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. 3, Issue 4, April 2015

# A Secure Cluster Based En-route Filtering Scheme in Wireless Sensor Networks

P.Pritto Paul[1], Kessamsetti . Thejaswi[2]

Assistant Professor, Dept. of CSE, Velammal Engineering College, Chennai, Tamilnadu, India [1]

PG Student, Dept. of CSE, Velammal Engineering College, Chennai, Tamilnadu, India [2]

**ABSTRACT:** Wireless Sensor Networking is one of the most prominent technology that is used in almost all real time applications. WSN is used in the estimation of temperature in Cyber Physical Network System(CPNS) where the sensor nodes are deployed in an unsecured environment. In this kind of environment the lifetime of the network , consumption of energy , re-election of cluster head plays an effective role . So, the network lifetime with limited battery power becomes a problematic issue. By selecting the cluster head randomly among the nodes may leads to the issue of battery loss , false data injection attacks. In order to prevent this we make use of Fuzzy logic technique. In fuzzy logic based cluster head election the base station is responsible for the cluster head election because the base station is more powerful than the sensor nodes in terms of power of computing , unlimited supply and storage of power , and memory. So by selecting the most efficient node as the cluster head we can securely forward the data to the base station by using secure algorithms.

**KEYWORDS:** Cyber physical network system, Fuzzy logic, Re-election.

## 1. INTRODUCTION

Wireless sensor networks are expected to interact with the physical world at an unpredictable level to enable various new applications. However, a large-scale sensor networks are deployed in a adverse or even in an unsecured environment which leads to the problem such as accidental failure of nodes in a network, False data injection . As the sensor nodes are relatively small in size and as they are deployed in absence of human environment they are highly sensitive to various risks such as compromising of nodes. False sensing reports can be inject through compromised nodes, which can lead to false alarms.

The false data injection in a cyber physical network system can be overcome by the formation of ***clusters*** where the neighbor sensor node with nearly similar properties will be organized into the form of clusters. In the hierarchical network structure each cluster has a leader, which is also called the *cluster head* (CH). The sensor nodes are responsible for periodically transmission of data to the cluster head(CH) nodes . CH nodes aggregate the data and transmit them to the base station (BS) either directly or through the intermediate communication with other CH nodes. The BS is the central processing unit for the data received from the sensor nodes. The Base Station is fixed at a place in a stationary manner which is far away from the all the sensor nodes .The primary function of cluster head is to collect the data from the nodes present within that cluster and perform aggregation of the data before sending it to the BS.

The advantages of cluster based environment is: 1) supporting network scalability and decreasing energy consumption through data aggregation 2) It can localize the route setup within the cluster and thus reduce the size of the routing table stored at the individual node. The main parameters included in clustering are: Number of clusters, Nodes and CH mobility, Nodes types and roles, Cluster formation, Cluster-head selection.

## II.RELATED WORK

**A) Statistical En-route Filtering** (SEF)[1] is the most basic mechanism in which dense deployment of large sensor networks takes place. To prevent any single compromised node from breaking down the entire system, SEF sends only limited of amount of security information assigned to each node, and depends on the collective decisions of multiple sensors for false report detection. As a report is forwarded through multiple hops toward the sink, each intermediate node verifies the correctness of the MACs carried in the report and drops the report if an incorrect MAC is detected. The disadvantage of SEF is probability of detecting incorrect MACs increases with the number of hops the report travels. SEF[1] and IHA[4] have the *T*-threshold limitations. That is, if the adversary compromises *T* nodes from different groups, they could inject false data to generate the false report.

**B) Location-Based Resilient Security** (LBRS)[2] approach which make use of two techniques: *location-binding keys* and *location-based key assignment*. In location based resilient scheme the location of the sensors and sink is stationary by which it can assign fixed key values for the sensor in order to provide security. Based on its location, a node stores one key for each of its local neighboring cells . LBRS provides a solution to this security problem, but it depends on the stationary of the sink and the fixed routing model such that it cannot work with mobile sinks and various routing protocols.

