A Secure Concealed Data Aggregation for Multiple Applications in Wireless Sensor Networks

Bharat Bhushan, Sandeep Verma, Amit Kumar Rai

Abstract— **Data Aggregation is an important aspect in Wireless Sensor Networks WSNs and this is because it reduces the amount of data to be transmitted over the network. This is done by either avoiding the transmission of redundant data or aggregating the result from different sensors and forwarding only the aggregated result further to BS. In previous studies authors used homomorphic encryption properties for concealing communication during aggregation such that encrypted data can be aggregated algebraically without decrypting them. These schemes are not satisfying multi applications which lead to proposal of CDAMA (Concealed Data Aggregation for Multi Applications). It is designed for multi applications, as it provides secure counting capability and also it reduces the effect of compromising secrets of a single application. In wireless sensor networks or environments the sensor nodes are defenseless and are vulnerable to some attacksTo prove our proposed scheme's robustness and efficiency, we conducted the simulations, comprehensive analysis and comparisons in the end.**

Index Terms—**Concealed Data Aggregation, Privacy homomorphism, Sensor nodes, wireless Sensor Networks**

I. Introduction

Wireless sensor networks (WSNs) have gained much significance in past few years because of its huge number of applications and areas of use. The application domain ranges from military investigations to environment monitoring and ecological monitoring. The sensor networks generally comprises of several sensor nodes gathered from deployed environments in a large scale [1]. Sensor nodes in sensor networks face a major problem as sensor nodes are energy constrained and these have limited power, storage, communication, and processing capabilities. Thus the major problem in wireless sensor network is energy consumption. Thus to conserve energy and power sensor networks brings forth the concept of data aggregation [2]. This means converting many values sensed from different environments into one single value and aggregated value is computed at sink by the use of some mathematical functions [3]. The technique for aggregation is used mainly for the reduction in amount of data to be sent in the sensor environments. As a result of reduction of amount of data communicated within WSNs, there is energy conservation of battery [4]. Sensor nodes send their readings to a special type of node for performing aggregation of data i.e., aggregators, that sends only the condensed or aggregated reading further [5]. These aggregators may be some kind of special nodes or normal sensor nodes also.

Sensor nodes requires high security as it prompts many security issues like confidentiality, data integrity, data authentication, key management, etc. High security is required in wireless sensor networks so it is one of the most popular research topics and much advancement have been reported on in recent years [6]. In this paper we mainly focus on security aspect of data transmission in WSNs and we propose a method of secure transmission of encrypted data across sensor nodes in sensing environments as well as secure key generation methods involved in attack detection and prevention in wireless sensor networks.

Encryption of data being transmitted in WSNs is necessary as this type of sensors can be subject to many different types of attacks. The attacker can either listen secretly the data being transmitted in WSNs (attacker may deduce the secret key) or send forged or duplicated data to sensor nodes, aggregators or base station (attacker may send forged data to cheat BS without knowing the secret key) or even compromise secrets of components of WSNs by capturing them.so as encryption is necessary sensor nodes must encrypt data on hop-by-hop basis. [7]. The mechanism of key generation involves an overhead activity making this an expensive and complicated operation [9]-[10]. Different key generation schemes have been proposed but they involve high computations for encryption of data and require more CPU, bandwidth and memory

II. Preliminaries

A. Privacy Homomorphism Encryption

An encryption scheme with homomorphic property is privacy homomorphism encryption. The homomorphic property means that the algebraic operations on PT can be executed with the manipulation of the corresponding CT with the help of a key.

Dk (Ek (m1) O Ek (m2) = m1 @ m2 ,

Where Dk ( ) is decryption with key K., Ek ( ) is encryption with key K, O denote operations on cipher text and @ denote operations on plaintext.

PH schemes are of two types, similar to conventional encryption schemes. First one is Symmetric cryptosystems where keys are identical and second one is Asymmetric cryptosystem where keys are different. Symmetric PH schemes have greater efficiency as compared to Asymmetric PH schemes. The best known Asymmetric schemes are the one based on ECC (Elliptic Curve Cryptography) which provides the same security as RSA cryptosystem and that too with a smaller key size and cipher text. A 160-bit ECC

Manuscript received May 19, 2015

Bharat Bhushan, Department of computer science & engg., Birla Institute of Technology,Mesra, Ranchi, India

Sandeep Verma, Department of computer science & engg., Birla Institute of Technology,Mesra, Ranchi, India

Amit Kumar Rai, Department of computer science & engg., Birla Institute of Technology,Mesra, Ranchi, India

cryptosystem provides the same security as provided by a 1,024-bit RSA cryptosystem [18].

