International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V67I4P119
Volume 67 Issue 4, 85-90, April 2019

Original Article

Survey on Wireless Sensor Network

Syeda Jabben Fathima[1]

Student, M.Tech. 4th Sem, P.G. Dept. Information. Science. & Engineering, AIT, Bangalore, Karnataka, India

Abstract *- There are several applications for wireless sensor networks it has assured exceptional features. Data aggregation mainly deals with data gathering and aggregates the data in an energy-efficient way to improve the network lifetime. Data transmission in WSN is based on a cluster-based method. In this method, the respective node transfers the data to the cluster head and cluster head combination and transfers it to the base station. WSN has applications in vital areas. Therefore security is very important.*
Wireless sensor network has numerous applications as it has positive, unique features. WSN has several applications in following and observing the background. It includes distributed sensor nodes where location plays and key role in collecting information. The sensor nodes collect the information and transmission it to the base station. The key concern in WSN is energy utilization in transmitting data information. To overwhelm this difficult data aggregation technique was applied. Data aggregation primarily deals with data information collecting and combinations of the data information in an energy-effective way to improve the network lifespan.

Keywords *- Wireless Sensor Network, Data Aggregation, MAC, Performance, Sensor Nodes*

I. INTRODUCTION

Wireless Sensor Network(WSN) has acquired a comprehensive variety of applications in numerous fields in the latest years because of its flexibility, power, and minimal-cost features in data collecting and little range wireless communication. The sensor network contains sensor nodes organized in the geographical area to be experiential for observing the environment.

A wireless network involves a set of distributed sensor nodes that observe and record environmental or physical conditions, such as pressure, wind, sound, and temperature at different geographical areas. In a network, each sensor nodes are little cost-effective power effective, with a transceiver and partial storage. The location of sensor nodes doesn't need to be prearranged. Some sensor nodes are prearranged. They are haphazardly located in a distant area that is to be observed.

II. DEFINITION

Wireless Sensor Network is an energy-consuming Network. Since most of the energy is used for transmitting and receiving data, a mechanism to save energy plays an important role. One of the important mechanisms to reduce energy consumption in WSN is data aggregation. Data aggregation refers to gathering and representing data in a summary form. It can effectively reduce the data size, resulting in significant energy reduction and efficient power utilization in transmitting and receiving data.

III. PURPOSE

Data aggregation aims to eliminate redundant information transmission to improve sensor nodes' energy consumption and reduce communication overheads to increase the quality of service. The clustering approach is introduced where the cluster head gathers the whole data from nodes and transfers aggregated packages to the base station. Aggregation causes load on the cluster head and affects the efficiency and reliability of the network. The data collection approach needs to be protected to avoid any attacks.

IV. FEATURES

The WSN has many features most of the features help in real-life applications. In a large network often, thousands of sensor nodes are available. An asymmetric flow of information is carried out from sensor nodes to command nodes.

Events trigger connections. For every node, there is a restricted amount of energy. Each node is of less cost. The security is limited compared to traditional wireless networks.

V. LITERATURE SURVEY

Mohammad Allah bakhsh, Aleksandar Ignjatovic[1] "An iterative method for calculating robust rating scores" Online rating systems are widely used to facilitate making decisions online. People may try to manipulate such systems for fame or profit by posting unfair evaluations. Therefore, determining objective rating scores of products or services becomes a very important yet difficult problem. Existing solutions are mostly majority-based, employing temporal analysis and clustering techniques. However, they are still vulnerable to sophisticated collaborative attacks. In this paper, we propose an iterative rating algorithm that is very robust against collusion attacks and random and

biased raters. Unlike previous iterative methods, our method is not based on comparing submitted evaluations to approximate the final rating scores. It entirely decouples the credibility assessment of the cast evaluations from the ranking itself.

Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, Sanjay Jha[2] "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks" Due to limited computational power and energy resources, aggregation of data from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging. However, such aggregation is highly vulnerable to node compromising attacks. Since WSN are usually unattended and without tamper-resistant hardware, they are highly susceptible to such attacks. Thus, ascertaining the trustworthiness of data and the reputation of sensor nodes is crucial for WSN. As the performance of very low power processors dramatically improves, future aggregator nodes will be capable of performing more sophisticated data aggregation algorithms, thus making WSN less vulnerable. Iterative filtering algorithms hold great promise for such a purpose. Such algorithms simultaneously aggregate data from multiple sources and provide a trust assessment of these sources, usually in the form of corresponding weight factors assigned to data provided by each source.