**C) Grouping-Based Resilient Statistical En-route Filtering** (GRSEF)[3] the GRSEF does not depend on sink . It improves the filtering efficiency by dividing the sensor nodes into certain number of groups and assigns authentications to the groups. GRSEF employees a multi-axis division technique to overcome the threshold limitation problem that we have seen in SEF[1] and IHA[4].

## III.PRELIMINARY

### A) The Basics of En-route Filtering:

The en-route filtering technique used in wireless networks with which the intermediate nodes checks the correctness of the data that is being travelled along the route from source to the sink with the help of intermediate nodes present in the network. The main function of intermediate node is not only checks the correctness of the data but also can filter the false data effectively.

### B) Proposed System for En-route Filtering:

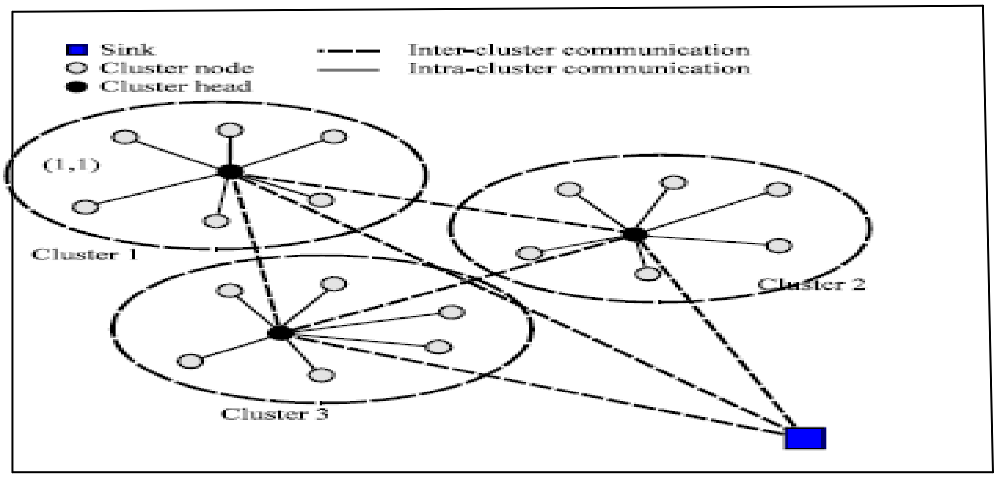
The proposed system for en-route filtering is based on cluster environment where the sensor nodes are organized into groups (clusters). The cluster head is elected by the nodes within the cluster in a random fashion by using the protocol like random seed distribution transitory with master key (rsdtmk). The random number generator produces a sequence of bits from an initial value with the help of recursive algorithm . As the cluster head is randomly elected among the nodes there occurs a delay in the transmission of data from source to destination when cluster head gets drained. The packet loss ratio is also high in random cluster head election.

### C) Security Model Of En-route Filtering:

We consider a large sensor network field where nodes are deployed. So after the network initialization phase the sensor nodes forms into groups and elect a cluster head based on different parameters like remaining energy etc. Whenever events of interest occurs in the terrain say if a tank moves, all the cluster members near to the event will sense the happening and report to their cluster heads. On receiving the reports cluster head aggregates them and sends a single copy of the valid report to the base station through selected report forwarding nodes. The selections of report forwarding nodes are up to the underlying routing protocol's work . And also the selection parameters are independent of the application. We assume that there are attackers present within the terrain are capable of monitoring the communication pattern between the sensor members and the cluster head to guess the message from the reports if intercepted. We assume that each cluster contains at most t-1 compromised nodes, which may collaborate with each other to generate false reports by sharing their secret key information. The potential attacks which we consider in our work DoS attacks. DoS attacks include selective forwarding and report disrupt

10.15680/ijircce.2015.0304051

### D) System Model:



The cluster formation process eventually leads to a two-levels of hierarchy where the CH nodes are the higher level of hierarchy and the cluster-member nodes are the lower level hierarchy. These sensor nodes periodically transmit their data to the corresponding CH nodes. The CH nodes aggregate the data (thus decreasing the total number of relayed packets) and transmit them to the base station (BS) either directly or through the intermediate communication with other CH nodes.