B. Data Aggregation and Encryption

There is a major problem of aggregation of encrypted data in WSNs which was firstly introduced by gira et al. in [9] and it was further refined in [11] .Homomorphic encryption schemes was used to enable arithmetic operations over cipher texts that is to be transmitted on a multi-hop basis. Secure aggregation also involves some problems with public-key encryption mechanisms. Solution to public key encryption mechanism is to equip nodes with private keys for increasing the security level. This limits the effect of attacker that compromises some of the nodes but this is not deployed yet because of certain reasons mainly being the high computational cost involved in encryption and decryption of plaintext and cipher texts. Also the expansion in bit size during plaintext to cipher text conversion involves high overhead hence depleting the sensors energy.

C. Routing Protocols

The efficiency of a sensor networks heavily depends on the routing protocols used. Energy Efficient & Secure Pattern Based Data Aggregation protocol (ESPDA) was proposed that considered data aggregation and security together for wireless sensor networks [12]. In ESPDA cluster heads prevent transmission of redundant data from sensor nodes making ESPDA as energy and bandwidth efficient. Next concept was Secure Reference Based Data Aggregation (SRDA) in which the raw sensed data by sensor nodes is compared with referenced data values and the only the differential data is transmitted rather than the raw data [13]. Hein Zelman, et al. [14] proposed a hierarchical clustering algorithm for sensor networks. This was Low Energy Adaptive Cluster Hierarchy (LEACH) based protocol. Here the operations were divided into rounds and during each round another set of nodes acts as CHs. Main advantage of this was that energy consumption is uniformly distributed among all the nodes and the main disadvantage was that it uses scheduling criteria based on (TDMA) time division multiple access which makes it inclined to long delays when it is applied to large sensor networks. An enhancement over LEACH protocol was published in [15]. This protocol was PEGASIS (Power Efficient Gathering in Sensor Information Systems). It was a chain based protocol designed for extending the lifetime of the network which elects a leader from the chain, based on residual energy level which results in average energy spent by each node being reduced. Virtual Grid Architecture (VGA) was another energy efficient routing paradigm proposed in [16]. This protocol used data aggregation and also in network processing to maximize the lifetime of the network as it performs data aggregation at two levels: local and global. PEGASIS greatly prolongs the lifetime of network when transmission range is limited and VGA saves more energy when transmission range is more.

D. CDA Based Privacy Homomorphism Schemes

Our work focusses on the solution for confidential data exchanges in WSNs that incorporates data aggregation. To the best of our knowledge, CDA (Concealed Data Aggregation) was the first concept that proposed a solution for end-to-end encryption along with the data aggregation model. In [7], the basic idea of CDA was introduced and it also showed the way to apply privacy homomorphism in WSNs. CDA provides end-to-end security along with providing in-network processing. They use algebraic properties of the applied PH: additive and multiplicative PH. In recent years, Castellucia, et al. Introduced an efficient data aggregation of encrypted data in WSNs and this is also based on additive homomorphism of encryption scheme [11]. Next concept introduced was CDAMA where the private keys is kept secret and it is only known by the base station. There is same public key for SNs in same group and no one outside knows the public key of the group. Also here BS extracts individual aggregated results from aggregated CT by performing individual decryption.

III. Module design

A. WSN set-up Model

In this module we set up a WSN environment in which network is divided into static clusters containing SN. Sensor nodes having limited energy and secure communication among them are necessary. Aggregator nodes are chosen based on residual energy level of nodes. Each sensor nodes sends the sensed data to corresponding aggregators which aggregates the received value and transfers the aggregated result to Base Station BS. We assume the Base Station to have immense computational power so it generates two types of keys, both public and private keys for sensor nodes using CDAMA scheme. All sensors have common public key but different private keys. Now the generated key is assigned to all the sensor nodes.