Xu Jian, Yang Geng, Chen Zhengyu, Wang Qianqian[3] "A survey on privacy-preserving data aggregation protocols for wireless sensor networks" Wireless sensor networks (WSNs) consist of plenty of sensor nodes with limited power, computation, storage, sensing, and communication capabilities. Data aggregation is a very important technique designed to substantially reduce the communication overhead and energy expenditure of sensor nodes during data collection in WSNs. However, privacy preservation is more challenging, especially in data aggregation, where the aggregators need to perform some aggregation operations on sensing data it received. We present a state-of-the-art survey of privacy-preserving data aggregation in WSNs. At first, classify the existing privacy-preserving data aggregation schemes into different categories by the core privacy-preserving techniques used in each scheme. And then compare and contrast different algorithms based on performance measures such as the privacy protection ability, communication consumption, power consumption, data accuracy, etc.

Vimal Kumar, Sanjay Madria[4] "Pip: Privacy and integrity preserving data aggregation in wireless sensor networks" With the exponential rise of pervasive computing applications, data privacy has become much more important. When data is aggregated at each hop in a sensor network, it becomes harder to protect privacy. Several privacy-preserving data aggregation algorithms have recently appeared for wireless sensor networks (WSNs); however, very few of them also address data integrity and privacy. Data privacy and integrity are two contrasting objectives to achieve in general. In privacy preserved data aggregation, it becomes easier for an attacker to inject false data; hence, we suggest that data privacy and integrity should be treated together. This paper presents an energy-efficient, privacy-preserving data aggregation algorithm that also preserves data integrity in WSNs. We analyze the algorithm's security and provide proof of confidentiality and integrity. We enhance this algorithm further to localize the corrupt aggregator to a certain degree.

Qiang Zhou, Geng Yang, Liwen he[5] "An efficient, secure data aggregation based on homomorphic primitives in wireless sensor networks" Data aggregation is an important method to reduce the energy consumption in wireless sensor networks (WSNs); however, it suffers from the security problems of data privacy and integrity. Existing solutions either have large communication and computation overheads or only produce inaccurate results. This paper proposes a novel secure data aggregation scheme based on homomorphic primitives in WSNs (abbreviated as SDA-HP). The scheme adopts symmetric-key homomorphic encryption to protect data privacy and combines it with homomorphic MAC to check the aggregation data integrity.

VI. IMPLEMENTATION

A. Architecture Diagram

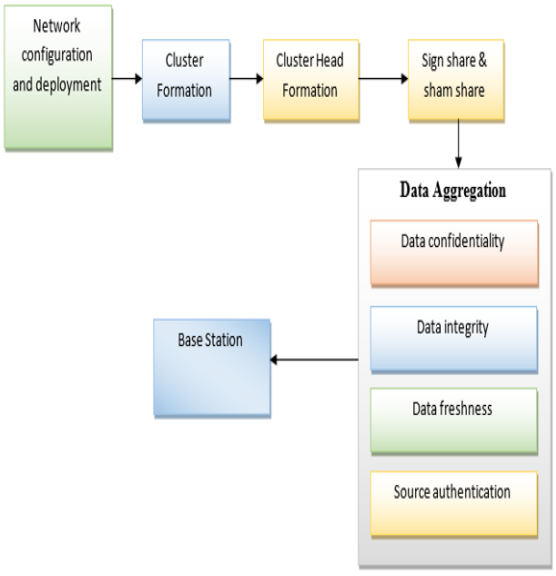

Fig. 1 Architecture Diagram

Below mentioned are implementations and execution modules used and, for implementation, some security measures.

B. Network Deployment

To begin with, characterize the Network setup parameters, i.e., indicate the number of hubs, beginning vitality, MAC, engendering, Receiver control, rest control, transmission control, Channel Type, Propagation or TwoRayGround, i.e., radio-proliferation show, arrange interface (Phy/Wireless Phy), MAC type(Mac/802_11), interface line type(CMUPriQueue), connect layer sort, reception apparatus demonstrate (Antenna/OmniAntenna), max packet in ifq, number of portable hubs, X pivot separate, Y hub remove Initial Energy, Initial vitality in Joules. At that point, convey every one of the hubs into the system with some moving speed. The system stack for a portable hub comprises a connection layer (LL), an ARP module associated with LL, an interface need line (IFq), a macintosh layer (MAC), and a system interface (netIF), all associated with the channel. These system segments are made and plumbed together in OTcl. The pertinent Mobile Node technique includes interface ().

