ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Dynamic Key Based Secure Cluster Head Data Aggregation for Wireless Sensor Network – A Review

Karamjit Kaur

Research Scholar, Dept. of C.S.E., YCoE, Punjabi University, Talwandi Sabo, Bathinda, Punjab, India

ABSTRACT: The network security in wireless that consists of sensors which are distributed in an ad hoc manner. These sensors work with each other to sense some physical phenomenon and then the information gathered is processed to get relevant results. The inevitable issue is that in large sensor networks, the amount of data generated is excessive for the base station to process. So methods like data aggregation are required that combine sensed data into high quality information which precedence to energy conservation by reducing the number of packets transmitted to base station. Thus, an important challenge is how to protect the user's privacy, especially when the aggregator is untrusted. To address these problems, we propose an efficient model, which will use the dynamic key exchange scheme for the highly secure communication between the cluster head and the regional cluster head. This will maximize the security during data aggregation.

KEYWORDS: WSN data aggregation, Pre-Shared key scheme in WSN, Energy efficient data aggregation, Energy efficient WSNs.

I. INTRODUCTION

Mobile Wireless Sensor Network (WSN) consists of various sensor nodes used to sense and store data from the environment. A special node is called the sink, is responsible for querying and collecting the data from the sensor nodes. Sensor nodes cooperate with each other to monitor environmental or physical conditions, such as sound, temperature, image, vibration, pressure, motion or pollutants. Each sensor node is also equipped with a radio transceiver or other wireless communication device, a microprocessor, and energy source (e.g., a battery). The development of WSNs was originally motivated by military and homeland security applications such as battlefield surveillance. However, WSNs are now also widely applied in civilian application areas, including industrial sensing, environment and habitat monitoring, health-care applications, home automation, and traffic control. Communication security is essential to the success of WSN applications, especially for those mission-critical applications working in unattended and even hostile environments. Nowadays, mobile phones' built-in-sensor, so they can also be considered as sensor nodes and no sensor deployment is necessary. As the users move in their day to day life, their devices will sense the environment and collect data. To ensure that the network functions correctly and safely as purposed, the following are four major security requirements for WSNs.

Authenticity: Authenticity enables a sensor to make sure the identities of its communicating entities so that no adversary could masquerade another entity, and disseminate forged messages.
Integrity: Integrity ensures that a message being transferred is never corrupted or modified by an adversary without being detected.
Confidentiality: Confidentiality ensures that the content of the message being transferred is never disclosed to unauthorized entities. Network transmission of sensitive information, such as military information, requires confidentiality.
Availability: Availability ensures the survivability of network services despite denial of service (Dos) attacks.

Data gathering is defined as the systematic collection of sensed data from multiple sensors to be eventually transmitted to the base station forprocessing. Data generated from neighboring sensors is often redundant and highly correlated. So

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

with the help of data aggregation we combine data into high quality information at the sensor or intermediate nodes which can reduce the number of packets transmitted to the base station resulting in conservation of energy and bandwidth.

II. DATA AGGREGATION

In typical wireless sensor networks, data must aggregate to save resources and energy because sensor nodes have limited battery. Data aggregation attempts to collect the most critical data from sensors and make it available to the sink in an energy efficient manner with minimum data latency. Data latency is important in many applications such as environment monitoring factor. Three types of nodes are consisted in wireless sensor network. These are Simple regular sensor nodes, aggregator node and querier. From these nodes Regular sensor nodes sense data packet from the environment and send this data to the aggregator nodes, these aggregator nodes collect data from multiple sensor nodes of the network, using a some aggregation function aggregates the data packet (like sum, max min, average and count) and then sends aggregates result to upper aggregator node or the querier node who generate the query. There are two types approaches are used for in network aggregation. First one is With size reduction and another is without reduction. In size reduction, it is the process in which compressing and combining the data received by a sensor node from its neighbors, in order to reduce the length of data packet to be sent towards the base station. In network aggregation without size reduction, data packets are received by different neighbors into a single data packet but without processing the value of data, which is useful to reduce energy consumption or increase life time of the network.

Performance measure of data aggregation: These performances are highly dependent on the desired application.

- **Energy Efficiency**: By the data-aggregation scheme, we can increase the functionality of the wireless sensor network, in which every node should've spent the same amount of energy in every data gathering round. A data aggregation scheme is energy efficient if it maximizes the functionality of the network.

