2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) 978-1-7281-4889-2/20/$31.00 ©2020 IEEE 10.1109/ICCMC48092.2020.ICCMC-000160

The Challenges for Context –Oriented Data Accumulation with Privacy Preserving in Wireless Sensor Networks

T.G.Babu[1,2]
[1]Assistant Professor,
PG & Research Department of Computer Science
Arignar Anna Government Arts college,Cheyyar
India,Tamilnadu
E-Mail :babuit.17@gmail.com

V.Jayalakshmi
Professor
School of Computing Science
[2]VISTAS,Pallavaram
Chennai,Tamilnadu
E-Mail:jayasekar1996@yahoo.co.in

Abstract -

Wireless Sensor Networks (WSNs) plays a vital role in our everyday lives. In WSNs the data are to be sensed between one node to another set of nodes in the network for the purpose of achieving transmission. At the time of transmitting sensed data in the Wireless Networks it may utilize large amount of energy (like power consumption, payload, etc.) for any operation. Accumulating data plays vital role in conserving energy in the network framed using wireless sensors. Accumulation of the data is a procedure which was mainly designed to minimize the overhead in the communication as well as control energy utilization in sensor nodes during the process of data collection. A data aggregation protocol plays a firewall for protecting data among the elements of wireless transmission. Enhancing the lifetime of wireless networks is a challenging issue. In this paper we analyse the challenges for privacy preserving in protocols of data accumulation (aggregation). initially the accumulation protocol is based on various metrics like energy consumption, accuracy of data, authentication of data and confidentiality of data. Here we also identify various resolvable issues for enhancing quality of preserving privacy in aggregation protocols.

Keywords: - Networks framed with the wireless sensors, Data Accumulation, Privacy preservation, Encryption, Decryption.

1. INTRODUCTION

Nowadays the networks are framed using sensors communicating in wireless medium play an unavoidable role in our day-to-day life because it changes everything as Internet of Things (IoT) in our life. Wireless Sensor Networks consists of spatially distributed wireless sensor devices which are used to observe the physical or environmental conditions such as behavioural monitoring, habitat monitoring, temperature, sound and pressure, etc. The Special characteristics of WSNs such as self-deployment and fault tolerance and identification to make them widely in many monitoring and tracking applications, including health and wellness monitoring, traffic monitoring, environmental monitoring, etc. A Sensor is an electronic device that response based on detecting some category atmospheric changes.[1].. However data points (nodes) are generally low-power energy based device.

In the process collecting data from multiple elements of wireless networks to the base station (Server Node) may contain redundant and highly correlated data. Data aggregation is a way for collecting or aggregating(performing some aggregate operations) using various data aggregation approaches. Data aggregation mainly used to reduce the redundant type of transmissions for increasing the bandwidth and energy utilization of elements in the WSNs[2]. The important performance of data aggregation protocols like security, accuracy, energy saving and others. Based on the above issues we can determine the protocol which is well suited for sensor nodes.

Structure of Data Aggregation

The Figure1 indicate the basic structure of data aggregation[3] in wireless sensor networks. It includes

Sensed data among heterogeneous WSNS – this is a process of collecting information between different types of nodes.

Data Aggregation Approaches – This is a set of procedures (algorithms) to perform data aggregation in the network. Several approaches or protocols can be implemented for achieving this task.

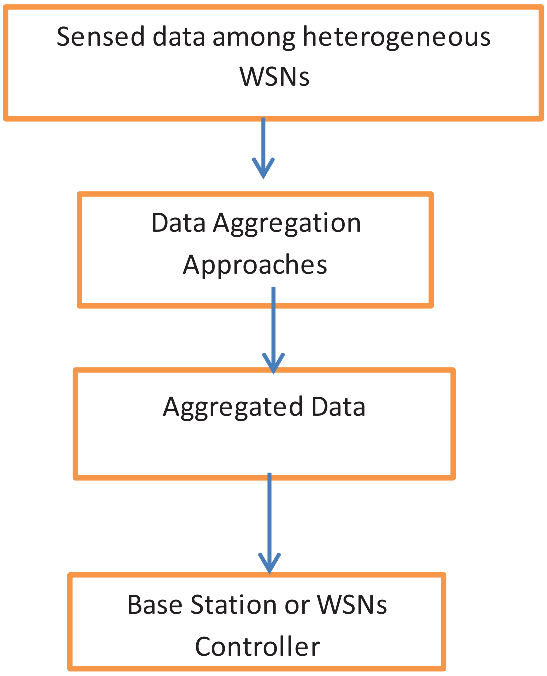
Sensed data among heterogeneous WSNs
Data Aggregation Approaches
Aggregated Data
Base Station or WSNs Controller

Fig 1.Structure For Accumulating Data Through the Wireless-Sensors.

