Secure based Clustering Algorithm for Wireless Sensor Networks

G. Vennira Selvi,
ME Student,
Department of Computer Science and Engineering,
Manonmaniam Sundaranar University,
Tirunelveli

R. Balasubramanian, Ph.D
Professor,
Department of Computer Science and Engineering,
Manonmaniam Sundaranar University,
Tirunelveli

ABSTRACT
Protecting the data from intruders and increasing the network lifetime is a major constraint in Wireless Sensor Network. The lifetime of the network is determined by the amount of energy consumed by each node. In order to increase the network lifetime and protect the data, the security based clustering algorithm is proposed. It construct the clusters to reduce the energy consumption among the sensor nodes in which the cluster head collects and aggregate the data from the cluster members. A special node MDC collects and aggregates the data from cluster head and forwards them to Base station. The data are protected from intruders by authenticates the Cluster head by MDC using the shared secret key and the Digital Signature. The simulation results prove that our algorithm is more efficiently secure the data and achieves more energy savings than Time Stamp Protocol and Polynomial Points Sharing Protocol.

General Terms
Wireless Sensor Networks, Clustering.

Keywords
Clustering, Network Lifetime,Security.

1. INTRODUCTION
In general, a wireless sensor network consists of thousands of sensors that are smaller in size, low rates, low computational ability and small memory constraint. These nodes are able to gather the data from the surroundings, storing and processing the gathered data and interacting and collaborating within the network [1]. Sensor networks have limited and non-rechargeable energy resources, so the energy effectiveness is one of the challenging factors to extend the lifetime of sensors, which affect the lifetime of overall sensor networks significantly.

Sensor nodes can be grouped into clusters to utilize the energy efficiently and increase the network lifetime [2]. In clustering, each cluster has a Cluster Head (CH) and the number of Cluster Members (CM) which can make a communication only with CH in order to broadcast the data to the Base Station (BS). The role of CH is to collect the data from the CM and it forwards them to the BS and rotates the CH periodically to equalize the energy between the nodes. The CH spends extra energy for gathering data and rotating the CH periodically.

To increase the network lifetime and utilize the energy efficiently, we propose and evaluate a Security Based Clustering Algorithm for addressing the security problem and increasing the lifetime of the network. It is a distributed clustering algorithm, where CHs is elected based on high residual energy of each sensor node and distance from the BS. To conserve more energy for each sensor, the CHs is not elected periodically. It can be re-elected based on some constraints to avoid the frequent re-election of CH. A special node MDC collects and aggregates the data from cluster head and forwards them to Base station. The data are protected from intruders by authenticates the Cluster head by MDC using the shared secret key and the Digital Signature. Our proposed algorithm effectively balances the energy consumption among the sensor nodes and achieves a great improvement in the network lifetime.

The rest of the paper is organized as follows: in the next section, we discuss the related work. Section III describes proposed work, in section IV discuss the Simulation and Experimental Results of the proposed algorithm finally we conclude the paper in section VI.

2. RELATED WORK
This section briefly discusses some well-known clustering algorithms in WSN. We classify the related work into two parts. First, we discuss about the concept of secure data gathering using Cluster Head and second is the concept of secure data collection using MDC.

LEACH [3] is designed to prolong life time of the whole network by distributing energy consumption. LEACH protocol has some assumptions that sensor nodes are uniformly spread over fields and all sensor nodes have enough power to transmit to Base Station(BS) directly. To reduce energy consumption, most sensor nodes send their sensing data to their aggregator. Aggregators will use data fusion function and transmit fused data to BS.

F-LEACH [4] was proposed to secure the cluster formation in LEACH. In this scheme, when a node declares itself as a cluster head, it employs common keys shared with the sink to request the authentication of the CH declaration to the sink. Normal nodes join in only one authenticated cluster head. However, this scheme has no mechanism to authenticate the normal nodes which join in any cluster.

To resolve this problem, Oliveira et al. Proposed SecLEACH [5] in which the sink authenticates the cluster head nodes and the cluster heads authenticate the joining nodes. In F-LEACH and SecLEACH, sensors are pre-assigned some keys for authentication before their deployment. However, both F-LEACH and SecLEACH can prevent only external attackers from joining the cluster formation process. In other words, they cannot prevent internal attackers from declaring themselves as cluster heads and from joining in any cluster.

Buttyan et al. proposed a cluster head election scheme which conceals the election process from external nodes using cryptographic techniques [6]. However the concealment works for only external attackers since a compromised node can easily unveil the selection result. Moreover, the compromised node can declare itself as a CH even though it is not qualified.

