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. 4, Issue 4, April 2016

Secure Data Dissemination in Cluster Based Wireless Sensor Networks

Darshan D C, Ravi Kumar

PG Student, Dept. of CSE, Rajeev Institute of Technology, Hassan, Karnataka, India.

Assistant Professor, Rajeev Institute of Technology, Hassan, Karnataka, India.

ABSTRACT: Security is a basic requirement of an organization in the world to keep their information secure from their competitors. Secure data transmission is a critical issue for wireless sensor networks. Clustering is an effective and practical way to enhance the system performance of WSNs. A secure data transmission for cluster-based WSNs is studied, where the clusters are formed dynamically and periodically based on k-medoids style routing protocols, AES algorithm for data encryption and RSA for authentication. Used protocols consume smallest amount of energy and provide high throughput.

KEYWORDS: Secure Data Dissemination, Clusters, wireless sensor networks, K-medoids protocol, AES, RSA.

I. Introduction

A wireless sensor network is a network consisting of multiple wireless sensors, also called nodes, which cooperate in sensing some sort of physical or environmental conditions, such as temperature, sound, vibrations, light, movement etc. The individual sensor nodes are small and have limited energy, computational power and memory. These wireless sensor nodes are tiny devices with limited energy, memory, transmission range, and computational power. A base station is usually present in the network, which receives the sensor data from the sensors. Such a base station is usually a powerful computer with more computational power, energy and memory. In most circumstances, wireless sensor networks require some amount of security in order to maintain high survivability and integrity of the network.

Several nodes may be tasked with sensing the same phenomenon these nodes may cooperate in a “cluster” where one node is tasked with compressing the sensor result from all the other nodes in the cluster and produce a “collective view” of the cluster on the situation, this is called data aggregation.

In wireless sensor network, collection of sensor nodes into a cluster is well-known as clustering. Every cluster contains a

Leader called cluster head. A cluster head may be selected by the group of cluster. A cluster head collects the information from the nodes within cluster and send this information to the base station (destination). Clustering can be used as an energy efficient communication protocol. The main aim of clustering is to minimize the total transmission power aggregated over the nodes in the selected path, and to balance the load between the nodes for extend the network lifetime. Cluster-based routing algorithms are growing to be an essential part of routing technology in wireless sensor networks on account of a form of advantages, such as larger scalability, less load, smaller amount energy consumption.

II. Related Work

Barla et.al [3], proposed a technique for anonymous sharing of private data between N parties is developed. This technique is used to allocate these node ID numbers ranging from 1 to N and also apply encryption on private data. These assignments are anonymous in that the identities received are unknown to the other members of the group. Animosity between other members is verified in an information theoretic sense when private communication channels are used. This type of serial numbers assignment allows more complex data to be shared and has applications to other problems in privacy preserving data mining, animosity avoidance in communications and distributed database access. The prescribed computations are distributed without using a trusted third party central authority. Existing and new

DOI: 10.15680/IJIRCCE.2016. 0404325

techniques for assigning anonymous IDs are examined with respect to trade-offs between communication and computational requirements.
Senthil Kumar et.al [1], a special sensor network, a wireless body area network (WBAN) provides an economical solution to real-time monitoring and reporting of patients physiological data wireless sensor networks are widely data applicable in monitoring and control of environment parameters. It is sometimes necessary to disseminate data through wireless links after they are deployed in order to adjust configuration parameters of sensors or distribute management commands and queries to sensor.

III. Proposed System

Figure1 shows the architecture of our proposed system.