- Create the occurrence for the superclass Simulator and utilize this reference variable to make and indicate the parameters for the hub.
- Create the name petition for summoning the nam window with the set charge and opening the nam record in the compose mode. For this document, the reference variable gives the order ns-Nam trace-all.
- Creating the topology with set topo charge and indicating the kind of the topology as flat grid and determining x value and system.
- Configuring the hubs by determining the estimations of the system parameters.
- Creating the hubs utilizing the for circle and "$ns-hub" order.
- Assign the positions for every one of the hubs with the setdest order and x value, y value
- Attach u dp specialist to the hub.
- Attach the CBR activity from source to sink by setting the bundle estimate and parcel interim.
- Connect the specialists

1. Link Layer

The main distinction is that the connection layer for the portable hub has an ARP module that settles all IP to equipment (Mac) address transformations. Ordinarily, for all friendly (into the channel) bundles, the parcels are passed on to the LL by the Routing Agent. The LL passes on bundles to the interface line. The macintosh layer hands up parcels to the LL for every approaching bundle, which is then given off at the node_entry_ point.

ARP: The Address Resolution Protocol (executed in BSD style) module gets inquiries from the Link layer. On the off chance that ARP has the equipment address for the goal, it composes it into the macintosh header of the parcel. Else it communicates an ARP question and stores the bundle incidentally. There is support for a solitary parcel for every obscure goal equipment address. If extra bundles to a similar goal are sent to ARP, the prior cushioned parcel is dropped. Once 151, the equipment address of a bundle's next jump is known, and the parcel is embedded into the interface line.

2. Interface Queue

The class PriQueue is executed as a need line which offers the need to direct convention bundles, embeddings them at the leader of the line. It underpins running an overall channel parcel in the line and evacuates those with a predefined goal address.

3. Mac Layer

ns-2 has utilized IEEE 802.11 conveyed coordination work (DCF) from CMU. Beginning with ns-2.33, a few 802.11 executions are accessible.

4. Tap Agents

Operators that subclass themselves as class Tap characterized in mach can enroll themselves with the macintosh question utilizing technique install Tap (). If the specific Mac convention grants it, the tap will indiscriminately be given all parcels gotten by the macintosh layer before address sifting is finished.

5. Network Interfaces

The Network Interphase layer fills in as an equipment interface utilized by the versatile hub to get to the channel. The remote shared media interface is executed as class Phy/Wireless Phy. This interface is subject to crashes, and the radio spread model gets bundles transmitted by other hub interfaces to the channel. The interface stamps each transmitted parcel with the meta-information identified with the transmitting interface, like the transmission control, wavelength, etc. The proliferation utilizes this meta-information in the packet header demonstrated in getting the system interface to decide whether the bundle has the least energy to be gotten or potentially caught or distinguished (transporter sense) by the accepting hub. The model approximates the DSSS radio interface.

C. Radio Propagation Model

It utilizes Friss-space weakening (1/r2) at close separations and a guess to two beams Ground (1/r4) at far separations. The estimate accepts specular reflection of a level ground plane. See ~ns/two rays ground. {cc,h} for execution. Receiving wire, an Omni-directional reception apparatus having solidarity pick up, is utilized by versatile hubs.

D. Cluster Formation

In cluster formation, every node group is formed together and arranged in one group. The main purpose of cluster formation is to reduce the Transfer

Rate and allocation of the group into subgroups, and finally, one leader will be selected.
For the Selection of the Group, various methods will be used.

1) My favorite method is Finding the nearby neighbors and joining the group.
2) Per group can have any number of nodes but mostly?
3) In cluster formation, many groups can be made inside a cluster can also be made
4) Like tree structure also be made to reduce the level so reduce the traffic
5) These cluster formations many research is made I am also doing certain research and formed particular cluster formations with my algorithm along with existing and obtain a new one.
6) Since it is a combination of two members, i cannot post the algorithm on my Blog.

Sign Phase

In the Sign-Share approach, each sensor node splits its data into multiple shares and sends some of them to the aggregators of its cluster, allowing the encoding of each share with simpler codes. For ease of description, we assume that the data sensed by each sensor each time is 32-bits long, and the 32-bit data is split into four 8-bit shares.

The sign-Share approach consists of the following phases:

Setup Phase: The following system parameters are generated and loaded into each sensor node at the design stage.

- The larger the P, the more secure the aggregations.
- A secret 32-bit pseudo-random binary sequence generator PRBSp[I; n], where I am the seed and n is the clock.