Aggregated Data – The aggregated data or processed data without redundancy and encrypted data based on aggregation approaches.

Base Station - The centralized node in the network system to execute the communication between networks.

The recent issue of Wireless Sensor Networks is how to protect the sensitive data being collected, transmitted and analysed in wireless sensor networks. In this paper we analysed the important challenges for privacy preservation techniques during data aggregation in WSNs.

2. PRIVACY PRESERVING TECHNIQUES IN WSNS

Privacy preservation is a way of protecting the data that are transmitted among the sensor nodes. Preservation is a process of retaining the securable data through various security policies.

There are two important privacy preserving mechanisms are:

Data-Oriented Privacy Preserving:- It focus the privacy of data that can be collected ,posted or sensed by the sensor nodes in WSNS

Context-Oriented Privacy Preserving:- It focus the privacy based on contextual information like location,timing,flow of data in WSNs.

Privacy preserving can be identifies based homogeneous networks and heterogeneous networks

We have chosen the parameters[2] to identify the challenges of various privacy preservation aggregation techniques is:

Accuracy – The purity of the information in the transmission. It indicates the level of originality of the sensed data among the networks. If the sensed data is not accurate, then the privacy of data transmitted is threatened.

Delay- The amount of time needed to transfer the sensed data between source and destination. The longest delay of sensed data may detect intrusions and violations of data.

Overhead- The execution cost to enhance to achieve security preservation in protocols. The algorithms must possess with low processing overhead.

Topology- It determines the organization of nodes in the wireless network.

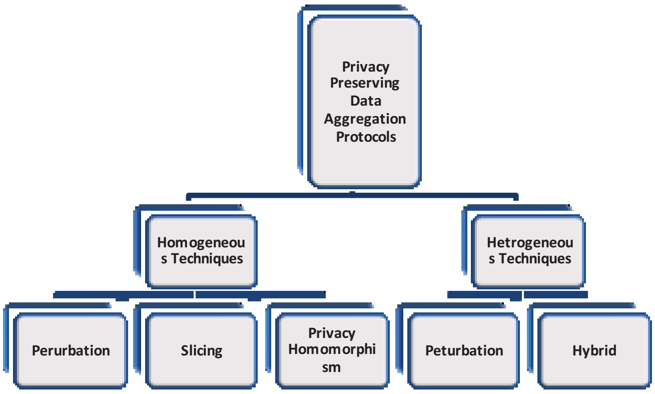

Fig 2. Privacy preserving techniques in data aggregation

Effectiveness- Indicating the computation power of privacy detection algorithms.

Here we can analyse the performance of existing protocols in the area of context oriented privacy preserving

3. ANALYSIS OF CONTEXT- ORIENTED PRIVACY PRESERVING

In wireless sensor networks, sensor nodes are actually resource-based and limited battery power, hence we aggregate data to avoid overhead and network traffic, since it enhance the energy[4] of sensor nodes.

To address the problems of privacy preserving during data aggregation several existing protocols are developed. Here we identify the challenges in three protocols:

A. CPDA**: CPDA**[5] **means Cluster based private Data Aggregation.** The first random key generation algorithm for encrypting sensed data to avoid attacks in the networks. CPDA consists of three levels of process: Cluster Forming, Calculate Aggregation between nodes and Cluster Head Data Aggregation.

Cluster Formation: CPDA categorizes the sensor nodes in WSNs into Cluster Head(CH) and Cluster Members. It creates group of sensor nodes into clusters and selecting a particular node as cluster head(CH) for all clients. The CH gather data from the specific cluster nodes and transmit the aggregated data to base station[6]. The main goal of forming cluster is to identify noise sensed data for the purpose of recognizing its source and destination address.

Cluster Data Aggregation: Here the data aggregation can be performed at each cluster. At the time data aggregation, every sensor node may generate confidential data with the help of shared public key and private key by using random key generation[7]. After generating keys the captured data are encoded and transmit to every data points inside the cluster network. After receiving the sensed data, each cluster node computes some polynomial operation for satisfying the additive property of polynomial as well as conveys it's each outcome to its corresponding head of the cluster. The outcome of each data points in cluster are simplified by figuring the inverse operating in head of the cluster. In this situation the head of the cluster may not recognize the addresses of received aggregated information. The secrecy of each node is not confirmed on data and identity, even every sensor node use many algorithms to achieve encryption/decryption and arithmetic operations; this leads to high cost for computation overload and longest delay time.