B. Aggregation Model

In WSN information is collected by sensor nodes from deployed environments and this collected information is forwarded to base station via multi-hop transmission based on cluster topology. This accumulated transmission results in high energy consumption for the intermediate nodes. Thus to increase the lifetime of the sensor networks cluster topology enables the intermediate nodes to perform data aggregation(AG).After performing aggregation AGs forwards the aggregated result to next hop. Aggregation of data takes place by two methods i.e., algebraic operations (e.g., adding or multiplying) or statistical operations (e.g., mean, median, mode, max, min). AG forwards only the aggregated result instead of forwarding the entire raw data.

C. Attack Model

Here in this model, we create two unauthorized sensor nodes called the attacker nodes which have more energy and threshold as compared to the normal nodes. There are different types of possible attacks on WSNs. Here we in this paper are considering the DOS attack Denial-of-Service attack which causes Black hole attack, Wormhole attack, Sybil attacks, Selective forwarding attacks etc. DOS attack is based on node-id. The attacker node behaves as normal nodes

with its changed node id and receives data packets and drops them causing loss of data. Attacker nodes also change the threshold of the normal nodes thus drying the energy of the normal nodes. There are two methods followed by the attacker nodes here. Firstly, it traces the node id and changes the node id (based on node id) and secondly changes the threshold value (based on energy level).

IV. System Design and Architecture

In this paper, we consider a wireless sensor network system consisting of a fixed base station and large number of sensor nodes. These sensor nodes are homogenous in functionalities as well as capabilities. We suppose, the sink as reliable always , but the sensor nodes are subject to be compromised by the attackers. In this wireless system, the data are sensed by the sensor nodes and are transmitted to a base station with the help of CHs that performs data aggregation. We also assume that, all sensor nodes and the BS use the symmetric radio channel, sensor nodes are distributed randomly, and are energy constrained. The protocol used is CDAMA that elects CHs, and a sensor node transmits the data to its CH.

V. Our Scheme

First we have used the AODV routing protocol and performed Denial of Service Attack over the AODV routing protocol which was removed by the use of Concealed data aggregation techniques.CDAMA was implement through following procedures.

A. Key generation procedure

1. If source is transmitting data
2. Count the number of requests
3. Evaluate N [expr($len_q1)*($len_$q2)*($len_$q3)]
4. Initialize E
5. Randomize GEN as value of index.
6. Evaluate H = [(q1)*(q2)]*GEN
7. Evaluate Tmax = [(T)/(x)]
8. Evaluate P = [(q2)*(q3)*(GEN)]
9. Find Public key [((N)*(E)*(P)*(H)*(Tmax))]
10. Return Public key

B. Encryption procedure

1. If data is received at destination
2. Count the number of reply
3. If request= message_id then randomize the value of R
4. Calculate cipher text as per expression C = [(M)*(P)+(R)*(H)]
5. Return the value of ciphertext as C.
6. Calculate aggregation count AGG_C=[(Message_id *P)+(Message_id *Q)+($Message_id *H)]
7. Return the value of AGG_C

C. Aggregation procedure

1. Compute the aggregated result as cipher text C'=C1+C2.it also includes the randomness of both groups.
2. Return C'

D. Decryption procedure

1. Compute M,M=logp(q2q3*C)
2. Return M.

VI. Simulation Parameters

This model is implemented using a network simulator 2.34. The simulation parameters are 500 X 500 sq. area, and consisted of 50 to 60 number of nodes with flat-grid topology, two ray ground ground radio propagation model and 802.15.4 MAC layer .AODV, and CDAMA from different perspectives such as Average-delay, Packet Delivery ratio, Energy Spent and Throughput. The network simulator set up is shown below in the table.

TABLE I
SIMULATION PARAMETERS

Sl. No.	PARAMETERS	Values
1	Simulation area	500 X 500 square meters
2	Propagation	Two ray ground propagation
3	Queue type	Drop tail
4	Antenna type	Omni antenna
5	Number of nodes	50 to 60 nodes
6	Topology	Flat grid topology
7	Routing protocol	CDAMA
8	Maximum packets in interface queue length	200
9	Network interface type	Phy/wireless
10	MAC type	802.11

VII. Simulation Results and Discussions

A. Average Delay

Average delay includes all the possible types of delays that may be either due to buffering during route discovery latency, or queuing at the interface queue or may be the transfer times of the data packets. The figure shows the end to end delay incurred in transferring the data from source node to sink node by different routing schemes. The maximum delay is in AODV with attack, Sybill attack. In an efficient network the average delay should be less and when CDAMA is compared to AODV under attack, it has lesser delay.