- **Network lifetime:** It defines the number of data fusion rounds. Till the specified percentage depends on the total nodes dies and the percentage depend on the application.

- **Latency**: Latency is evaluate data of time delay experiences by system, means data send by sensor nodes and received by base station, basically delay involved in data transmission, routing and data aggregation. Communication Overhead: It evaluates the communication complexity of the network fusion algorithm.

- **Data Accuracy**: It evaluates the ratio of total number of reading received at the base station to the total number of generated.

III. LITERATURE REVIEW

A literature review goes beyond the search for information and includes the identification and articulation of relationships between the literature and our field of research. While the form of the literature review may vary with different types of studies, the basic purposes remain constant: **Qinghua*et al*. [1]** which explained how to protect the users' privacy in mobile sensing, especially when the aggregator is untrusted in existing work they do not consider the min aggregate, which is quit useful in mobile sensing. To protect user privacy, they design encryption schemes in which the aggregator can only decrypt the sum of all users' data but nothing else. They defined efficient protocol to obtain the Sum aggregate, which employs an additive homomorphic encryption and a novel key management technique to support large plaintext space & also extend the sum aggregation protocol to obtain the Min aggregate of time-series data.**Qinghua Li*et al.* [2]** which explained a scheme for privacy-preserving aggregation of time-series data in presence of untrusted aggregator, which provides differential privacy for the sum aggregate & a novel ring-based interleaved grouping technique to efficiently deal with dynamic joins and leaves to achieve low aggregation error. Specifically, when a node joins or leaves, only a small number of nodes need to update their cryptographic keys.**Guohong Cao *et al.* [3]** which explained a distributed scheme to detect packet dropping in DTNs (disruption tolerant networks). In this, a node is required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet. Trace-driven simulations show that our solutions are efficient and can effectively mitigate routing misbehavior. **Qinghua Li *et al.* [4]** which explained a Social Selfishness Aware Routing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

(SSAR) algorithm to select an effective forwarding node, SSAR considers both users' willingness to forward and their contact opportunity, and derives a metric with mathematical modelling and machine learning techniques to measure the forwarding capability of the mobile nodes. Trace-driven simulations show that SSAR allows users to maintain selfishness and achieves good routing performance with low transmission cost. **R.N. Wright*et al.* [5]** which proposed a simple cryptographic approach that is efficient even in a many-customer setting, provides strong privacy for each customer, and does not lose any accuracy as the cost of privacy. This method requires no interaction between customers, and each customer only needs to send a single flow of communication to the data miner. To illustrate the power of our approach, we use our frequency mining computation to obtain a privacy- preserving naive Bayes classifier learning algorithm. **D. Song *et al.* [6]** which explained Existing protocols for this private distributed aggregation model suffer from various drawbacks that disqualify them for application in the smart energy grid and they are not fault – tolerant. So they provide a protocol that fixes these problems and furthermore, supports a wider range of exchangeable statistical functions and requires no group key management. A key-managing authority ensures the secure evaluation of authorized functions on fresh data items using logical time and a custom zero-knowledge proof providing differential privacy for an unbounded number of statistics calculations. **A.T. Campbell *et al.* [7]** present: a description and prototype implementation of the system architecture, an evaluation of sensing and inference that quantifies cyclist performance and the cyclist environment; a report on networking performance in an environment characterized by bicycle mobility and human unpredictability; and a description of BikeNet system user interfaces. **K. Nissim *et al.* [8]** which explained a homomorphic public key encryption scheme based on finite groups of Composite order that support a bilinear map, which allow for one multiplication on encrypted values and obtain a system with an additive homomorphism. Homomorphic encryption enables "computing with encrypted data" and is hence a useful tool for secure protocols. Current homomorphic public key systems [20, 13, 28] have limited homomorphic properties: given two cipher texts Encrypt (PK, x) and Encrypt (PK, y), anyone can compute either the sum Encrypt (PK, x+y), or the product Encrypt (PK, xy), but not both. **G. Tsudik *et al.* [9]** which explained we propose a simple and provably secure encryption scheme that allows efficient additive aggregation of encrypted data. Only one modular addition is necessary for cipher text aggregation. The security of the scheme is based on the in distinguish ability property of a pseudorandom function (PRF), a standard cryptographic primitive.**R.N. Wright *et al.* [10]** which explained a simple cryptographic approach that is efficient even in a many-customer setting, provides strong privacy for each customer, and does not lose any accuracy as the cost of privacy. Another key technical contribution is a privacy-preserving method that allows a data miner to compute frequencies of values or tuples of values in the customers' data, without revealing the privacy-sensitive part of the data.

