IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 4 (April. 2013), ||V4 || PP 43-46

Secure Data Accumulation and Certification Procedure for Sensor Networks

Kuttyamma A.J [1],Chinchu Krishna.S [2]
Professor & HOD, Department of Information Technology, Rajagiri School of Engineering and Technology, Cochin, Kerala, India
Assistant Professor ,Department of Information Technology, Rajagiri School of Engineering and Technology, Cochin, Kerala, India

Abstract: The Wireless Sensor Network appears as an emerging technology which consists of thousands of small and low cost sensors. These sensors have limited power, computation, storage and communication capabilities. The data aggregation framework process is required which combines the data coming from various sensors, remove the redundancies in those data and then enroot them. In this paper, we have proposed a secure data aggregation protocol for wireless sensor networks (WSNs) that is robust to deceitful nodes. The goal of this protocol is to guarantee the essential security needs (like authentication, data confidentiality & data integrity) as well as to achieve the low communication overhead and be fitted with various aggregation functions (like sum, average, max, min etc.).To achieve these security needs, it uses symmetric encryption and message authentication code. Encryption ensures data confidentiality while message authentication code ensures authentication and data integrity. An anomaly detection algorithm is used to detect the anomaly or outliers and thus prevent the deceitful corrupted data from being contributed to the final aggregated results.

Keywords: *Wireless Sensor Network,Data aggregation.*

I. INTRODUCTION

A wireless sensor network (WSN) is collection of a large number of sensor nodes that have limited computation, communication and power resources. Due to the limited resources, the amount of data transmission should be minimized such that the lifetime of the sensor nodes and bandwidth utilization of the network can be improved. Due to this, the concept of data aggregation is come into the final picture. Data aggregation is the data process of combining the data coming from various sources and enroute them after removing redundancy such as to improve the overall networks lifetime [1]. The in-network frame processing is done on the aggregator node. The aggregator node aggregate the data received from its child node as per the required aggregation function (like min, max, average, sum etc.) and send the other high level aggregated node or sink. But in hostile environment these aggregated result should be protected from the various type of the attacks in order to achieves data confidentiality, data integrity and source authentication. So security is necessary to be employed with data aggregation. Recently various data aggregation protocols [2,3] have been proposed to remove the redundancy in the transmitted data so as to decrease to the amount of data transmission which saves a considerable amount of energy and bandwidth. But, these protocols do not provide the security means to the aggregated data. In many situations, it is necessary to rotect the aggregated data from various types of attacks. In this paper, we have proposed a secure data aggregation protocol that achieves the security requirements of the aggregated data.

II. RRELATED WORK

Secure data aggregation in wireless sensor networks in many applications, the physical phenomenon is sensed by sensor nodes and then reported to the base station. To reduce the energy consumption of the sensor nodes, these applications may employ in-network aggregation before the data reaches the base station. Compromised nodes can thus perform malicious activities which affect the aggregation results. The security requirements of WSNs is required to strengthen attack resistant data aggregation protocols. In Secure DAV[4], cluster key establishment (CKE) protocol is used to establish the secret cluster keys in the WSN. These secret cluster keys are used for the partial signature generation on the aggregated data. Elliptic Curve Cryptography (ECC) is used for the secure key management because it has smaller key size and faster computation. After that, a Secure DAV protocol is used which guarantees that the sink does not accept the altered data for an upper bound of t compromised sensor within a cluster where $t < n/2$ where n is the number of nodes in the cluster. Cluster head then generates the full signature after combining partial signatures from all the sensors within the cluster and then sends this full signature along with the average reading to the sink. Sink having possession of public key then verifies this signature. Merkle Hash tree is used to check the integrity of the sensor node's readings. Secure DAV can be applied only to average aggregation function and have a high communication overhead.