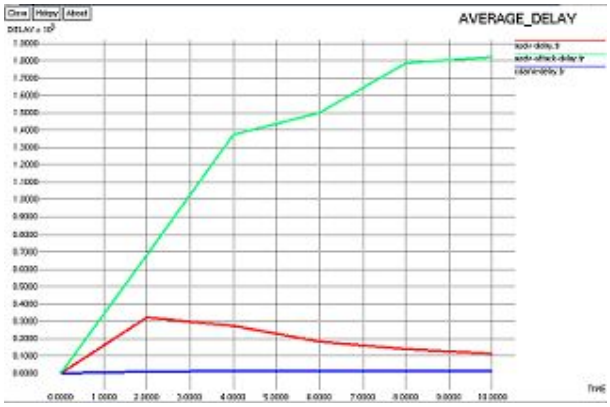

Fig.1. Variation of average delay with time

B. *Packet Delivery Ratio*

Packet Delivery Ratio is the ratio of the data packets that has been delivered to destinations to those that has been generated by constant bit rate (CBR) sources. The figure shows the packet delivery ration achieved by different routing techniques. The packet delivery ratio is highest for CDAMA technique followed by normal AODV and then the least packet delivery ration is with AODV under attack.

Fig.2. Variation of Packet delivery Ratio with Time

C. *Energy Consumption*

Average Energy Consumption by the sensor nodes in the network is one of the most important metrics to evaluate energy efficiency of the routing protocol that has been proposed. The figure shows the energy spent by nodes in the sensor network. Energy consumption for CDAMA technique is lesser than AODV and maximum energy consumption is by the AODV under attack.

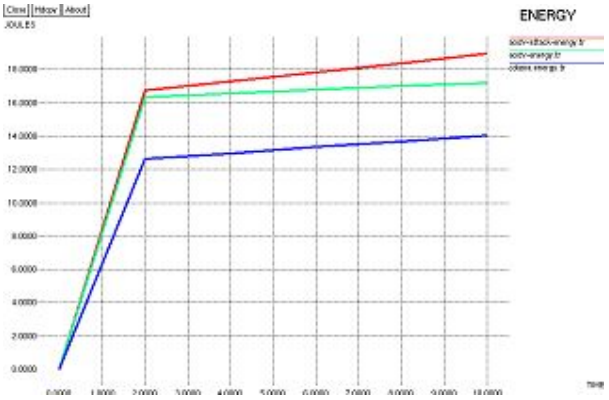

Fig.3. Variation of energy consumption with time

D. *Throughput*

Throughput is the total number of routing packets transmitted per data packets that has been delivered at destination. The throughput is maximum for AODV followed by CDAMA and then AODV under Attack.

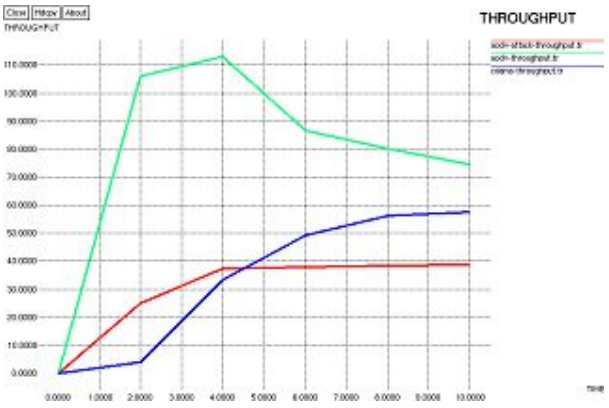

Fig.4. Variation of Throughput with time.

VIII. CONCLUSION

The work proposes a secure, increased throughput and a better packet delivery ration scheme than normal technique. Here the concealed data aggregation technique is used where cipher text of different applications can be aggregated together. CDAMA technique that mitigates the impact and reduces the overall damage to acceptable condition. CDAMA performs better than the traditional AODV routing protocol but the proposed technique provides higher security. The proposed technique defends the altered routing, selective forwarding and wormhole attacks. This technique may be vulnerable to some attacks.In our future work we will be proposing a technique for higher security than the proposed technique.