IV. SECURITY ISSUES IN DATA AGGREGATION

Security in data transmission and aggregation is an important issue to be considered while designing sensor networks. In many applications, sensors are deployed in open environments and are susceptible to physical attacks while might compromise the sensor's cryptographic keys. The one of security issue is that the existing system does not offer any method to protect the initial phase of communication, and use static key management method, where the key tables or key chains are not updated dynamically. Another security issue is that the cluster head performs the aggregation task but doesn't perform any data stream analysis before the aggregation, which adds the probability of attacker data being aggregated without any scanning.

V. PROPOSED WORK AND METHODOLOGY

The proposed model will use a pre-shared key based secure initial setup phase with higher level of nodal integrity. This will use the dynamic key exchange scheme for the highly secure communication between the cluster nodes and the cluster head and the regional cluster heads. The cluster head and the regional cluster heads are well connected nodes along with the secure data aggregation methods along with the pre-aggregation analysis to prevent the malicious data from entering the aggregated streams of the data. This research study has included the detailed literature on the data aggregation methods for the wireless sensor networks (WSNs). The literature review has aimed at reading the advantages and shortcomings of the existing models. The general and critical issues of solution design for existing models has been studied in detail in order to know the impact of the various designs or solutions on the data aggregation process. Then, the proposed model has been designed to overcome the shortcomings of the latter solutions

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

while keeping their advantages intact. The proposed model has been designed with keeping the issue of data security in focus. The proposed aggregation data security model has been aimed solving most of the problems reported in the existing studies. The proposed work is based upon the key management model, which has inspired us to study the prominent key management schemes used in various other applications to know their advantages and possibilities of uses in the WSNs, specifically during the aggregation model. Then the solution will be implemented using the appropriate simulation environment with all essential input and output parameters. The simulation environment implementation will be followed by the detailed result analysis conducted on the results collected from the proposed model simulation. Afterwards, the result comparison would be performed on the results collected and analyzed against the shortlisted existing techniques in order to evaluate the performance level of the proposed model.

VII. FUTURE WORK

In the future, we proposed model can be enhanced using high security mechanism like we can encrypt the data along with authentication and second method is that we can use any another mechanism to check the integrity of the user for better security and efficiency.

REFRENCES

1. Q. Li and G. Cao, "Efficient and Privacy-Preserving Data Aggregation in Mobile Sensing," Proc. IEEE, vol.11, no. 2,pp 115-127, 2014.
2. Q. Li and G. Cao, "Efficient Privacy-Preserving Stream Aggregation in Mobile Sensing with Low Aggregation Error," IEEE, 2013.
3. Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.
4. Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," Proc. IEEE INFOCOM, pp. 1-9, 2010.
5. Z. Yang, S Zhong, and R.N. Wright, "Privacy-Preserving Classification of Customer Data without Loss of Accuracy," Proc. Fifth SIAM Int'l Conf. Data Mining (SDM '05), pp. 21-23, 2005.
6. T.-H.H. Chan, E. Shi, and D. Song, "Privacy-Preserving Stream Aggregation with Fault Tolerance," Proc. Sixth Int'l Conf. Financial Cryptography and Data Security (FC '12), 2012.
7. S.B. Eisenman, E. Miluzzo, N.D. Lane, R.A. Peterson, G.-S. Ahn, and A.T. Campbell, "The Bikenet Mobile Sensing System for Cyclist Experience Mapping," Proc. ACM Fifth Int'l Conf. Embedded Networked Sensor Systems (SenSys '07), pp. 87-101, 2007.
8. D. Bonet, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF Formulas on Ciphertexts," Proc. Second Int'l Conf. Theory of Cryptography (TCC'05), 2005.
9. C. Castelluccia, A.C.-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks," ACM Trans. Sensor Networks, vol. 5,no. 3, pp. 20:1-20:36, 2009.17
10. Z. Yang, S. Zhong, and R.N. Wright, "Privacy-Preserving Classification of Customer Data without Loss of Accuracy," Proc. Fifth SIAM Int'l Conf. Data Mining (SDM '05), pp. 21-23, 2005.