A Survey on Privacy Preserving Aggregation in Wireless Sensor Network

Damor Meena[1]Panchal Krunal[2]
[1,2]ME Student, Computer engineering
[1]Gujarat technological University, Ahmedabad
[2]L.J. Institute of Engineering and Technology, GTU

Abstract—*Security is always a booming in wireless sensor networks (WSNs).Providing data Aggregation while preserving data privacy is a problem in wireless sensor network research. Privacy-preserving data aggregation has emerged as an important concern in designing data aggregation algorithm. Data aggregation while privacy preserving data privacy and security is a main challenging problem in wireless sensor network research. protecting the data privacy in many Wireless sensor network applications is a major concern data aggregation scheme privacy. This survey paper reviews different techniques for the privacy.*
Keywords: – Data aggregation, security, homomorphic encryption, privacy preserving , encryption

I. INTRODUCTION

A wireless sensor network (WSN) is an ad-hoc network composed of small sensor nodes deployed in large numbers to sense the physical world. Wireless sensor networks have very broad application prospects including both military and civilian usage. They include surveillance [1], tracking at critical facilities [2], or monitoring animal habitats [3]. Sensor networks have the potential to radically change the way people observe and interact with their environment. Sensors are usually resource-limited and power-constrained. They suffer from restricted computation, communication, and power resources. Sensors can provide fine-grained raw data. Alternatively, they may need to collaborate on in-network processing to reduce the amount of raw data sent, thus conserving resources such as communication bandwidth and energy. We refer to such in-network processing generically as *data aggregation*. In many sensor network applications, the designer is usually concerned with aggregate statistics such as *SUM*, *AVERAGE*, or *MAX/MIN* of data readings over a certain region or period. As a result, data aggregation in WSNs has received substantial attention.

II. DATA AGGREGATION

In typical wireless sensor networks, sensor nodes are usually resource-constrained and bettry –Limited .In order to save resources and energy, data must be aggregated to avoid overwhelming amounts of traffic in the network. There has been extensive work on data aggregation schemes in sensor networks, The aim of data aggregation is that eliminates redundant data transmission and enhances the lifetime of energy in wireless sensor network. Data aggregation is the process of one or several sensors then collects the detection result from other sensor. The collected data must be processed by sensor to reduce transmission.It can be the base station or sometimes an external user who has permission to interact with the network. Datatransmission between sensor nodes, aggregators and the querier consumes lot of energy in wireless sensor network. and reporting them back to the upper nodes where sensor nodes sensing.[19]

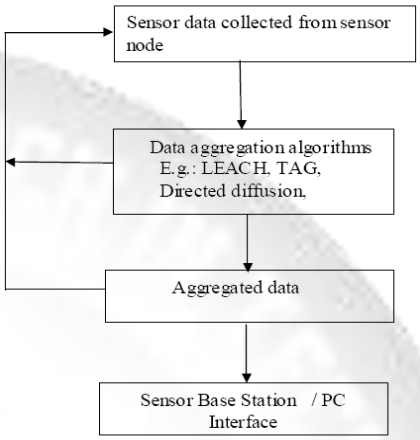

Fig. 1: General architecture of the data aggregation algorithm.

A. Advantage

With the help of data aggregation process we can enhance the robustness and accuracy of
information which is obtained by entire network, certain redundancy exists in the data collected from sensor nodes thus data fusion processing is needed to reduce the redundant information. Another advantage is those reduces the traffic load and conserve energy of the sensors.

B. Disadvantage:

The cluster head means data aggregator nodes send fuse these data to the base station. this cluster head or aggregator node may be attacked by malicious attacker. If a cluster head is compromised, then the base station (sink) cannot be ensure the correctness of the aggregate data that has been send to it. Another drawback is existing systems are several copies of the aggregate result may be sent to the base station (sink) by uncompromised nodes. It increase the power consumed at these nodes.

III. AGGREGATION TECHNIQUES

There are many types of aggregation techniques are present some of them are listed below

1) Centralized Approach: This is an address centric approach where each node sends data to a central node via the shortest possible route using a multihop wireless protocol. The sensor nodes simply send the data packets to a leader, which is the powerful node. The leader aggregates the data which can be queried.