Sirivianos et al. proposed the SANE (Secure Aggregator Node Election) protocol [7] in which all CH candidates in a cluster contribute to the generation of a random value and a CH is elected randomly using the random value. SANE is classified into three sub-schemes according to how to generate and distribute the random value. They are Merkle's puzzle based scheme, commitment based scheme, and seed based scheme.

Second concept is secure data collection using MDC, The MDC-based data collection is studied thoroughly in the literature in the context of various mobility models. However, the security aspect in MDC-based data collection is not studied in detail. In [8] key management for secure communication and data collection in distributed WSN is discussed. The scheme ensures only confidentiality of the collected data. Identifying malicious MDC and attacks caused by malicious MDC are not considered. In [9], mobile sink is used for secure data collection. Here a fixed path is used by the mobile sink and only the nodes in this path will be able to communicate with the mobile sink and transfer data. The nodes in the path are overloaded with data transfer function every time a mobile sink visits the nodes for data collection. Also, deterministic path used by MDC leads to various attacks.

All the above proposed algorithms spend more energy while rotating the CH periodically and gathering data from its Cluster Members. Some algorithm provides the solution for securing the data, and some algorithm concentrated to increase the efficiency of network life time but both are not addressed together. This paper protect the data from intruders by attaching both Digital signature and share key to the Cluster head and increases the lifetime of sensor networks by reducing the number of re-clustering and data gathering in CH.

3. PROPOSED WORK

The Proposed Algorithm constructs clusters and electing the Cluster Head (CH) based on the high residual energy and number of neighbours. The CH can be re-elected when the energy level of current CH reaches its predefined threshold value, which reduces the frequent re-election of CH to increase the lifetime of sensor nodes. In addition, to preserve some more energy, data from the sensor nodes is directly transferred to the nearest CHs which forward them to the BS to avoid data gathering in the CH. A Special node Mobile Data Collector (MDC) collects and aggregates the data from CH and transfers it to the Base Station (BS). The CH can be protected by authenticating the MDC using the Shared key and Digital key signature.

Basic Assumptions

There are N numbers of sensor nodes are deployed in the square field. After deployment the nodes and base station are stationary. The nodes can be assumed as homogeneous and location unaware. The cluster head can communicate with the base station directly. Each sensor nodes can know the location of the base station. Each node has an unique identity (id). The energy model is adopted from [10].

The radio energy dissipation model [10] is used to transmit the k bit messages over a distance d is:

$$ET_x(k,d) = \begin{cases} k * E_{elec} + k * \in_{fs} * d^2, & d < d_0 \\ k * E_{elec} + k * \in_{mp} * d^4, & d \geq d_0 \end{cases} \quad \text{……..} \quad (1)$$

Where *E*elec denotes the electronic energy and the ratio of €fs and €mp is constants, that denote the amplifier energy to keep the suitable signal to noise ratio. To receive the message, the energy spent for the radio is.

$$ER_x(k) = k * E_{elec} \quad (2)$$

3.1 Cluster Formation and Key Management

The clustering topology is divided into two phases. 1. Setup phase 2. Data Transmission phase. The setup phase is divided into three sub phases: neighbor node phase, cluster head competition phase, and cluster formation phase; in the data transmission phase, cluster members collect local data from the environment, and send the collected data to the cluster heads, cluster heads receive and aggregate the data from their cluster members, and then send the aggregated data to the next cluster heads. In a data transmission phase, to prolong the network lifetime, we choose the nearest Cluster Head (CH) with high residual energy as a next hop to forwarding an aggregated data to the destination instead of selecting cluster members as a next hop.

BS selects a session key SKi for the ith round of the MDC and constructs the following beacon message: {SKi_TSi}CCHK_h(SKi)_IDMDC. Before deployment MDC is preloaded with session key SKi and the beacon message. Here CCHK is shared by all the CHs and the BS, SKi is the session key and TSi is the time stamp assigned to the MDC for the ith round. Here time stamp TSi corresponds to current time, we assume that the clock value of all CHs and BS are synchronised. Also every CH maintains a table in which it stores information regarding the TSi along with unique Identifier (ID) of the MDC IDMDC. Finally the Digital Signature (DS) is attached to the each cluster Head. After deployment the MDC traverses in the monitoring area and establishes connection with the CH in the region. The MDC sends the beacon message {SKi_TSi}CCHK_h(SKi)_IDMDC to the CH. Now the CH decrypts the session key SKi and the time stamp TSi using the key CCHK. After obtaining the session key Ski and time stamp TSi, CH authenticates the MDC.