B. SMART:Slice-mixed aggregation SMART[8] is an additive slice based aggregation protocol that is compromised with the protection for every data sensed either in tree topology or cluster topology. It consists three operations: slicing, mixing and aggregation. every data point divides its data to M pieces; here M is the number of adjacent nodes that can be chosen randomly. Each cluster node may reserve one piece of data; the remaining M-1 pieces are encrypted using shared key and send it to all adjacent nodes[9]. Each sensor performs some aggregation.one slice conveys the outcome to next and he sensors in the middle convey the gathered information to it base terminal.

C. **RPDA: RPDA**[10] **means Rotation-based Privacy-preserving Data Aggregation:** The network that is structured with the sensors is segregated into disjoint cluster that are constituted with the head and members . a random number protect the data sensed[11] circulates the data that is mixed with the other members. This process enables all the members to hide their data under the mixed data until the head is reached. Accumulated results are gained by the head by subtracting the random number [6] and the outcomes are stored in the head that conveys it to its parent node. At last the intermediate outcomes are accumulated and conveyed to sink. The method offers, considerable delay and less overhead compared to CPDA and SMART.

In general based on the survey and study of the above privacy preserving techniques[12] we notifies the following comparison between that techniques

Metrices	**CPDA**	**SMART**	**RPDA**
Structure	**Cluster Based**	**Tree Based**	**Cluster Based**
Accuracy	**High**	**High**	**High**
Overhead	**High**	**Medium**	**Low**
Time Delay	**High**	**High**	**Medium**
Effectiveness	**Low**	**Low**	**Low**

TABLE I: Comparison Table

4. CONCLUSION

preserving of privacy is a challenging research area in WSNs specifically the field of medical applications, home applications, where hackers are use public eavesdropping technique for breaking the sensitive information. the paper elaborates the comparison of existing privacy preservation among various data aggregation techniques in networks conceived using the wireless sensors. Here protocols that relies on context are overviewed. We aim, in the next level, to create the implementation of this work for a thorough analysis and future enhancement. As my future work, we plan to design an efficient new protocol or approach with high privacy preservation for sensitive data.

5. REFERENCES

[1] T. Wang, X. Qin, and L. Liu, "An energy-efficient and scalable secure data aggregation for wireless sensor networks," *Int. J. Distrib. Sens. Networks*, vol. 2013, 2013.

[2] A. Alami, L. Benhlima, and S. Bah, "An overview of privacy preserving techniques in smart home Wireless Sensor Networks," *2015 10th Int. Conf. Intell. Syst. Theor. Appl. SITA 2015*, 2015.

[3] V. I Puranikmath, S. S Harakannanavar, S. Kumar, and D. Torse, "Comprehensive Study of Data Aggregation Models, Challenges and Security Issues in Wireless Sensor Networks," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 3, pp. 30–39, 2019.

[4] R. Soosahabi, M. Naraghi-Pour, D. Perkins, and M. A. Bayoumi, "Optimal probabilistic encryption for secure detection in wireless sensor networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 3, pp. 375–385, 2014.

[5] S. Hu, L. Liu, L. Fang, F. Zhou, and R. Ye, "A Novel Energy-Efficient and Privacy-Preserving Data Aggregation for WSNs," *IEEE Access*, vol. 8, no. 1, pp. 802–813, 2020.

[6] S. Boubiche, D. E. Boubiche, A. Bilami, and H. Toral-Cruz, "An outline of data aggregation security in heterogeneous wireless sensor networks," *Sensors (Switzerland)*, vol. 16, no. 4, 2016.

[7] P. B. Gaikwad and M. R. Dhage, "Survey on secure data aggregation in wireless sensor networks," *Proc. - 1st Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2015*.

[8] C. Li and Y. Liu, "ESMART : Energy-Efficient Slice-Mix-Aggregate for Wireless Sensor Network," vol. 2013, 2013.

[9] P. Yang, Z. Cao, X. Dong, and T. A. Zia, "An efficient privacy preserving data aggregation scheme with constant

communication overheads for wireless sensor networks," *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1205–1207, 2011.

[10] X. Zhang, H. Chen, K. Wang, H. Peng, Y. Fan, and D. Li, "Rotation-based privacy-preserving data aggregation in wireless sensor networks," *2014 IEEE Int. Conf. Commun. ICC 2014*, pp. 4184–4189, 2014.

[11] A. Latha, S. Prasanna, S. Hemalatha, and B. Sivakumar, "A harmonized trust assisted energy efficient data aggregation scheme for distributed sensor networks," *Cogn. Syst. Res.*, vol. 56, no. March, pp. 14–22, 201.

[12] N. John and A. Jyotsna, "A Survey on Energy Efficient Tree-Based Data Aggregation Techniques in Wireless Sensor Networks," *Proc. Int. Conf. Inven. Res. Comput. Appl. ICIRCA 2018*.