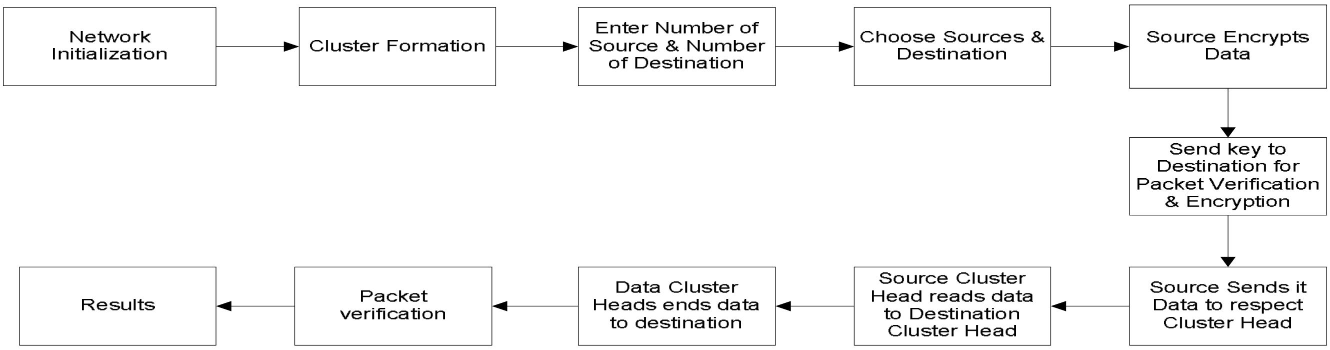

Network Initialization
Cluster Formation
Enter Number of Source & Number of Destination
Choose Sources & Destination
Source Encrypts Data
Send key to Destination for Packet Verification & Encryption
Source Sends it Data to respect Cluster Head
Source Cluster Head reads data to Destination Cluster Head
Data Cluster Heads ends data to destination
Packet verification
Results

Figure1: Shows the Architecture of our block diagram.

a) *Network initialization:*

In network initialization phase, the network owner creates its public and private keys, and then loads the public parameters on each node before the network deployment it consists of number nodes as packets by initializing each node. Figure2 shows the flow diagram of the proposed system.

b) *Cluster formation:*

Collection of sensor nodes into cluster is well-known as clustering.

a) *Enter Number of source and number of destination:*

With help of k-medoids style the labeling will be done for each cluster.

b) Choose Source & Destination:

Clusters are created by assigning each object to the cluster of the representative (medoids) that is closest to that object.

c) Source Encrypts Data:

The key has encrypted using algorithm RSA and AES

a) *Send key to destination for packet verification & encryption:*

The encrypted key sends from sources end destinations. Packets are transferred from source to destination via the cluster heads. At destination packets are verified. The packets which fail to get verified are discarded.Figure2 explains the flow diagram.

A. K-medoids algorithm

The k-Means algorithm is sensitive to outliers since an object with an extremely large value may substantially distort the distribution of data. Instead of taking the mean value of the objects in a cluster as a reference point, a medoid can be used, which is the most centrally located object in a cluster. Thus, the partitioning method can still be performed based on the principle of minimizing the sum of the dissimilarities between each object and its corresponding reference point.

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. 4, Issue 4, April 2016

This forms the basis of the k-Medoids method. The basic strategy of medoids clustering algorithms is to find k clusters in n objects by first arbitrarily finding a representative object (the medoids) for each cluster. Each remaining object is clustered with the medoid to which it is the most similar. The k-Medoids method uses representative objects as reference points instead of taking the mean value of the objects in each cluster is the key point of this method. The algorithm takes the input parameter k, the number of clusters to be partitioned among a set of n objects. Using Euclidean distance as a dissimilarity measure, compute the distance between every pair of all objects as follows

$$d_{ij} = \sqrt{\sum_{a=1}^{p} (X_{ia} - X_{ja})^2} \qquad i = 1 \ldots\ldots\ldots n; \; j = 1 \ldots\ldots\ldots n \qquad (1)$$