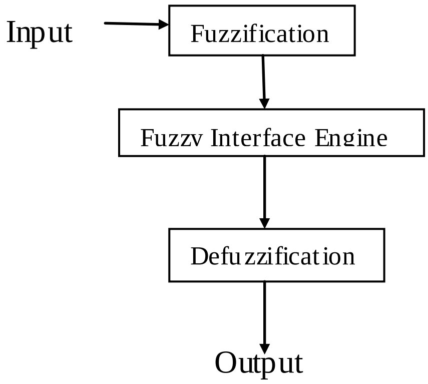
## IV. IMPLEMENTATION MODELS AND ALGORITHMS

### A) Cluster Head Election using Fuzzy logic:

In Fuzzy logic technique the control will be constructed in the Base Station which has the global view over the whole network. The Base Station is responsible for the cluster head election based on the following three parameters : Energy, Concentration, Centrality. Energy is available within each node. Concentration is number of neighbor nodes for the base station. Centrality is the value that is based on how close is the node to the cluster. The input's of fuzzy inference system are the energy and the distance of a particular node to the base station.

Node Energy = Energy remaining/Initial Energy

### B) Design of Fuzzy system



a. Fuzzification : The input value is converted into Fuzzy values.
b. Fuzzy Interface Engine : The converted Fuzzy values are applied to the fuzzy rules. The aggregation of all the outputs of all the rules are unified.
c. Defuzzification : aggregating outturn of fuzzy set and the outturn is a single value.

**C) Security Model:**

After the election of cluster head the data has to be securely forwarded to the base station. The data can be securely transmitted from the cluster head to the base station as the cluster head is trusted party elected by the base station. The data being transmitted must be enclosed with Cluster ID. The fuzzy logic technique makes use of Energy balance loss protocol.

**D) Key generation:**

The key generation is an important step in cluster formation as it provides security for the transmission of data between the nodes. In key generation process the steps such as encryption and decryption of data takes place.

## V. RESULTS AND DISCUSSION

The results are estimated and the graph is generated when the data transmission takes place from cluster to the sink. The ns2 simulator tool is used to compare the two protocols such as random seed distribution with the help of master key(rsdtmk) and energy balance loss protocol(eblp) which is used in the fuzzy logic based cluster head election. And the graphs clearly show that eblp protocol is more efficient than the existing protocol like rsdtmk.

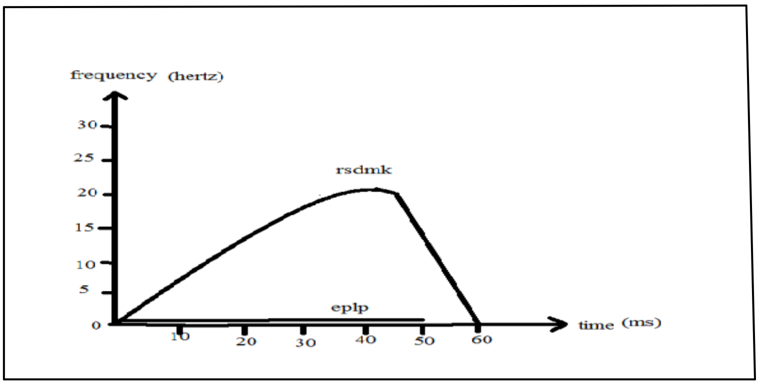


Fig. 1 Delay measurement

The fig.1represents the comparison between the two protocols that represents the measurement of delay while transferring the data from the source to destination. The occurrence of delay is reduced by using the energy balance loss protocol which is employed in fuzzy logic technique.

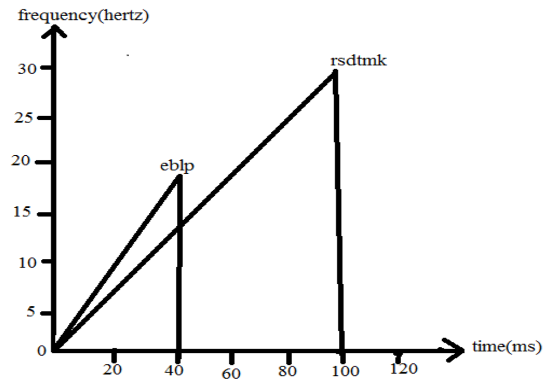


Fig. 2 Packet loss ratio

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. 3, Issue 4, April 2015

The fig. 2 represents the comparison graph of packet loss ratio between the rsdtmk and eblp. The packet loss ratio is comparatively high when we use random cluster head election method. The packet loss ration can be reduced by energy balance loss protocol which employed in fuzzy logic technique.

