Rasmi and V. Paul, "An implementation of a new public key system based on RSA which leads hackers solve multiple hard problems to break the cipher," in *Intelligent Systems Design and Applications (ISDA), 2012 12th International Conference on*, 2012, pp. 656-661.

[12] L. Peng, R. Li, H. Wang, X. Gu, K. Wen, and Z. Lu, "An Encrypted Index Mechanism in Ciphertext Retrieval System," in *Web Information Systems and Applications Conference (WISA), 2011 Eighth*, 2011, pp. 131-136.

[13] S. Hohenberger, A. Lewko, and B. Waters, "Detecting dangerous queries: a new approach for chosen ciphertext security," in *Advances in Cryptology–EUROCRYPT 2012*, ed: Springer, 2012, pp. 663-681.

[14] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," *International Journal on Computer Science and Engineering (IJCSE) Vol*, vol. 4, pp. 877-882, 2012.

[15] M. Li, S. Yu, W. Lou, and K. Ren, "Group device pairing based secure sensor association and key management for body area networks," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1-9.