Secret Sharing: Signature Phase: When a senor node vi senses the physical environment and prepares its data D to be sent to its aggregators, it does the following:
Each sensor vi splits its data as follows:
1) Encode the data: D0 = D_PRBSp[I; n], where is the bitwise XOR.
2) Split the encoded data into 4 B0, B1, B2, and B3 shares.
3) Encode each byte Bk using the key-set K

Aggregation Phase: When an aggregator node receives the tuple from every member of its cluster, it does the following:
Let (B00; _0); (B01; _1); _ _ _ ; (B0w□1; _w□1) be all the tuples received.

Verification-Decoding Phase: When the base station receives the data from every aggregator AGi, it does the following:

- Let w be the number of shares received from AGi.
- Extract the Q bytes of each tuple received from AGi.
- Recover the 32-bit data of each node vi as follows:

1) Decode each byte using the key-set K of vi:
Bk = ((B0k□ _k) _ _□1k) mod256 (6)
2) Merge the decoded bytes into one 32-bit integer D0.
3) Decipher the data: D = D0 _ PRBSp[I; n].
Verify D by using Boneh et al. algorithm [13].

Shame Share

In Sham-Share approach consists of the following phases:

Setup Phase: The base station generates the following key pair (puvi; prvi) for each sensor node vi as in, where puvi is the public key kept in the base station, and prvi is the private key loaded to each sensor node vi along with H, the hash function for all the sensor nodes.

Secret Sharing-Signature Phase: When a senor node vi senses the physical environment and prepares its data S to be sent to its aggregators, it performs the following tasks:
The sensor node vi splits the data S into 4 shares as follows:
1) Generate two random numbers, a0; a1.
2) Construct the following polynomial function:
f(x) = S + a0x + a1x2 (7)
3) Construct 4 shares with each share represented by a pair (x; f(x))(x = 1; 2; 3; 4). Shares start from (1; f (1)) because f (0) is the data S.
4) Let IDi be the ID of the sensor node vi. Encode each share of vi as follows:
Qi = x + 10IDi + 1000f(x).

- Send the tuples (Q1; _1), (Q2; _2) to one aggregator, and (Q3; _3), (Q4; _4) to the other aggregator.

Aggregation Phase: After an aggregator, AGi receives the tuple from every member of its cluster, it performs the following tasks:

- The aggregator gathers all the w tuples (Q0; _0), (Q1; _1), :::; (Qw□1; _w□1) from the members of its cluster.
- Send the data in an array which contains the aggregated signature and the aggregated shares.

Reconstruction-Verification Phase: After the base station receives the data from all the aggregators, it performs the following tasks for each aggregator AGi:

- Let w be the number of shares received from AGi.
- Disaggregate Qi of each array received from AGi as follows:
- Gather 3 shares of each sensor node vi, and reconstruct its data S.

E. Data Aggregation

In the mill remote sensor systems, sensor hubs are generally asset compelled and battery-restricted. To spare assets and vitality, information must be amassed to abstain from overpowering movement measures in the system. There has been broad work on information total plans in sensor systems. The point of information total is that it kills repetitive information transmission and upgrades the lifetime of vitality in remote sensor organization. Information conglomeration is the procedure of one or a few sensors that then gathers the discovery result from another sensor. The sensor must handle the gathered information to diminish transmission trouble before they are transmitted to the base station or sink. The remote sensor organization has comprised three sorts of hubs: Simple normal sensor hubs, aggregator hub, and questions.

F. Performance Analysis

In this mathematical operations are performed based on the above all the operations then result will be stored into the x graphs.

G. Enhancement

While significantly more robust against collusion attacks than the simple averaging methods, several existing iterative filtering algorithms are nevertheless susceptive to a novel, sophisticated collusion attack we introduce. To address this security issue, we propose an improvement for iterative filtering techniques by providing an initial approximation for such algorithms, which makes them not only collusion robust, but also more accurate and faster converging.

By providing an initial trust estimate based on a robust estimation of errors of individual sensors. When the nature of errors is stochastic, such errors essentially represent an approximation of the error parameters of sensor nodes in WSN, such as bias and variance. To prove robust in cases when the error is not stochastic due to coordinated malicious activities.

VII. RESULTS AND SNAPSHOTS

The designed framework's simulation area and performance development concerning output, packet delay, overhead, and energy consumption. These snapshots are mentioned below.