REFERENCES

[1] I. Akyildiz,W. Su,Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks" IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] R. Min,A. Chandrakasan, "Energy-Efficient Communication for Ad-Hoc Wireless Sensor Networks," Proc. Conference Record of the

35th Asilomar Conference Signals, Systems and Computers, vol. 1, 2001.

[3] B. Przydatek, D. Song,,A. Perrig, "SIA: Secure Informations Aggregation in Sensor Networks," Proc. First International Conf. Embedded Network Sensor Systems, pp. 255-265, 2003.

[4] R.Chandramouli, S.Bapatla, and K.P.Subbalakshmi, "Battery power-aware encryption.ACM transactions on information and system security," pp. 162-180, 2006.

[5] K.Akkaya,M.Demirbas, RS.Aygun, "The Impact Of Data Aggregation on the performance of Wireless Sensor Networks," wiley wireless Communication Mobile Computing (WCMC), J(8), 171-193, 2008.

[6] J.Girao, M. Schneider, and D.Westhoff, "CDA:Concealed Data Aggregation in wireless sensor networks,"Proceedings of the ACM workshop on Wireless Security, 2004.

[7] 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.

[8] C.d. Westhoff,B.Lamparter, and A.Weimerskirch,"on digital signaturesin ad hoc networks," J.Eur.Trans. telecom, vol.16, no. 5, pp. 411-425, 2005.

[9] R.Watro, D.Kong, S.Cuti, C.Gardiner, C.lynn, and P.kruus, "Sensor networks with public key technology", in proc. 2nd ACM Workshop Security ad hoc sensor network, pp.59-64, 2004.

[10] C.karlof ,D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures,"in the proc IEEE Int. Workshop Sensor Netw. Protocols Appl., May 2003, pp. 113-127, May 2003.

[11] C.castelluccia, E.Mykletun and G.Tsudik, "Efficient Aggregation of encrypted data in wireless sensor networks," Mobile and Ubiquitous Systems: Networking and Services, 2005.

[12] H. Cam, S. O¨zdemir, P. Nair, D. Muthuavinashiappan, and H.O. Sanli, "Energy-Efficient Secure Pattern Based Data Aggregation for WSNs," Computer Comm., vol. - 29, no. - 4, pp. 446-455, 2006.

[13] H. Sanli, S. Ozdemir, and H. Cam, "SRDA: Secure Reference based Data Aggregation Protocol for WSNs," Proc. IEEE 60th Vehicular Technology Conf. (VTC '04-fall), vol. 7, 2004.

[14] M. Younis,M.Youssef and K.Arisha,"Energy Aware Routing in Cluster Based Sensor Networks", in the Proceedings of the 10th IEEE/ACM(MASCOTS2002), Fort Worth, TX , October 2002.

[15] S.Lindsay and C.Raghavendra, "PEGASIS: Power Efficient gathering in Sensor Info. Systems",international conference on communications, 2001.

[16] J.N.Al-Karaki,et al., "data Aggregation in Wireless Sensor Networks-Exact and approximate algorithms," Proc IEEE Wks. High Perf. Switching and Routing 2004, phoenix, AZ , Apr.18-21,2004.

[17] Sanjeev Setia, a. Sankardas Roy and Sushil Jajodi "Secure Data Aggregation in Wireless Sensor Networks" Proc. of 33rd STOC, pp. 266–275, 2001.

[18] N. Koblitz, A. Menezes,S., Vanstone,"State of Elliptic Curve Cryptography,"Designs, Codes & Cryptography, vol. 19, no. 2, pp. 173-193, 2000.

Bharat Bhushan (M'26).Date Of Birth-17th Dec 1989. MTech Information Security (Dept. Of Computer Sc. & Engg.) student at Birla Institute Of Technology, Ranchi, Jharkhand-835215, India.

He has worked as Network Engineer for 1 years in HCL Infosystems Ltd., Noida.

Sandeep Verma (M'25).Date Of Birth-1st Jan 1991. MTech Information Security (Dept. Of Computer Sc. & Engg.) student at Birla Institute Of Technology, Ranchi, Jharkhand-835215, India.

Amit Kumar Rai (M'28).Date Of Birth-5th May 1987. ME Software Enggineering (Dept. Of Computer Sc. & Engg.) student at Birla Institute Of Technology, Ranchi, Jharkhand-835215, India.