International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 10, December- 2012

A Privacy Data Aggregation for Data Integrity in Wireless Sensor Network

Mano Chithra. N
II M.E, Computer Science and Engineering, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India

Hemal Babu. H
Assistant Professor, Department of Computer Science and Engineering, Sri Shakthi Institute of Engineering and Technology, Coimbatore,India

Abstract

A fundamental challenge in the design of wireless sensor networks (WSNs) is to maximize their lifetimes. Since many sensors have correlated readings, data aggregation has emerged as an efficient approach to reduce the number of transmissions, and hence minimize overall power consumption in the network. An important aspect of data aggregation is the placement of aggregation points and how aggregated data is routed to the gathering points. In existing work, they have introduced a concept named Recoverable Concealed Data Aggregation (RCDA). In RCDA, a base station can recover each sensing data generated by all sensors even if these data have been aggregated by cluster heads (aggregators).In this design, the base station can recover all sensing data even these data has been aggregated which properties is called "recoverable." With these individual data, two functionalities are provided. First, the base station can verify the integrity and authenticity of all sensing data. Second, the base station can perform any aggregation functions on them. Then, we propose two RCDA schemes named RCDA-HOMO and RCDA-HETE for homogeneous and heterogeneous WSN respectively. But in this work the signatures bring additional costs. In proposed work, we are encoding the problem of correlated data gathering in WSNs with the objective of minimizing the total transmission cost in terms of power consumption. We particularly focus on the problem of finding the set of aggregation points that satisfy our objective. A novel routing scheme is introduced in this enhancement work for correlated data gathering in wireless sensor networks. Two rooted trees T_R and T_r are used in the scheme to transmit raw data and encoded data, respectively. Inverse links are allowed in T_R for the sake of energy saving, When the double-tree routing scheme is adopted; it is equivalent to partitioning the set of sensor nodes into two sets S_R and S_r , and then constructing T_R and T_r on them so that the total communication cost is minimized.

1. Introduction

Wireless sensor network(WSN) is used in many application including military field,environmental monitoring,healthcare etc.WSN is composed of many sensor and each sensor can communicate with each other to form communication network.Each sensor should sense the data and transmit the sensed data to the base station(BS).Power consumption plays an important role in the construction of WSN.For example if some sensors are deployed to sense the gas leakage or some structural damage,the controllers at the base station should receive the data from all sensors with in some specific period of time else it will lead to some unpredictable action.A practical solution to this problem is data aggretation,it will aggregate the data from multiple sensors and then send the aggregated results to the base station.By sending the aggregated results to the base station communication cost is reduced.Even though base station receives the aggregated result alone,which causes two problem.First,there will be some limited usage of aggragated function.Second,base station cannot confirm the data integrity for all the sensing data.To solve this above two problem recoverable property has been proposed.In that recoverable property signature is generated to all the sensing data so that all the data can be recovered by the base station.Eventhough signature is generated for all sensing data it brings the additional cost so that a novel routing scheme is introduced for correlated data gathering.Two rooted trees T_R and T_r are used in this scheme to transmit raw data in one root and encoded data in another root.Inverse link concept is also introduced inorder to save the energy.

2. Related Works

Wireless sensor network consists of various requirement and encryption scheme they are detaily described as follows.

2.1. Requirement of Wireless Sensor Network

Usually WSN is constructed with battery power applications, lifetime of the sensor is one of the important factor in the WSN.So the algorithm should be designed in such a way to increase the lifetime of the wireless sensor network.Minnimum spanning tree algorithm is used to find the shortest path among the sensors so that data can be transmitted in that path without any congestion..

2.2. Physics and Math

Battery power consumption is one of the important issue in WSN.Large amount of data is being transferred from all the sensors,so it take more power consumption.One way to solve this problem by data aggregation.Another important issue in WSN is security and integrity.All the sensing data should be encrypted and then transmit to the base station.By encrypting the data adversary cannot inject the forged message into the data packet.