3.2 TSP with Digital Signature

After the cluster formation and cluster head selection the MDC is deployed at regular intervals for collecting the data from the cluster head. After deployment, the following operations are considered:

Key Generation: the Base station generates the shared key SK_i using the key generator and set the time stamp TK_i using time stamp generator and digital signature for MDC. All the keys are then distributed to all the cluster heads and base station [13].

Digital Signature: the sending node generates a digital signature $DSIG_i$, with the given message MSG and Time Stamp TS. Then transmit these data to the cluster members in its clusters.

Private Key Generator: A sensor node generates a private key P_k associated with the node ID.

Verification: Sensor node ID, MSG and DSIG is verified whether it is authorized by the Base station. If DSIG is valid, then the node receiving an accept otherwise reject.

The proposed protocol has initialization prior to the node deployment and operates in rounds during communication, which consists of (i) cluster formation phase (ii) Key management phase in each round.

3.3 Protocol Initialization:

The time is divided into discrete intervals using TDMA [11], Time Stamp T_s for Base Station to node transmission and by T_H for cluster member to cluster head. The key distribution is an efficient method to improve communication security, so the pairing parameters are preloaded in the sensor node during the initialization [12]. In protocol initialization, the Base Station performs the following operation for key distribution to the entire sensor node:

i. Generate secrete key PSK_i to encrypt the data where k € (m-1), where m is largest integer. Base Station only shares the key to decrypt the data.

ii. The MDC sends the Beacon signal paired with TS_i and SK_i with ID. It also generates the hash function $h(sk_i)$ to the cluster head along with its DSIG.

iii. The cluster head decrypts the session key SK_i and Time Stamp TS_i using cluster heads own key and verify the signature DSIG.

iv. After verifying the DSIG, the cluster head authenticates the MDC. The paired key (TS_i , SK_i) is shared only to the cluster heads. Therefore an authorized cluster head is able to authenticate the MDC.

Once the MDC is authenticated by the cluster head, The Cluster head transfers the aggregated data to the MDC by encrypting the data using its secret key PSK_i. The cluster head generates the cluster key CK_i, which is shared by all the cluster members in the cluster. The cluster members within the cluster can transmit the data securely using CK_i.

3.4 Algorithm for Proposed work:

i. Choose the cluster head and send the HELLO message to the nearest node.

ii. The nodes send the join message to the cluster head.

iii. After cluster formation, the MDC establishes the connection with the cluster head in the region.

iv. MDC sends the beacon signal to cluster head with $ID||\{SK_i || DSIG\} || h(sk_i)$.

v. Compare the DSIG with the Digital Signature stored in the table.

vi. Computes the hash function for shared key $h(sk_i)$.

vii. Compare the computed hash value with the received value. If not equal, then declare that the node is malicious.

4. SIMULATION AND RESULTS

We have used a simulation model based on NS 2.2 in our evaluation. Our performance evaluations are based on the simulations of 500 wireless sensor nodes that form a WSN over a rectangular (1000 m × 1000 m) flat space. The medium access control (MAC) layer protocol used in the simulations was the distributed coordination function (DCF) of IEEE 802.11. The performance setting parameters are listed Table 1.

Table 1. Parameters Used in Simulation

Simulation Parameters	Values
Network Area	100*100m
Number of nodes	50-250
Transmission Range	100-450m
Network Topology	2D Grid topology
Initial Energy	50J
Propagation model	Two-Ray Model
Queue Type	Drop Tail
Speed	1 m/s to 10 m/s
MAC Type	MAC/802.11
Antenna Type	Omni Antenna
E_{elec}	50 nj/bit
$€_{\beta}$	100 pj/bit/m^2
Data packet size	512 bytes
d_0	50 m
δ	0.2
a_0	0.5
b_0	0.0

The following assumptions can be made about the WSN and the malicious node.

1. WSN nodes are deployed uniformly at random in a planar square region.
2. All the nodes are implemented with the AODV routing algorithm, and have loosely synchronized clocks.
3. Each node transmits one data packet at a random time during a specified send interval. The payload of each packet indicates the originator of the data. No encryption mechanism has been deployed within the network.
4. A single malicious node is present when the WSN is first deployed. The malicious node may be a compromised node or an implanted node. It has the same basic capabilities as the legitimate sensor nodes.

Figure 1. shows the number of CH re-elected with respect to the number of nodes. The initial energy of each node is assigned as 2 joule. The minimum energy is 0.2. The CH re-election is reduced when comparing with TSP and PPSP. This will preserve some more energy to increase the network lifetime.