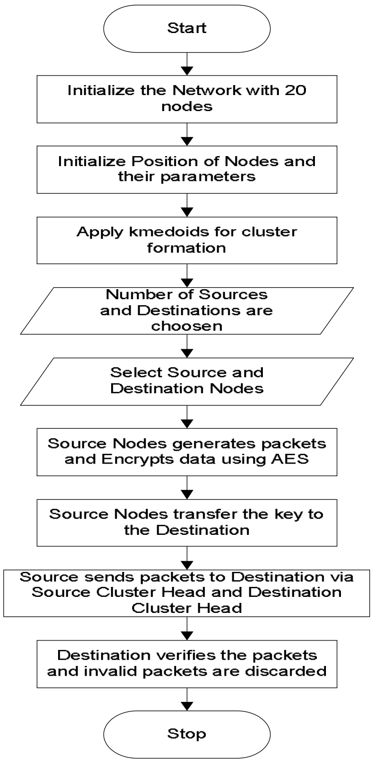

Start
Initialize the Network with 20 nodes
Initialize Position of Nodes and their parameters
Apply kmedoids for cluster formation
Number of Sources and Destinations are choosen
Select Source and Destination Nodes
Source Nodes generates packets and Encrypts data using AES
Source Nodes transfer the key to the Destination
Source sends packets to Destination via Source Cluster Head and Destination Cluster Head
Destination verifies the packets and invalid packets are discarded
Stop

Figure1 shows the architecture of our proposed system

B. RSA for key generation

Public key cryptography, also known as asymmetric cryptograph, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both public and the private keys can encrypt a message. The opposite keys from one used to decrypt it.

VI. RESULTS

The menu is first created from where execution of program starts. The menu is as shown in figure 4. The Network Initialization is opted, and then network is initialized with 20 nodes with parameters initialized as in figure 5.

DOI: 10.15680/IJIRCCE.2016. 0404325

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. 4, Issue 4, April 2016

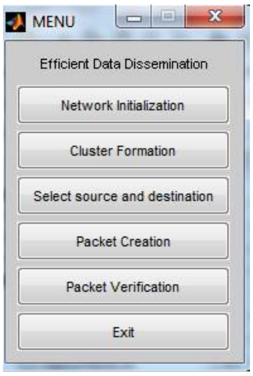


Figure4: Shows the main menu

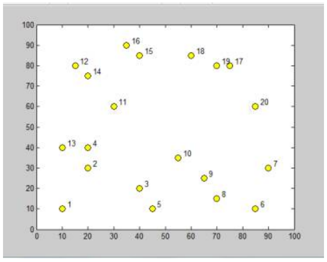


Figure 5. Network Initialization

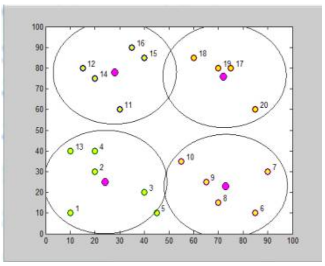
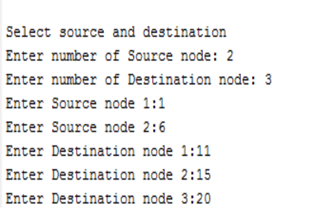


Figure 6: Cluster Formation

Next module is cluster formation, when Cluster formation module is opted, the cluster formation is done as shown in figure 6.



```
Select source and destination
Enter number of Source node: 2
Enter number of Destination node: 3
Enter Source node 1:1
Enter Source node 2:6
Enter Destination node 1:11
Enter Destination node 2:15
Enter Destination node 3:20
```

Figure7: Selecting Number of Sources and Destinations

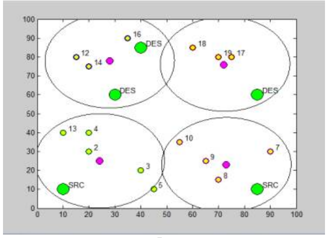
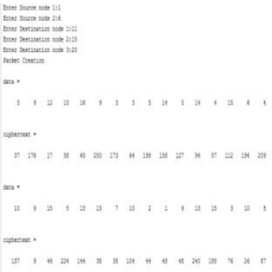


Figure 8: Selecting Source and Destinations



```
Enter Source node 1:1
Enter Source node 2:6
Enter Destination node 1:11
Enter Destination node 2:15
Enter Destination node 3:20
Packet Creation

data =

     5     9    12    15    16     9     3     3     5    14     5    14     4    15     6     4


ciphertext =

    37   176    17    38    65   250   173    64   198   158   127    94    57   112   194   209


data =

    10     9    15     5    15    13     7    10     2     1     9    13    15     3    10     8


ciphertext =

   137     9    46   224   144    38    38   104    44    45    48   240   188    76    26    87
```