3. Data Aggregation WSN

Base station controls the wireless sensor network.Base station is constructed with large bandwidth and some stable power to support the cryptographic and routing requirement of the Generally all the sensors in WSN is divided into several cluster and WSN.Sensors are deployed to sense the data and transmit the sensed data to the base station.

cluster head(CH) is present at each cluster which is responsible for collecting and aggregating the sensing data from sensors with in the same cluster.So that base station receives only the aggregated results from the cluster head(CH).

3.1. Encryption scheme

Encryption is one of the important technique in WSN for data confidentiality.All the sensing data should be encrypted and then transmit to the sink node.Base station will decrypt the message,so that adversary cannot inject any forged message.To achieve end-to-end encryption privacy homomorphism encryption scheme is used.

3.2. Privacy Homomorphism Encryption

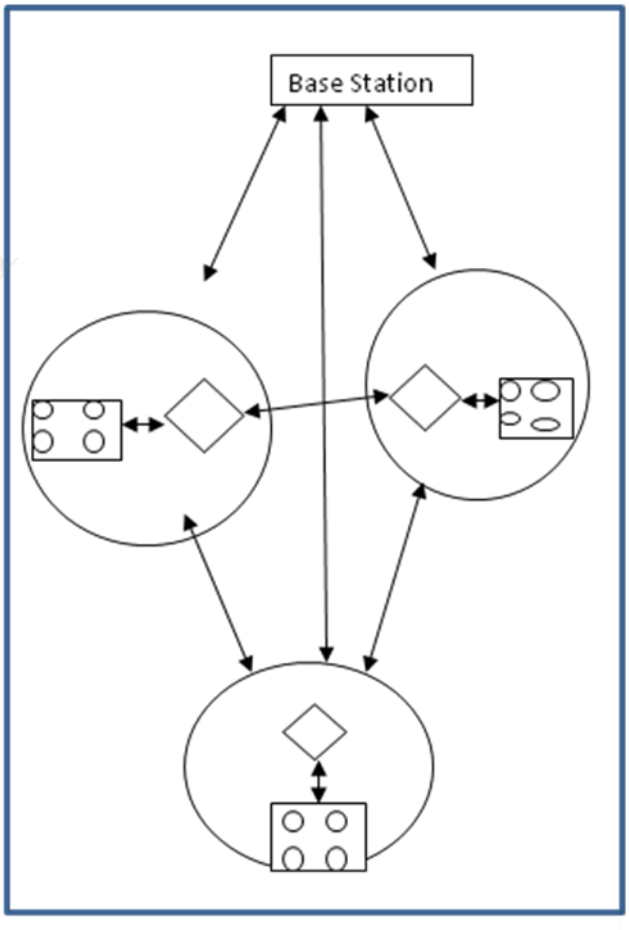
The basic idea behind this encryption scheme is,"sum of numbers can be computed without revealing the single numbers".

Encrypted + Encrypted = Encrypted
Message1 Message2 (message1+ message2)

In privacy homomorphism encryption ,it encrypt message M1by using secret keyK ,so that it produces a ciphertextC.Let C1 denote the first encrypted message M1 with secret keyK1 i.e.,$C1=Enc_{k1}(M1)$ and C2 denote second encrypted messageM2 with secret keyK2 i.e.,$C_2=Enc_{k2}(M2)$.Then it become $C_1.C_2=Enc_k(M1+M2)$.

○Sensor node

◇Cluster head



4.1. Content Searching

In a content search function, the input is a set of keywords representing a user's interests and the output is a set of resources containing these keywords. In the content search context, resources represent text documents or metadata of general resources. Some of these resources are software applications, computer platforms, or data volumes. Content search is useful when a user does not know the exact resource names of interests; this case is common in P2P-based searches as well as in web searches.

Flooding is the basic method of searching in unstructured P2P networks; however, large volume of unnecessary traffic is seen in blind flooding

Fig. 1 Cluster based wireless sensor network

4. Boneh et al.'s signature scheme

Signature is generated for all sensing data so that it take more power consumption.To reduce that Boneh et al.'s signature scheme is used.The concept behind this scheme is to merge the set of distant signature into single aggregated signature.It consists of five procedure namely key generation, signing, verifying, aggregation and verifying aggregated signature.