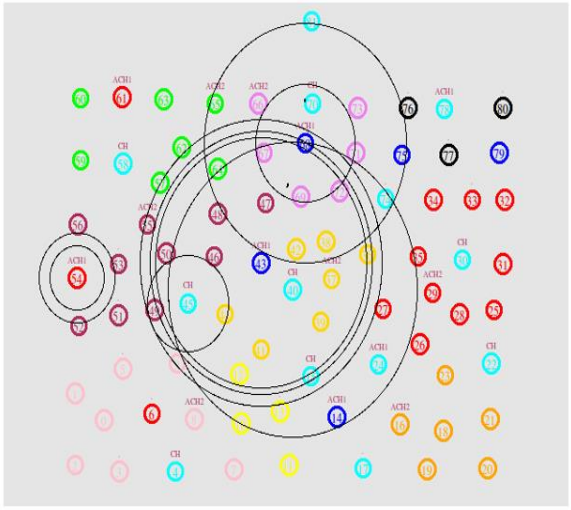

Fig. 2 Output

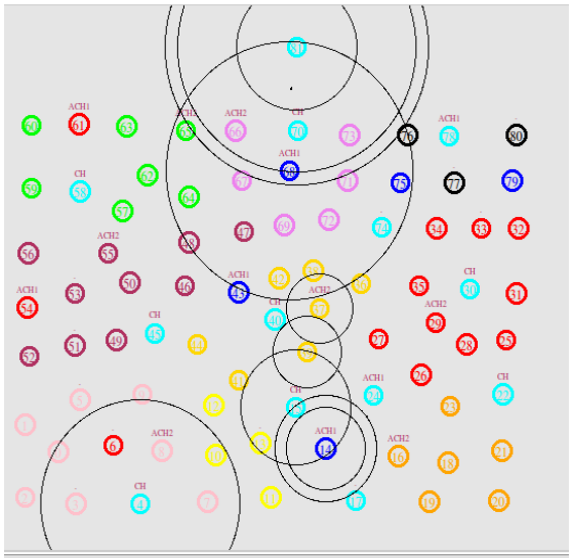

Fig. 3 Output

VIII. CONCLUSION

The author proposed two reliable and secure end-to-end data aggregation approaches that conceal the sensed data and allow the base station to detect selective forwarding and modification attacks. The simulation results show that both of our approaches perform better than PIP and RCDA-HOMO in aggregation processing time and sensor processing time. They perform significantly better than PIP in terms of network lifetime, network delay, and aggregation energy consumption.

REFERENCES

[1] M. Allahbakhsh and A. Ignjatovic, “An iterative method for calculating robust rating scores," Parallel and Distributed Systems, IEEE Transactions on, vol. 26, no. 2, pp. 340–350, 2015.

[2] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, “Secure data aggrega- tion technique for wireless sensor networks in the presence of collusion attacks,” Dependable and Secure Computing, IEEE Transactions on, vol. 12, no. 1, pp. 98–110, 2015.

[3] Xu Jian, Yang Geng, Chen Zhengyu, Wang Qianqian “A Survey on the Privacy-Preserving Data Aggregation in Wireless Sensor Networks" China Communications, vol. 12, no. 5, pp. 162–170, 2015.

[4] V. Kumar and S. Madria, "Pip: Privacy and integrity preserving data aggregation in wireless sensor networks," in Reliable Distributed Systems (SRDS), 2013 IEEE 32nd International Symposium. IEEE, 2013, pp.10–19.

[5] Q. Zhou, G.Yang, and L.He, "An efficient secure data aggregation based on homomorphic primitives in wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2014, 2014.

[6] C.-M. Chen, Y.-H. Lin, Y.-C. Lin, and H.-M. Sun, "Rcda: recoverable concealed data aggregation for data integrity in wireless sensor net- works," ParallelandDistributedSystems, IEEE Transactions on,vol. 23, no. 4, pp. 727–734, 2012.

[7] Y.-H. Lin, S.-Y. Chang, and H.-M. Sun, “Cdama: concealed data aggre- gation scheme for multiple applications in wireless sensor networks,” Knowledge and Data Engineering, IEEE Transactions on, vol. 25, no.7, pp. 1471–1483,2013.

[8] B. Przydatek, D. Song, and A. Perrig, “Sia: Secure information aggregation in sensor networks,” in Proceedings of the 1st international conference on Embedded networked sensor systems. ACM, 2003, pp. 255–265.

[9] Y. Yang, X. Wang, S. Zhu, and G. Cao, “Sdap: A secure hop-by-hop data aggregation protocol for sensor networks,” ACM Transactions on Information and System Security (TISSEC), vol. 11, no. 4, p. 18, 2008.

[10] E. Mykletun, J. Girao, and D. Westhoff, "Public key based cryp- toschemes for data concealment in wireless sensor networks," in Communications, 2006. ICC'06. IEEE International Conference on, vol. 5. IEEE, 2006, pp.2288–2295.