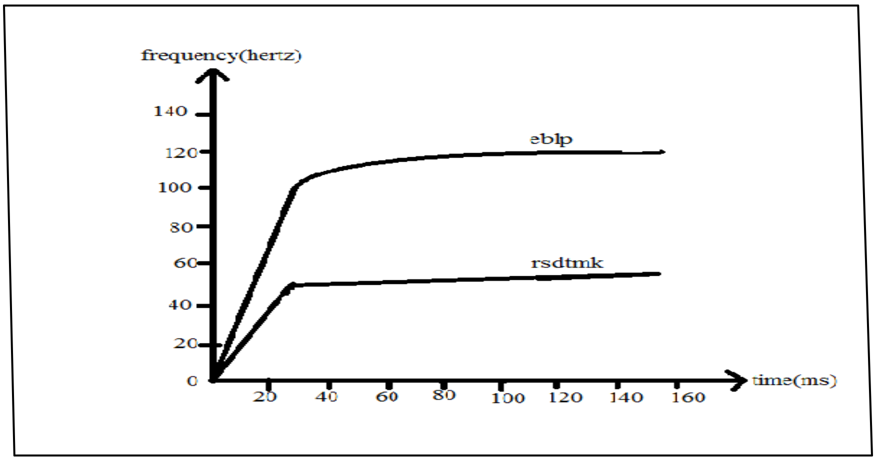


Fig. 3 Transmission Channel Ratio

The fig.3 graph clearly shows the transmission channel established in eblp is higher than the channel established in rsdtmk. So, the data is more securely transferred in the channel established through eblp rather than rsdtmk. As the transmission channel ration is high the data loss ratio can be reduced.

## VI. CONCLUSION

The clustering scheme achieves not only high en-routing filtering probability but also high reliability for filtering the injected false data with multi-reports without depending on static routes and node localization. Due to the simplicity and effectiveness, the cluster based scheme could be applied to other fast and distributed authentication scenarios in wireless network.

## REFERENCES

1) F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injection false data in sensor networks," *IEEE Journal on Selected Areas in Communications (JSCA)*, vol. 23, no. 4, pp. 839–850, 2005.
2) H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward resilient security in wireless sensor networks," in *Proc. of the 6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc'05)*, 2005, pp. 34–45.
3) L. Yu and J. Li, "Grouping-based resilient statistical en-route filtering for sensor networks," in *Proc. of the 28th IEEE International Conference on Computer Communications (INFOCOM'09)*, 2009, pp. 1782–1790.
4) "Clustering in Wireless Sensor Networks" textbook Basilis Mamalis, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou.
5) "Filtering Schemes for Injected False Data in Wsn" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 6 (Jul. - Aug. 2013), PP 29-31.
6) "Fuzzy logic based energy efficient protocol in wireless sensor networks" ICTACT JOURNAL ON COMMUNICATION TECHNOLOGY, DECEMBER 2012, VOLUME: 03, ISSUE: 04
7) "A New Approach in key generation and Expansion in Rijndael Algorithm" The International Arab Journal of Information Technology, vol. 3, No.1, January 2006.
8) "An Optimized Low Loss Energy-Aware Routing Protocol for Wireless Sensor Networks" International Journal of Computer Applications (0975 - 8887) Volume 65 - No. 21, March 2013.
9) "A Survey on Algorithms for Cluster Head Selection in WSN" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, No 5, May 2013.
10) "Algorithms For Wireless Sensor Networks" Sartaj Sahni and Xiaochun Xu
Department of Computer and Information Science and Engineering, University of Florida, Gainesville, FL 32611 {sahni,xxu}@cise.ufl.edu September 7, 2004.