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. 2, Issue 3, March 2014

Effective and Secure Transmission Approach for Multi Cluster Based Wireless Sensor Network.

R.Pushpa Raghunath[1], K.Venice Christopher[2], R.Vignesh[3], S.Deepika[4], M.Radhamani[5]

UG Scholar, Department of Computer science & Engineering, Sree Sakthi Engineering College,

Coimbatore, Tamilnadu, India[1, 2, 3, 4]

Assistant Professor, Department of Computer science & Engineering, Sree Sakthi Engineering College,

Coimbatore, Tamilnadu, India[5]

ABSTRACT: The wireless sensor networks have wide processing capacity in which the data transmission plays a vital role in WSN. We are enhancing a system to have a better data transmission rate. Based upon the study we found that the transmission of data in the Military is still not highly secure. So our system enhancing the security based on the Digital Signature and the security under digital signature. Initially we group the nodes in the form of cluster and those clusters have the cluster head to access the region. After the formation of the cluster region, need to analyze the mobility, and therefore to process the data transmission. For the transmission of data we propose the algorithm EEDC in the existing they have used LEECH. Being the process in wireless network, clusters are formed periodically and dynamically. In the security part we are using two ways, one is the identity based digital signature and Identity based online/offline Digital Signature. So the system will be much more secure than the present strategy. The attacker can be easily identified with this network.

Keywords: EEDC Algorithm, LEECH protocol, Digital Signature, Cluster node.

I. INTRODUCTION

In this modern world we thrive in using technology which is the most effective and easier in terms of viewing, scanning and to process the obtained data. Wireless sensor network has become a vital part in such activities. The wireless sensor network comprises of node which interfaces with nodes that scan the environment which are sensor nodes, and as the name depicts “wireless”, the obtained data is transmitted wirelessly to the base station which acts as a repository.

One of the major threats in wireless sensor network is security and huge consumption of energy which has to be addressed. Energy consumption can be constrained through clustering. Clustering is an effective way of avoiding complexities between sensor nodes of a network which will transmit data to the base station through the cluster head. Security for wireless sensor network can be provided using digital signature which is a critical security service offered in asymmetric key management like cryptography. As we have introduced clustering technique our network becomes a “cluster based wireless sensor network”.

Dynamic clustering of the sensor nodes will help in reducing the energy consumption to an extent by multi-hop technique. For this EEDC algorithm is used. The Energy Efficient Dynamic Clustering (EEDC) algorithm which supports two tier hierarchy networks for providing data to multiple base stations is known as two tier hierarchy network.

II. LITERATURE SURVEY

A. *Paper Title: Balanced energy sleep scheduling scheme for high density cluster-based sensor networks.*

This in paper the concept analyzed as, Conserving Battery power in sensor network is an important aspect , to achieve this nodes which are ideal can be put to sleep so that the energy can be used only those nodes which are active [2] . Three scheduling schemes can be used, which are Balanced-energy scheduling scheme (BS), Randomized scheduling scheme (RS), Distance Based scheme (DS).

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. 2, Issue 3, March 2014

Randomized Scheduling scheme (RS) selects the nodes randomly, which are ideal and puts them to sleep. Distance based scheduling scheme (DS) selects the ideal nodes with respect to the distance of those nodes from the cluster head. Balance-energy scheduling scheme maintains the average energy consumption of all the nodes in the cluster to be same. The BS is as same as DS. The mechanism used to put the ideal nodes to sleep has to be aware of putting only the ideal nodes and not the nodes which are active.

Timer will be provided to those nodes which are put to sleep which will consume very low energy in order to keep track of the time duration of the sleeping nodes.

B. Paper Title: Routing Techniques in Wireless Sensor Networks: A Survey

This paper enhances the major issue in Wireless Sensor Network is Energy consumption which would reduces the lifetime of the network [7]. Since the entire sensor nodes are battery powered, certain steps should be taken to conserve the battery power. Clustering could reduce the energy consumption to some extent.