5. Results

Eventhough base station receives aggregated results alone,there occur two problems.

1. First, there is some constrained on the usage of aggregated function.
2. Second, base station cannot check integrity for all sensing data.

The above two problem can be solved by using recoverable property.In this all sensing data can be received by the recoverable property and check integrity for all sensing data.

5.1. DOUBLE TREE ROUTING SCHEME

The main goal of this paper is to maximize the lifetime of wireless sensor network.Eventhough all sensing data is received by the base station and data confidentiality is provided the transmission speed is not adequate.In order to increase the transmission speed i have introduced a new concept called "DOUBLE TREE ROUTING SCHEME" in which two touting scheme are provided so that encoded data can be transmitted through one tree and raw data can be transmitted through another rooted tree,So that all the data cannot be transmitted through one path and also congestion problem will not occur.

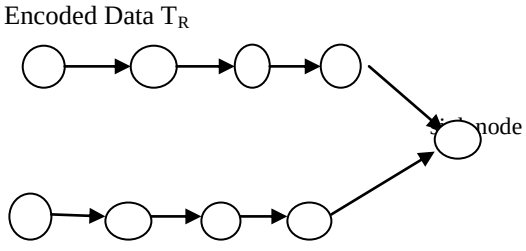


Fig. 2 Double tree routing scheme

6. MINIMUM SPANNING TREE

Usually sink node will decide the path in which data can be transmit from the source node.The sink node will calculate the shortest path by using minimum spanning tree.Minimum spanning tree is constructed using prim's algorithm.

ALGORITHM

//Prim's algorithm for constructing a minimum spanning tree
//Input:A weighted connected graph G=(V,E)
//Output:E_T,the set of edges composing a minimum spanning tree of G
$V_T \leftarrow \{v_o\}$ //the set of tree vertices can be initialized with any vertex
$E_T \leftarrow \varnothing$
for i $\leftarrow$ 1 to |V|- 1**do**
find a minimum-weight edge $e^* = (v^*,u^*)$ among all the edges (v,u) such that v is in V_T and u is in V-V_T
$V_T \leftarrow V_T \cup \{u\}$
$E_T \leftarrow E_{T \cup \{e\}}$
return E_T

Prim's algorithm constructs a minimum spanning tree through a sequence of expanding subtrees.The initial subtree in such a sequence consists of a single vertex selected arbitrarily from the set V of the graph's vertices.On each iteration,we expand the current tree in the greedy manner by simply attaching to it the nearest vertex not in that tree.

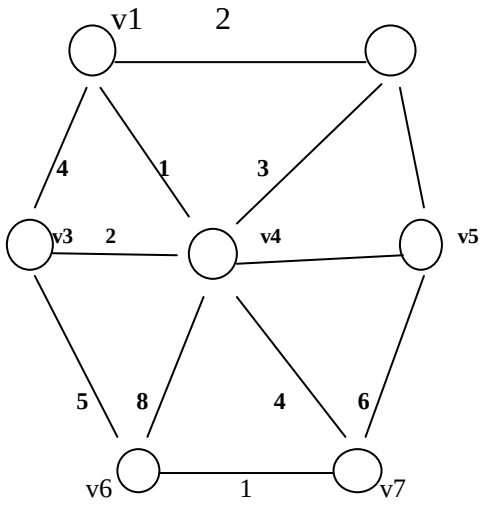


Fig. 3a Example of minimum spanning tree without finding shortest path

The algorithm stops after all the graph's vertices have been included in the tree being constructed.Since the algorithm expands a tree by exactly one vertex on each of its iterations,the total number of such iterations is **n-1,**where **n** is the number of vertices in the graph.