In [8], the author presents a mechanism to find out the misbehaving nodes. In this protocol, sensed data is not aggregated at the immediate next hope rather it is aggregated on the second hop. This protocol guaranties data integrity and source authentication but it does not provides the source data confidentiality. In [5], cryptographic operation is required only when any cheating activity is detected. A secure aggregation tree (SAT) is built with the topological constraint for the detection and prevention for cheating. The SAT is built in such a way that the child is able to listen all the incoming data from its sibling to its father so that the child node can observe the behavior of its father, then the cheating activity of any non-leaf (aggregator) source node can be detected. If the aggregated result from an aggregator is uncertain then a weighted voting scheme is introduced for taking the final fit decision about whether the aggregator node is cheating. If cheater aggregator node is found then a local recovery scheme is employed which rebuild the SAT such that the cheater node is removed from the tree. It does not provide data confidentiality.
In SELDA [9], to develop trustworthiness for the environments and neighboring nodes, action of the neighboring nodes are observed by the sensor nodes. Aggregators consider sensor node's reading received using the web of trust to enhance the reliability of aggregated data. If any aggregator is under the denial of- service attack, then it can be detected using the monitoring mechanism. It ensures data integrity and source authentication but it does not provide data confidentiality.

- Security needs of Wireless Sensor Network In hostile environment security is an important issue for the wireless sensor network. There are several security needs of wireless sensor networks that are discussed below:-
- Data confidentiality Data confidentiality is the protection of transmitted data from passive attacks. In wireless sensor network, the transmitted data should not be disclosed to an unauthorized user which is a challenging task. So information should be sent in encrypted form to preserve its secrecy. So encryption should be done by the secret key such that the intended party that has possess this key could open and read this data.
- Data integrity Data integrity ensures that the transmitted data has not been tempered either by the spiteful node or by any accident during the transmission. It means it ensures that the data are received as sent, with no duplication, insertion, modification, reordering.
- Data freshness Data freshness ensures that the transmitted data is fresh and not long past data has been used for the replay attack. So data freshness provides safety for the transmitted data from repay attack.
- Source Authentication Source authentication allows a receiver to verify that the data is truly sent by the claimed sender. An attacker without having source authentication can false show as like a node and gain the unauthorized access to the resources and secret information of that node to disrupt the normal operation of the network. So to prevent Sybil attack, source authentication is required. In this attack, an attacker captures a node and gain access over the secret information stored in that node. Thus node compromise attack can influences the data aggregation results.
- Efficiency The goal of data aggregation is to reduce the number of messages transmitted within the sensor network, thus reduce resource and power usage. Data aggregation achieves bandwidth efficiency by using in network processing. In private data aggregation schemes, additional overhead is introduced to protect privacy. However, a good private data aggregation scheme should keep that overhead as small as possible.
- Accuracy An accurate aggregation of sensor data is desired, with the constraint that no other sensors should know the exact value of any individual sensor. Accuracy should be a criterion to estimate the performance of private data aggregation schemes.
- Data Availability Ensures that the network is alive and that data are accessible. It is highly recommended in the presence of compromised nodes to achieve the network degradation by eliminating these bad nodes. Once an attacker gets into the WSN by compromising a node, the attack will affect the network services and data availability especially in those parts of the network where the attack has been launched. Moreover, the data aggregation security requirements should be carefully implemented to avoid extra energy consumption.

III. SYSTEM MODEL

A. Assumptions

Here we make following assumptions:

- WSN consisting of a large number of resource constraint sensor nodes.
- There exists a powerful fixed base station (BS).
- The clusters are static i.e. are formed the start of the network.
- Cluster heads (CHs) work as an aggregator.
- All sensor nodes are immobile.

B. Network Model

Figure 1shows the network model used. Various symbols and terms used are shown in Table I. All sensor nodes are immobile. Links between the two sensor nodes is considered bidirectional. There is only single channel for communication between sensor nodes.