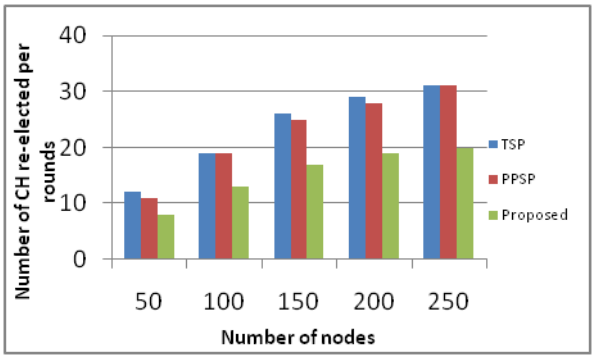

Fig.1. Number of CH re-elected per rounds

Figure 2 clearly shows that the nodes nearer to the BS die much faster than the nodes farther away from the BS. Compared to TSP and PPSP, our proposed algorithm increases the network lifetime of each node nearer to the BS by increasing the number of nodes closer to the BS and it will avoid the node from dying earlier.

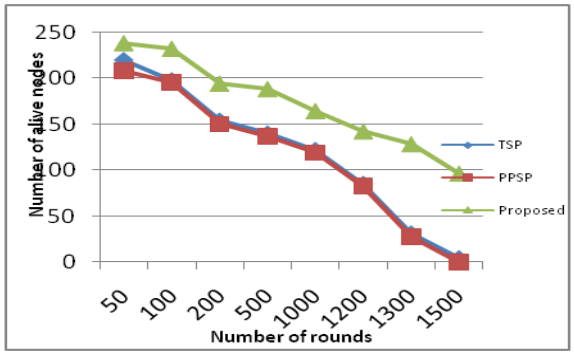

Fig 2. Number of alive nodes over time

The graph for energy consumption vs. number of nodes of proposed algorithm and existing algorithm TSP and PPSP is shown in Figure 3. The total energy consumption includes energy consumption in transferring and receiving a packet in a given time. The transmission consumes greater energy than reception for transferring data packets while calculating total energy consumption in our simulation. The sensor nodes in TSP and PPSP consume more energy to communicate with the BS because of the longer distance between sensor nodes and the BS. However, in Proposed, the number of clusters nearer to the BS is more than TSP and PPSP. The total energy consumption of TSP, PPSP and Proposed algorithms increases when number of nodes or traffic load increases. However, performance of proposed algorithm is improved than TSP and PPSP for different number of nodes.

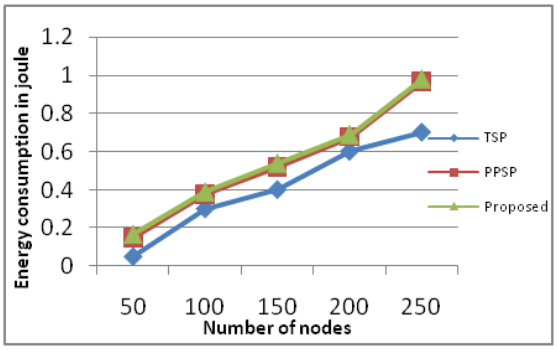

Fig 3. Energy Consumption using TSP,PPSP and proposed

Packet delivery ratio is the proportion of the total amount of packets reaching the receiver and the amount of packets transferred by the source [14]. Mathematically we can define as

$$PDR\ (\%) = \frac{\text{Number Packets delivered}}{\text{Number of Packets sent}} * 100 \quad (7)$$

Figure 4 gives percentage of packets delivered for each round using Proposed, TSP and PPSP algorithms for WSNs. Fig.7.4 illustrates that proposed algorithm provides high packet delivery ratio compared with TSP and PPSP algorithm.

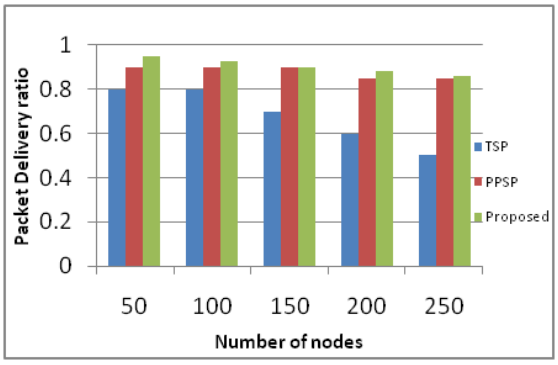

Fig 4. Packet Delivery Ratio of TSP, PPSP and Proposed

The security of the proposed algorithm can be analyzed by injecting the malicious nodes along with the normal nodes. In our experiments, 15 nodes are deployed in the field and the numbers of malicious nodes are varying from 2, 4, 6, 8, and 10. Fig 5 shows that the proposed algorithm can effectively determined the malicious nodes among the normal nodes.