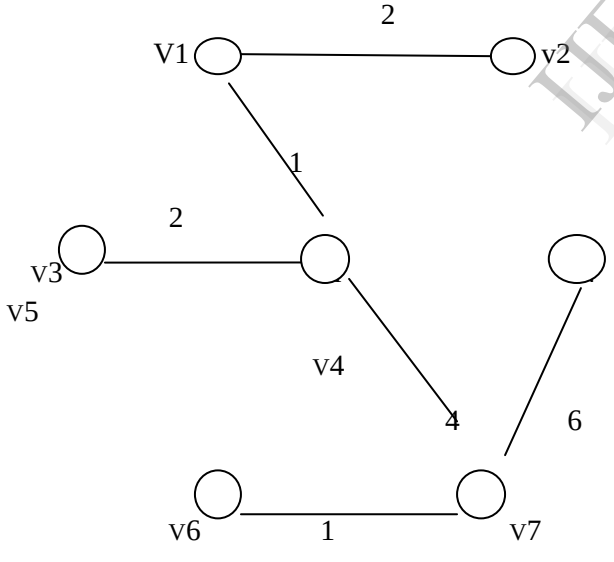


Fig. 3b A graph G and its minimum spanning tree

7. FUTURE WORK

The project is implemented in EOSINT S750.It is a double laser sintering system for the direct,tool less production of sand cores and moulds for metal casting.The EOSINT S 750 is the only double laser sintering system world wide for the processing of the croning mould materials.Using direct casting method,the system builds core and mould for sand casting.Directly from CAD data,fully automatically,with a building speed of upto 2500CM^3/h and without any tooling.

7.1.Problem and solution

Once EOSINT S 750 machine is ready for processing,the controller cannot judge wheather the process is going correctly or not.if the process is not going properly means then the product will get damage.so we going to sense the process running in that machine.By sensing the temperature and every level of processing, we can obtain a better result.if any damage occuring inside the machine is sensed by the sensor means then it should transmit the data to the controller immediately,so that controller can stop the machine by using emergency exit.During transmission the data should be transmitted to the base station very quick so double tree routing scheme is implemented in that machine.

8. Conclusion and Future Enhancement

The recoverable concealed data aggregation schemes for homogeneous/heterogeneous WSNs integrate the aggregate signature scheme to ensure data authenticity and integrity in the design. The problem of minimizing the total communication cost arose from correlated data gathering in wireless sensor networks due to limitations in existing system. It was shown that the proposed double-tree routing scheme was more effective than the single spanning tree routing scheme for correlated data gathering in wireless sensor networks. The approach is further extended to maximize the lifetime of wireless sensor networks while performing correlated data gathering. Minimizing the total energy consumption of sensor nodes is not equivalent to maximizing the lifetime of wireless sensor networks. The energy of some sensor nodes may be over consumed for a minimum-cost routing scheme. Thus the energy consumption of sensor nodes should be balanced in order to extend the lifetime of wireless sensor networks.

9. References

[1] S.M.Mete R.Rajagopalan and P.Varshney,"Data Aggregation techniques in Sensor Networks:A Survey,"IEEE Comm. Surveys Tutorials,vol. 8,no. 4,pp.48-63,oct-Nov.2006

[2] H., am, S. O ¨ zdemir, P. Nair, D.muthuavinashiappan, and H. Ozgur Sanli, "Energy-Efficient Secure Pattern Based DataAggregation,for Wireless Sensor Networks," J. Computer Comm., vol. 29, pp. 446-455, 2006.

[3] D. Westhoff, J. Girao, and M. Acharya, "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks:Encryption, Key Distribution, and Routing Adaptation," IEEE Trans. Mobile Computing, vol. 5, no. 10, pp. 1417-1431, Oct.2006.

[4] C.Castelluccia, E. Mykletun, and G. Tsudik, "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," Proc. Second july 2005.

[5] E. Mykletun, J. Girao, and D. Westhoff, "Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Comm., vol. 5, pp. 2288-2295, June 2006.

[6] "Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A Secure Hop-by- Hop Data Aggregation Protocol for Sensor Networks," ACM Trans. Information and System Security (TISSEC), vol. 11, no. 4, pp. 1-43, 2008

[7] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 416-432, 2003.

[8] M. Demirbas, A. Arora, V. Mittal, and V. Kulathumani, "A Fault-Local Self-Stabilizing Clustering Service for Wireless Ad Hoc Networks," IEEE Trans. Parallel Distributed Systems, vol. 17, no. 9, pp.912-922,sept.2006