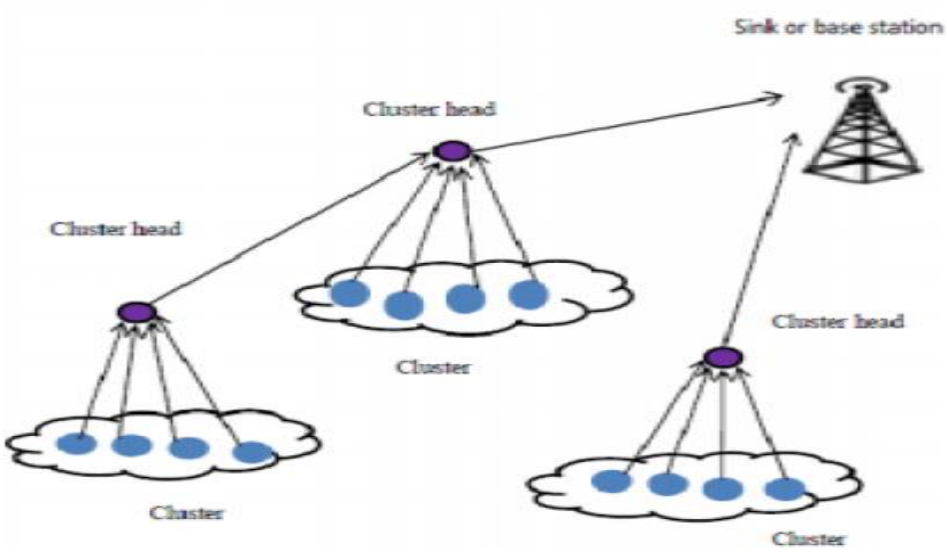

Figure 1. Network Model

Ch_{id}	ID Of The Cluster Head	E	Encryption
$\|CH_i\|$	ID Of Cluster Head In Cluster I	$K_{\{BS,u\}enc}$	Shared Pair Wise Key Between Base Station And Sensor Node U Used For Encryption
Q	Query	f_{ag}	Aggregation Function
|	Concatenation	U_{id}	ID Of The Sensor Node u
R	Random Number	MAC	Message Authentication Code
U	Regular Sensor Nodes	$K_{\{BS,u\}MAC}$	Key Used To Calculate MAC By Base Station
R_u	Reading Of Sensor Node u	CH_c	Child Cluster Head
CH	Cluster Head	CH_p	Parent Cluster Head
BS	Base Station		
Agr	Aggregation Reading		

Table 1: Notations used in this table

IV. PROPOSED PROTOCOL

Base station (BS) starts the sensing process determine by sending a broadcast message to those sensor nodes which are located in the area of interest. For authenticated broadcast of query, we have used with some modifications[6]. Sensor nodes then report back with their readings to the base station through aggregator. Aggregator then processes the received readings of sensors. In addition to aggregation process, it also identifies the anomaly or outlier sensor nodes by using anomaly detection algorithm [7].It then reports back to the next level aggregator or BS with aggregated reading, outlier count & outlier sensor's ids

A. Query Dissemination

In process of query dissemination from BS to the network, sensor should have the required knowledge about aggregation function which is used for the aggregation of sensor's readings. Every sensor nodes have their distinct private key shared with the BS which is computed by taking hash on the master key of BS (KB) with their respective ids. In ddition to this, each sensor node shares pair wise key with their children these which is used for encryption. The format of node query packet sent by BS to the aggregator looks as follows:

BS □ u:E(K{BS ,u}enc . fag |q|r|BS) MAC(K{BS,u}MAC . fag |q|r|BS)

B. Transmission of sensor nodes reading to the BS

Transmission of sensor nodes readings to the base station can be done in three phase: Sensor node to cluster head, child cluster head to parent cluster head, and cluster head to base station.

- Sensor nodes to clusters head Sensor nodes send their readings to their cluster head. The packet sent by the sensor nodes to the cluster head includes ids of the sensor nodes, result readings, random number. The packet format transmitted by sensor node to cluster head is like: u ->CH:E(K {u,ch}enc. Ru|r|uid) | MAC(K{u}Mac(K{u}MAC. Ru|r|uid)