Figure 9: Data Encryption

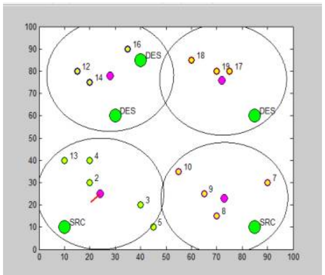
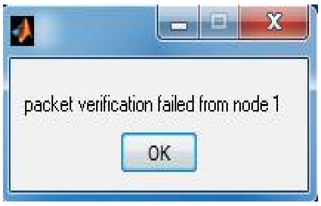


Figure 10: Packet Transfer

Packets are transferred from source to destination via the cluster heads. At destination packets are verified. The packets which fail to get verified are discarded


packet verification failed from node 1

.Figure 11: Packet Verification Failure of Node1

packet verification failed from node 2

Figure 12: Packet Verification Failure of Node 2.

VII. CONCLUSION

Cluster based routing schemes are very efficient in performance growth of WSNs. But some of the problems stated in wireless sensor networks are network lifetime, power consumption and security. In order to overcome these problems cluster network model is used. The main objective of clustering for secure data dissemination is to increase the network lifetime and reducing power consumption of each node in the wireless sensor network .The cluster heads reduces the load by avoiding the redundant data. And also Clustering approach reduces the packet delay. It increases the scalability of the network by reducing the size of routing table. In this paper, we have used cluster formation protocol K-medoid .K-medoid protocol is more robust against the attackers. The performance of the Medoid protocol is better than the LEACH, HEED and K-means protocols.

REFERENCES

[1] A. Senthil Kumar, “A Secure Distributed Data Discovery and Dissemination In Wireless Sensor Networks,” International Journal of Engineering & Science Research, Vol-5, pp 708-713, 2015.

[2] D.He, “DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks,” IEEE Trans, Vol. 11, No. 5, pp. 1946–1956, May2012.

[3] Barla,” Efficient and Secure Data Sharing By Applying AES Algorithm with Anonymous Id Assignment”, International Journal of Science and Research (IJSR) ISSN, pp 2319-7064, 2012

[4]D. Jana, "Privacy and anonymity protection in computational grid services," Int. J. Computer. Sci. Applicant., Vol. 6, No. 1, pp. 98-107, Jan. 2009.

[5] Jisha, “Data dissemination protocols in wireless sensor networks-a survey”, IJARCCE, March 2014.

[6] Akyildiz, “survey on sensor networks”, IEEE Communications Magazine, Vol. 40, No. 8, pp 102– 114, 2002.

[7] Tyagi S, Kumar N. “A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks”, Journal of Network and Computer Applications, Elsevier, Vol. 36, No. 2, 2013, pp 623-645.

[8]YanweiWu, "Energy-Efficient Wake-Up Scheduling for Data Collection and Aggregation, Parallel and Distributed Systems”, IEEE Transactions, Vol.21, No.2, pp.275- 287, Feb. 2010.

[9] A. Manjeshwar, “TEEN: a protocol for enhanced efficiency in wireless sensor networks”, Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, USA, April 2001.

[10] Kemal Akkaya,“A survey on routing protocols for wireless sensor networks”, ELSEVIER, Ad Hoc Networks, Vol. 3, pp 325–349, 2005.

[11] Z.Fan ,“A Multi-weight Based Clustering Algorithm for Wireless Sensor Networks,” College of Computer Science & Educational Software Guangzhou University,2012.

[12] F.Awad,v”Energy-Efficient and Coverage-Aware Clustering in Wireless Sensor Networks,” Wireless Engineering and Technology, Vol. 03, No. 03, pp. 142– 151, 2012.

[13] S. Lindsey, “Data Gathering Algorithms in Sensor Networks Using Energy Metrics,” IEEE Transactions on Parallel and Distributed Systems, Vol. 13, No. 9, pp. 924–935, 2002.

[14] A. G. Delavar, “SLGC: A New Cluster Routing Algorithm in Wireless Sensor Network for Decrease Energy Consumption,” International Journal of Computer Science, Engineering and Application, Vol. 2, No. 3, pp. 1, 2012.