Another method to reduce the energy-consumption is using Routing techniques. The data sensed by the sensor nodes are routed to the base station by some strategy which will reduce the energy consumption to a great extent. Routing in Wireless Sensor Network has three classification and they are

- Flat-based routing - all the nodes have equal functionality in the network
- Hierarchical-based routing - nodes have different functionality in the network
- Location-based routing - position of the nodes in the network decides the functionality.

In all the above routing techniques the best path that consumes less energy for the data transmission than any other path in the network is found and data is sent through it. If any node in the founded path is damaged or failed then the routing algorithm itself should accommodate a new path to the base station. The main objective is reducing the energy consumption of the nodes in the network. But the data delivery is not compromised.

C. ***Paper Title: Secure Routing In Wireless Sensor Networks: Attacks And Countermeasures***

Many routing protocols have been proposed to reduce the energy consumption in the network. But none of them had concerned with the security issues in the wireless sensor network [9]. If a Wireless sensor network is attacked, then it would cause a serious loss than any other network.

The two classes of attacks against the sensor networks are sinkholes and Hello floods.

- **Sinkhole Attack** – It compromises a node in the network, attracts the neighboring nodes and makes every data to go through it with respect to the routing algorithm.
- **Countermeasure** – Geographic protocol is used to avoid sinkhole attack. This protocol uses the localized interaction and information to construct a topology and also avoid the initiation from the base station.
- **Hello Flood attack** – An attacker outside the network who has large transmission power may send a HELLO packet to every node in the network and them to believe that it is within the network. So, attacker can easily steal the data.

Countermeasure - Each node is provided with an ID. And during data transmission each node should authenticate its neighboring node using Identity verification protocol to avoid Hello Flood attack. Multipath protocol can be used to avoid compromised nodes. In this protocol the data is routed over 'n' paths and the nodes in it are disjoint.

D. Paper Title: A Survey of Security Issues in Wireless Sensor Networks

This paper analyzes the efficiency of the Wireless sensor networks which are mainly used for military purpose for send and receive the code or message [3] . It rectifies the open research issues for direction on security in WSNs. Secure

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. 2, Issue 3, March 2014

routing protocols are be considered in key distribution the node sends the message from one node to base station. Aggregation of sensor data is to be secured. It produce less important for low level data to save energy level and produce high level security for more sensitive data.

The main purpose of security requirements is to identify the information and resource from attacks and misbehavior. Symmetric key cryptography is power consumption in sensor nodes. Open research issues are high speed and low energy cost. In this efficient and flexible key distribution are to be design. There are many routing techniques are been designed for WSNs. Some networks are been design security as a goal. Wireless sensor network are VULNERABLE to many kind of attack in secure routing protocols.

Secure routing is a ad hoc network similar to sensor network. It depends on appropriate key management scheme in WSNs. Data aggregation is mainly for WSNs. The nodes are been provide by pair wise key and other node are in multiple hops. The cluster head collect all the information and send it to the base station as they required. Sensor nodes are constrained by less energy.

III. EXISTING SYSTEM

In the current system the functionality is that they have used a single cluster for overall system. So that the formations of nodes are in hierarchical and for this they used LEECH protocol. The main drawback of this system is that reduces the energy level and it rotates randomly, dynamically and periodically because of this there may cause of misusing of data`s and it rearrange the cluster and link. Node to node trust is not adequate and also the pair wise key is one of the problems in the transformation.

IV. PROPOSED SYSTEM

In the proposed system, the main alter is the protocol, we use the EEDC protocol in which it is mainly used in the wireless Sensor Network for the transmission in the multipath environment.