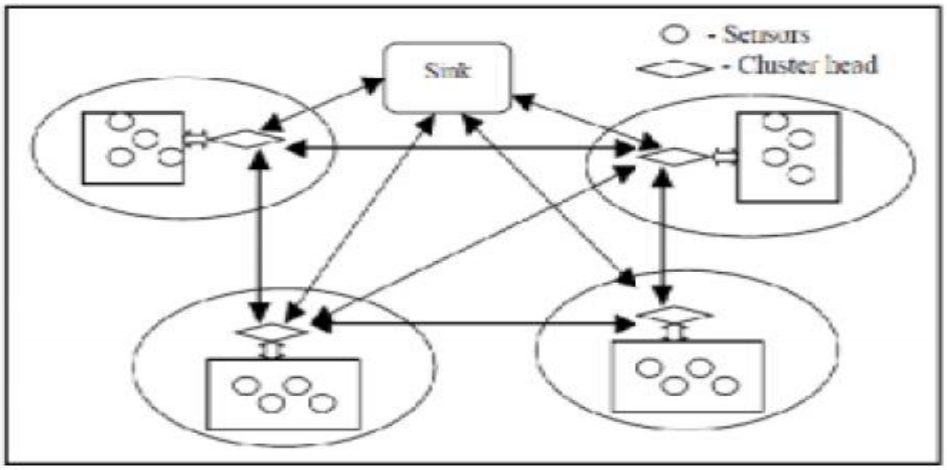

Figure 2: Cluster based sensor network. The arrows indicate wireless communication links.

- Child cluster head to parent cluster head Upon the reception of readings from its cluster members, cluster head performs the anomaly detection algorithm. Thus, it finds the outlier and drops the readings of outliers. Cluster head then aggregates the readings and sends the aggregated reading along with outlier ids, outlier count to the parent cluster head. The packet format sent by the child cluster head to the parent cluster head is like: CHc CH:E(K {CHc CHp}..Agr|r|CHid|outlier count |outlier ids)|MAC(K{CHC}MACAgr|r|CHcid|outlier count|outlier ids)
- Cluster head to base station When cluster head receives readings from all of its children, it first runs anomaly detection algorithm to filter out the anomaly or outlier readings. After that it aggregates the readings of its children nodes according to the specified aggregation functions in the query packet and then it finally sends the aggregated readings with outlier ids and count to the base station. The packet format sent by cluster head to base station.

V. CONCLUSION

This proposed approach is based on detection and filtration of deceitful sensor source nodes with their sensed readings in wireless sensor networks. It uses outlier detection algorithm to detect and filter out the outlier sensor nodes. And it is provides high outlier detection rate due to the use of the distributed approach. It uses MAC for data authentication and data integrity. In order to provide confidentiality, it uses symmetric encryption. It uses the pair wise shared key for the purpose of encryption. The proposed approach is achieves high outlier detection rate, accuracy improvement rate and the average of total transmission energy consumed per node.

REFERENCES

[1]. Mahimkar, T.S. Rappaport , "Secure DAV: a secure data aggregation and verification protocol for wireless sensor networks",In Proceedings of the 47th IEEE Global Telecommunications Conference on (Globecom), November 29–December 3,Dallas, TX,2004.

[2]. Perrig, R. Szwezyk, A. Woo, S. Hollar , D . Culler , and J. Tygar, "SPINS: security protocols for sensor networks," in mobile computing and networking, 2001,pp.189-199.

[3]. C. Intanagonwiwat, R. Govindan, D. Estrin , J. Heidemann , F. silva , "Directed diffusion for wireless sensor networking," in : proceeding of IEEE/ACM Transactions on Networking, Vol.11, 2003, pp. 2-16.

[4]. K. Wu, D. Dreef, B. Sun, Y. Xiao,Secure data aggregation without persistent cryptographic operations in wireless sensor networks, AdHoc Networks 5 (1) (2007) 100–111.

[5]. L. Hu, D. Evans, Secure aggregation for wireless networks, in:Proceedings of the Workshop on security and Assurance in Ad Hoc Networks, Orlando, FL, 28 January 2003.

[6]. Suat Ozdemir, Yang Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview", Computer Networks,vol. 53, Elsevier, pp. 2022–2037, 2009

[7]. S. Pattem, B. Krishnamachari, R. Govindan , The Impact of Spatial Correlation on the Routing with Compression in the Wireless Sensor Networks, On ACM/IEEE IPSN04, Berkeley, CA, 2004.

[8]. S. Rajasegarar, C. Leckie, M. Palaniswami , James C. Bezdek,et al. "Distributed anomaly detection in wireless sensor network," in the proceeding of IEEE conference on mobile computing and networking, USA, 2006