2) In-Network Aggregation[13]: In-network aggregation is the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption (in particular energy), thereby increasing network lifetime. There are two approaches for in-network aggregation: with size reduction and without size reduction.

In-network aggregation with size reduction refers to the process of combining & compressing the data packets received by a node from its neighbors in order to reduce the packet length to be transmitted or forwarded towards sink. In-network aggregation without size reduction refers to the process merging data packets received from different neighbors in to a single data packet but without processing the value of data.

*3) Tree-Based Approach[14]:*In the tree-based approach perform aggregation by constructing an aggregation tree, which could be a minimum spanning tree, rooted at sink and source nodes are considered as leaves. Each node has a parent node to forward its data. Flow of data starts from leaves nodes up to the sink and therein the aggregation done by parent nodes.

*4) Cluster-Based Approach[15]:*In cluster-based approach, whole network is divided in to several clusters. Each cluster has a cluster-head which is selected among cluster members. Clusterheads do the role of aggregator which aggregate data received from cluster members locally and then transmit the result to sink.

IV. PRIVACY PRESERVING TECHNIQUES

Wen bo he et al.[4] gave two privacy-preserving data aggregation schemes for additive aggregation functions. The first scheme – Cluster-based Private Data Aggregation (CPDA) leverages clustering protocol and algebraic properties of polynomials. The second scheme – Slice-Mix-AggRegaTe (SMART) builds on slicing techniques and the associative property of addition.

CLAUDE CASTELLUCCIA et al.[5] they propose a simple and provably secure encryption scheme that allows efficient additive aggregation of encrypted data. Only one modular addition is necessary for ciphertext aggregation. The security of the scheme is based on the in distinguishability property of a pseudorandom function (PRF), a standard cryptographic primitive. We show that aggregation based on this scheme can be used to efficiently compute statistical values, such as mean, variance, and standard deviation of sensed data, while achieving significant bandwidth savings. To protect the integrity of the aggregated data, we construct an end-to-end aggregate authentication scheme that is secure against outsider-only attacks, also based on the in distinguishability property of PRFs.

Arijit Ukil [6] gave scheme is developed to provide privacy preservation in a much simpler way with the help of a secure key management scheme and randomized data perturbation technique. We consider a scenario in which two or more parties owning confidential data need to share only for aggregation purpose to a third party, without revealing the content of the data. Through simulation results the efficacy of our scheme and compare the result with one of the established scheme the system model, based on which the scheme is developed. It is shown that there are N numbers of source nodes or sources which collect or produce the private data. These sources are the owners of the private data. Against the query of the service provider or the server, the sources answer the query of the server

MARK MANULIS et al.[7] design the first general framework for secure information aggregation in WSNs focusing on scenarios where aggregation is performed by one of its nodes. The framework achieves security against node corruptions and is based solely on the symmetric cryptographic primitives that are more suitable for WSNs in terms of efficiency. We analyze performance of the framework and unlike many previous approaches increase confidence in it by a rigorous proof of security within the specially designed formal security model.

Suat Ozdemir et al.[8] investigates the relationship between security and data aggregation process in wireless sensor networks. A taxonomy of secure data aggregation protocols is given by surveying the current ‘‘state-of-the-art’’ work in this area. In addition, based on the existing research, the open research areas and future research directions in secure data aggregation concept are provided they present a comprehensive overview of secure data aggregation concept in wireless sensor networks. they survey the state-of-the-art data aggregation protocols and categorized them based on network topology and security. Although the presented research addresses the many problems of data aggregation, there are still many research areas that needs to be associated with the data aggregation process, especially from the security point of view. As for the general data aggregation concept, the relation between routing mechanisms and data aggregation protocols have been well studied as they are highly correlated topics.

Butty ANet al.[9] The aim of the proposed work is to compare the performance of TAG in terms of energy efficiency in comparison with and without data aggregation in wireless sensor networks and to assess the suitability of the protocol in an environment where resources are limited.
Vimal Kumar et al.[17] present an energy efficient, privacy preserving data aggregation

algorithm which also preserves data integrity in WSNs. analyze the security of the algorithm and provide proofs for confidentiality and integrity. Enhanced algotirhm which can detect corrupt aggregators that inject false data into the system. Results establish that the algorithms are lightweight in terms of energy and introduce very little delay in the network.