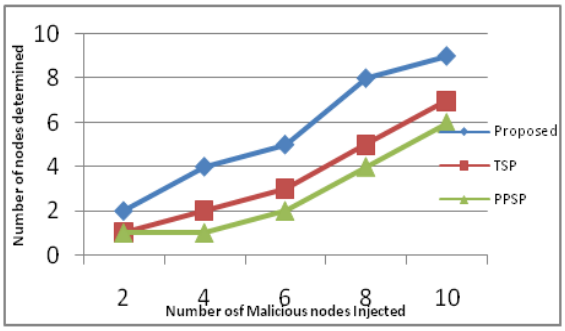

Fig 5. Security analysis of TSP, PPSP and Proposed

5. CONCLUSION AND FUTURE WORK

The data collection using MDC in clustered WSN is one of the important techniques to increase the network lifetime. The secure data collection in clustered WSN using MDC is not explored in detail in the literature. We proposed three protocols TSP, PPSP and Proposed work for MDC-based secure data collection in clustered WSN. The protocols are designed using tree-based key management scheme. The designed protocols address some of the important security issues like identifying malicious MDC and replay messages. The detailed performance and security analysis of the proposed protocols along with energy analysis is explained. The analysis shows that the proposed protocols provide varying level of security against node compromise attack by imposing additional computation overhead. In future research will focus on the optimization of our algorithm for effective

energy consumption among all the nodes and for improving the network lifetime. We shall extend our algorithm to heterogeneous WSNs.

In future, the proposed algorithm will be implemented in heterogeneous networks to increase the network lifetime and consume energy more efficiently. It will also include the trust management between the cluster head and cluster members.

6. REFERENCES

[1] W. Su Y. Sankarasubramaniam E. Cayirci Akyildiz, I.F. A survey on sensor- networks. *IEEE Communications Magazine*, pages 102{114, 2002.

[2] Kumar.S.P. Chee-Yee Chong. Sensor networks: Evolution, opportunities, and challenges. *Proc IEEE*, August 2003.

[3] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An

[4] Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.

[5] L. B. Oliveira, H.C. Wong, M. W. Bern, R. Dahab, and A.A. Loureiro, "SecLEACH-a random key distribution solution for securing clustered sensor networks," Proc. Of 5th IEEE Int'l Symp. On Network Computing and Applications, Cambridge, Massachusetts, USA, Jul. 24-26, 2006

[6] L. Buttyan and T. Holczer, "Private Cluster Head Election in Wireless Sensor Networks," Proc. of the Fifth IEEE Int'l Workshop on Wireless and Sensor Network Security (WSN '09), IEEE, pp. 1048-1053, 2009

[7] M. Sirivianos et al., "Non-manipulable Aggregator Node Election Protocols for Wireless Sensor Networks," Proc. of Int'l Sympo. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '07), Cyprus, pp. 1-10, Apr. 2007

[8] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.

[9] A.S. Poornima1 B.B. Amberker, "Secure data collection using mobile data collector in clustered wireless sensor networks", Published in IET Wireless Sensor Systems Received on 25th October 2011 Revised on 7th February 2011 doi: 10.1049/iet-wss.2010.0086

[10] A S Poornima, B.B.Amberker Tree-based Key Management Scheme for Heterogeneous Sensor Networks 14th IEEE International Conference on Networks, New Delhi, 2008.

[11] Sarika Agarwal Leszek Lilien Maleq Khan, Bharat Bhargava and Pankaj. Self-configuring node clusters, data aggregation, and security in microsensor networks. *Department of Management Information Systems Krannert Grad- uate School of Management Purdue University, West Lafayette*, (IN 47907), 2007. pankaj@mgmt.purdue.edu.

[12] Sundeep Karthikeyan Vaidynathan, Sayantan sur and Sinha. Data aggregation techniques in sensor networks. *Technical Report,OSU-CISRC-11/04- TR60*, 2004.

[13] D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. *Proceedings of the 2nd inter- national conference on Embedded networked sensor systems*, pages 239{249, 2004. ACM Press.

[14] Xiuli Ren and Haibin Yu1. Security mechanisms for wireless sensor networks. *IJCSNS International Journal of Computer Science and Network Security*, VOL.6(No.3):100{107, March 2006.

[15] S. Setia S. Zhu and S. Jajodia. Leap: efficient security mechanisms for large scale distributed sensor networks. *Proceedings of the 10th ACM conference on Computer and communications security*, pages 62{72, 2003. ACM Press.

[16] A. Chandrakasan W.R. Heinzelman and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor network. *IEEE Proceedings of the Hawaii International Conference on System Sciences*, pages 1{10, Jan- uary 2000.