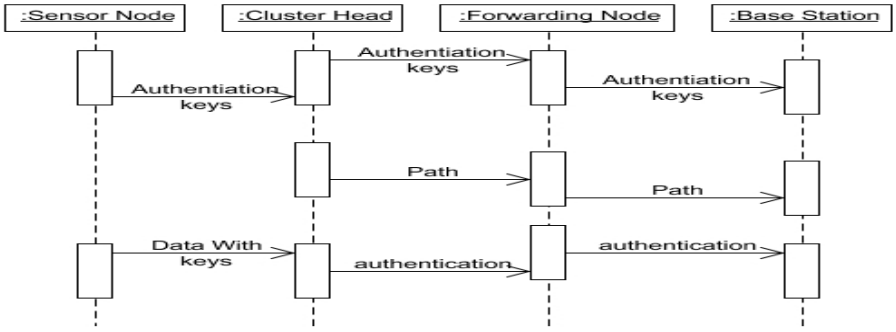

Fig 1: Proposed Method

And the security used is the Digital Signature in two ways as explain in the abstract those methods follows the instruction as the name as identity so that the level of security is high and also the communication and computational problem is resolved.

Every node created by the cluster head is analyzed, to the base station for the authentication and the transfer of node can be done by means of the mobility of the sensor head. This can be analyzed by means of various levels of authentication and the level of transparency. Thus when compare to the existing system here we analyzed that the efficiency of various nodes in the cluster will be available in case of the authentication when processed in the transfer of the message in multi cluster environment.

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. 2, Issue 3, March 2014

V. EXPRIEMENTAL RESULT

The result shown the overall performance of the proposed system the analyses can be found that the cluster region formed is to be a node and the access point and the notification can be formed in the mobility space and for the node formation the distance is to be mentioned in a practical way. The levels of the experimental process are given below. It shows the complete analysis of the proposed method.

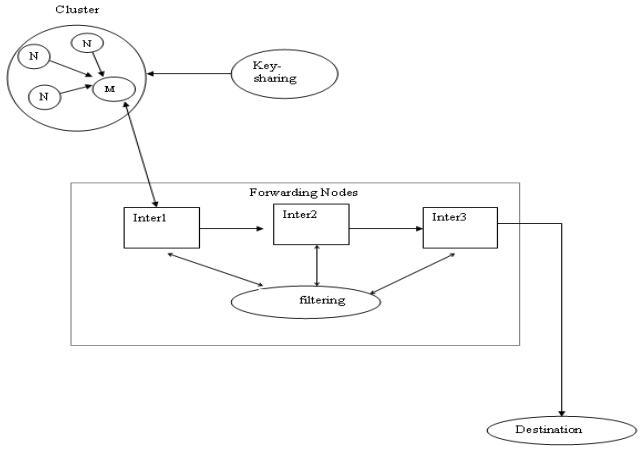

Fig 2: Formation of Cluster

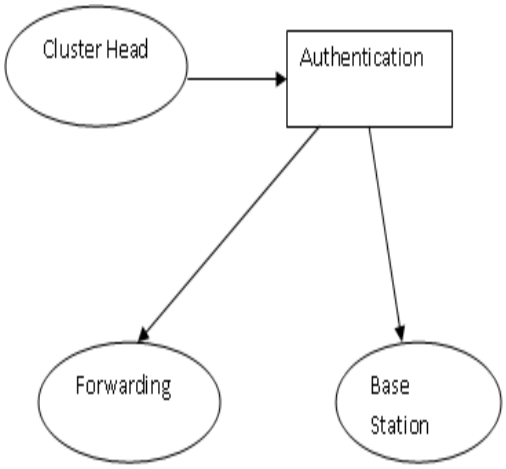

Fig 3: Authentication

The sensor node can be also identified for the detection it will be aware of the attacker side process.