V. HOMOMORPHIC ENCRYPTION TECHNIQUES

There are various homomorphic techniques for the secure aggregation

Craig gentry[18] propose a fully homomorphic encryption scheme – i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Our solution comes in three steps. First, we provide a general result – that, to construct an encryption scheme that permits evaluation of arbitrary circuits, it suffices to construct an encryption scheme that can evaluate (slightly augmented versions of) its own decryption circuit; they call a scheme that can evaluate its (augmented) decryption circuit bootstrappable

Wu Jiehong et al.[11] presents a protection scheme of mobile agent(AMHCFES) in network management application,which combining protect method of Homomorphic encryption and composite function technology.in this The correctness and security proof of AMHCFES protection scheme are given and malicious hosts can be avoided effectively using this scheme

Liang Chen et al.[12] presents the concept of exponential homomorphism and porposes an exponential hommorphism and proposes an exponential homomorphic encryption algorithm based on RSA.Thecorrectness and the security of the proposed exponential homomorphism are analyzed. The exponential homomorphism is also an algebraic homomorphic encryption algorithm. The proof and the example show the proposed algorithm can encrypt coefficients and exponents of polynomial functions, hide the skeleton of the encrypted polynomial, and implement non-interactive evaluation of encrypted exponential functions and polynomial functions.

Fangyuan JIN et al.[17] presents a scheme is the verifiability of Evaluate function. Its security and other parameters are based on concrete Fully Homomorphic Encryption scheme they put the FHE's evaluation functions into different groups, constructing the verifiable evaluation function, and get a secure Verifiable Evaluate function. they used the verifiable evaluation functions to have constructed a semantic secure and input/output verifiable VFHE scheme. Guangli Xiang et al.[16] the interrelated technique is discribed and a modified ElGamal Encryption is introduced. The modified Encryption can meet multiplicative homomorphism and additive homomorphism and advance security.

VI. Conclusion

In This paper surveyd that existing works of data aggregation and homomorphic encryption and their techniques. those techniques are analyzed and performance of the security of data but still much works need to be in aggregation and homomorphic encryption for the better performance.

References

[1] D. Culler, D. Estrin, And M. Srivastava, "Overview Of Sensor Networks," Ieee Computer August 2004.
[2] N. Xu, S. Rangwala, K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, And D. Estrin, " A Wireless Sensor Network For Structural Monitoring "Proceedings Of The Acm Conference On Embedded Networks Sensorsystems, Baltimore, Md, November 2004.
[3] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, And J. Anderson, "Wireless Sensor Networks For Habitat Monitoring" Wsna '02 Atlanta, Geprgia, September 2002.
[4] Wen Bo He, Xue Liu,,Hong Nguyen,Klara Nahrsted " Pda: Privacy-Preserving Data Aggregation In Wireless Sensor Networks" Ieee 2011.
[5] Claude Castelluccia" Efficient And Provably Secure Aggregation Of Encrypted Data In Wireless Sensor Networks" Acm Transactions On Sensor Networks, Vol 5, No. 3, Article 20, Publication Date: May 2009.
[6] Arijit Ukil "Privacy Preserving Data Aggregation In Wireless Sensor Networks" Ieee Icwcmc 2010
[7] Mark Manulis Jo¨ Rg Schwenk "Security Model And Framework For Information Aggregation In Sensor Networks" Acm Transactions On Sensor Networks, Vol. 5, No. 2, Article 13, Publication Date: March 2009.
[8] Suat Ozdemir A,*, Yang Xiao" Secure Data Aggregation In Wireless Sensor Networks: A Comprehensive Overview" 2009 Elsevier.
[9] Vimal Kumar, Sanjay Madria "Pip:Privacy And Integrity Preserving Data Aggregation In Wireless Sensor Networks " International Symposium On Relible Distribute Systems Ieee 2013
[10] Butty´An, L., Schaffer, P., and Vajda, I. 2006. "Ranbar: Ransac- Based Resilient Aggregation In Sensor