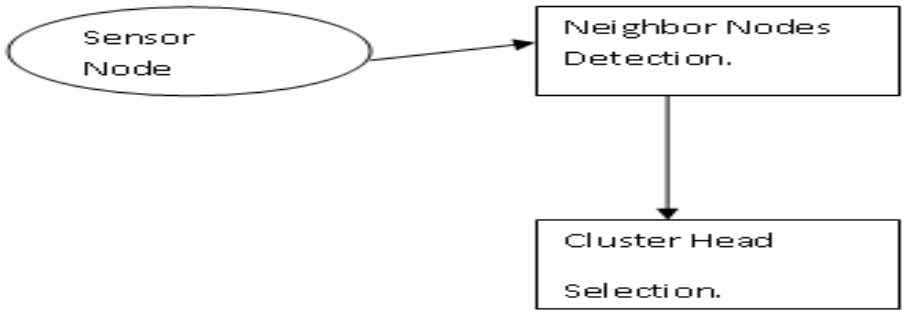

Fig 3: Sensor Node

By the Formation of the cluster region the data start transform from one node to another by means of analyzing the transfer rate and the mobility of the sensor. If any change in access level end then it is to be found that the attacker is sending and won't accept the data inside the cluster. This is to analyses the level of security.

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. 2, Issue 3, March 2014

VI. CONCLUSION

We first analyzed the data transmission issues and the security issues in CWSNs. Then the absence of the symmetric key management for secure data transmission has been discussed. Then, we accessed two secure and efficient data transmission protocols for CWSNs, they are SET-IBS and SET-IBOOS and the feasibility is also analyzed again the routing mechanism. Finally, the comparison in the calculation and results shows that the proposed protocols have better performance than the existing secure protocols for CWSNs. With respect to both computation and communication costs the system efficiency is moderately good.

REFERENCES

1. Huang Lu, Jie Li and Mohsen Guizani "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks" Ieee Transactions On Parallel And Distributed Systems, Vol. 25, No. 3, March 2014.
2. Deng, Jing; Han, Yunghsiang S.; Heinzelman, Wendi B.; and Varshney, Pramod K., "Balanced energy sleep scheduling scheme for high density cluster-based sensor networks" (2004). Electrical Engineering and Computer Science. Paper 102.
3. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tuts., vol. 8, no. 2, pp. 2–23, 2006.
4. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," Comput. Commun., vol. 30, no. 14-15, pp. 2826–2841, 2007.
5. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670, 2002.
6. Mohamed Younis, Moustafa Youssef, Khaled Arisha, "Energy-Aware Routing in Cluster-Based Sensor Networks".
7. Jamal N. Al-Karaki, The Hashemite University Ahmed E. Kamal, Iowa State University "Routing Techniques In Wireless Sensor Networks: A Survey", , 1536-1284/04/$20.00 © 2004 IEEE IEEE Wireless Communications, December 2004
8. K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," Int. J. Comput. Applications, vol. 47, no. 11, pp. 23–28, 2012.
9. Chris Karlof , David Wagner., "Secure routing in wireless sensor networks: attacks and countermeasures," 1570-8705/$ - see front matter _ 2003 Elsevier.
10. R.Shanmugapriya," Secure Transmission Approach for Multi Cluster Wireless Sensor Network", conference publication.
11. P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in Proc. IEEE NCA, 2007, pp. 145–152.
12. K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," in Proc. WiCOM, 2008, pp. 1–5.

BIOGRAPHY

R.Pushpa Raghunath is an Under Graduate Student in the Dept of Computer Science and Engineering, in Sree Sakthi Engineering College, Coimbatore, under Anna University. Area of Interest is Sensor Network, Network Security.

K.Venice Christopher is an Under Graduate Student in the Dept of Computer Science and Engineering, in Sree Sakthi Engineering College, Coimbatore, under Anna University. Area of Interest is Software Testing, Parallel and distributed Computing.

R.Vignesh is an Under Graduate Student in the Dept of Computer Science and Engineering, in Sree Sakthi Engineering College of, Coimbatore, under Anna University. Area of Interest is Networking, Model Creation.

S.Deepika is an Under Graduate Student in the Dept of Computer Science and Engineering, in Sree Sakthi Engineering College, Coimbatore, under Anna University. Area of Interest is Data mining, Sensor Network.

M.Radhamani Completed her PG in the Dept of Computer Science and Engineering, and currently working as the assistant professor in Sree Sakthi Engineering College, Coimbatore, under Anna University. Her Area of Interest is Networking, Internet Programming, and Network Security.