ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Special Issue (April)

Online - 2455-3891
Print - 0974-2441

Full Proceeding Paper

GENETIC ALGORITHM-BASED CLUSTERING OF WIRELESS SENSOR NETWORK WITH NOVEL DATA ENCRYPTION

BACHU JAYENDRA KUMAR[1], RAJYA LAKSHMI DEVI K[1], VERGIN RAJA SAROBIN M[2]*

[1]Department of Software Engineering, VIT University, Chennai, Tamil Nadu, India. [2]School of Computing Science and Engineering, VIT University, Chennai, Tamil Nadu, India. Email: verginraja.m@vit.ac.in

Received: 23 January 2017, Revised and Accepted: 03 March 2017

ABSTRACT

Wireless sensor networks (WSNs) have been used widely in so many applications. It is the most efficient way to monitor the information. There are so many ways to deploy the sensors. Many problems are not identified and solved. The main challenge of WSN is energy efficiency and information security. WSN power consumption is reduced by genetic algorithm-based clustering algorithm. Information from cluster head to base station may have a lot of chances to get hacked. The most reliable way to manage energy consumption is clustering, and encryption will suit best for information security. In this paper, we explain clustering techniques and a new algorithm to encrypt the data in the network.

Keywords: Wireless sensor networks, Encryption algorithms, Clustering, Genetic algorithm.

 DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19575

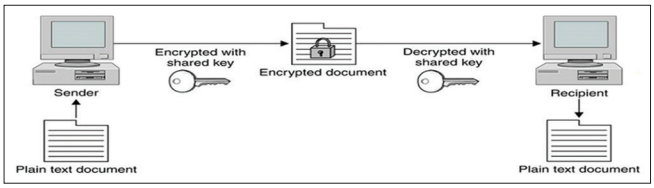
INTRODUCTION

Research in wireless sensor networks (WSNs) field has brought a revolutionary change in the usage of sensors [1]. The size, efficiency, and cost of sensors have been tremendously modified. Modern era sensors efficiency is inversely propositional to its cost and size. In general, the clusters are designed to send the gathered and processed data to the base station. However, this leads to inefficiency as each node has to individually send the data and network traffic will be high [2]. To overcome this problem, clustering method has been introduced. Group of nodes is clustered and any node will be elected as cluster head (CH). All the nodes in the cluster will send data to CH, and CH will send data to base station. One more challenge is data security, while the data will be transferred through the network; it is more prone to danger [3]. To overcome this problem, many encryption methods are used. Encryption is the formal name of scrambled process; the data that are going to be transmitted will be converted into a form which might look unintelligible to observers. Many encryption methods are used in WSN, but each has their own loopholes. This paper is organized as follows: Describes types of encryption algorithms, describes the energy consumption problem challenges, explains clustering using genetic algorithm [4], and explains random key encryption algorithm (RKEA) for encryption in clustering [5].

Types of encryption algorithms

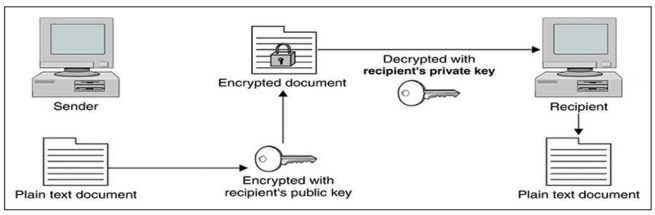
Symmetric algorithm

In this encryption algorithm, sender and receiver have the same key. Using the shared key, sender will encrypt the data and receiver will decrypt it [6]. The major drawback is that as same key is used on both the sides, it will take fraction of seconds for the intruder to hack it.



Asymmetric algorithm

In this encryption algorithm, receiver will have a private key; a public key will be derived from private key. Sender uses that public key to encrypt the data and receiver uses private key to decrypt it. As two keys are used, the chance of getting hacked is comparatively low. To enhance the security, keys can also be encrypted along with data.



Applications of WSN

In military, WSNs are used to sense the missile locations and nuclear weapons [7,8]. It is also used to detect the environmental disasters such as tornadoes and earthquakes. Modern buildings are equipped with sensors for intrusion detection.

Efficiency of sensors α_1/size

LITERATURE SURVEY

So far, for encrypting messages, algorithm has been used. In Rivest, Adi Shamir, Leonard Adleman (RSA) algorithm [9], we will use two keys (public, private). RSA algorithm is widely used because of its integrity, confidentiality, and availability. Integrity of RSA will not allow to modify the data in an unauthorized way, confidentiality will not allow unauthorized persons to access the data, and availability will make the information accessible all the time.

Drawbacks of RSA

- Intruders can penetrate and can hack the message.
- As "n" value is shared through network, it is very easy for the hackers to catch the message.
- As each node needs to store the public key and private key, it leads to huge memory usage.

To overcome the drawbacks of RSA, random key generation algorithm has been proposed.

PROPOSED WORK

To overcome the energy challenges, we can evaluate the energies of each node at specific time intervals and assign them the role of CH.

Clustering using genetic algorithm

Genetic algorithm is used to find the best chromosomes for mutation from the population. In clustering, we will use genetic algorithm for choosing CH [10]. Each cluster will have maximum of nine nodes; the fitness of each node is calculated using fitness equation [11]. If the fitness is "1," the node is capable of being as CH; otherwise, it should act as normal sensor node to collect and process data. This fitness equation was suggested by Younis *et al.* [12]. Binary representation of chromosome:

1	0	1	1	0	0	1	0	1

Fitness function [13,14]:

Fitness = weight (d1 d2) + (1 weight) (n n (ch))

d1: Sum of span length from all sensors to sink.

d2: Sum of span length from normal sensors to cluster master.

n: Count of sensors in cluster.

n (ch): Count of CH.

RKEA

To overcome the above-mentioned drawbacks, RKEA proposed. In this algorithm, key database will play a critical role of string and evaluating keys of each node, key generation will also take place inside key database, and that key will be distributed to sender and receiver node.

Algorithm:

Step 1: Sender will send<sender node name, receiver node name, and sender node key>to key database.

Step 2: Key database will validate the sender node key and generate random key "e" by invoking RKEA () algorithm.

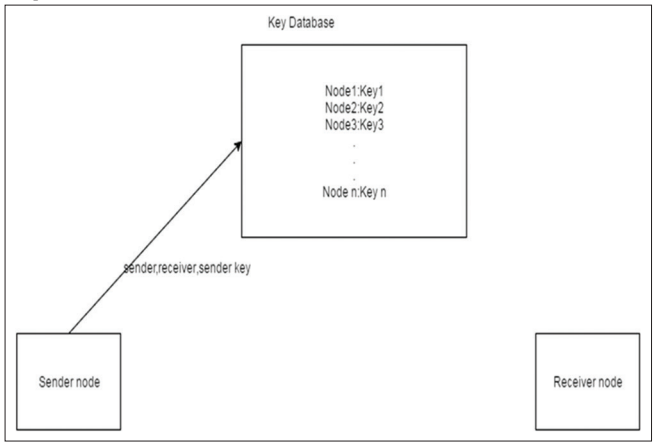
Step 3: <Sender name node, receiver name node, e>will be sent to sender and receiver nodes by key database.

Step 4: Sender will encrypt message using key "e" and send to receiver.

Step 5: Receiver will decrypt the message using key "e".

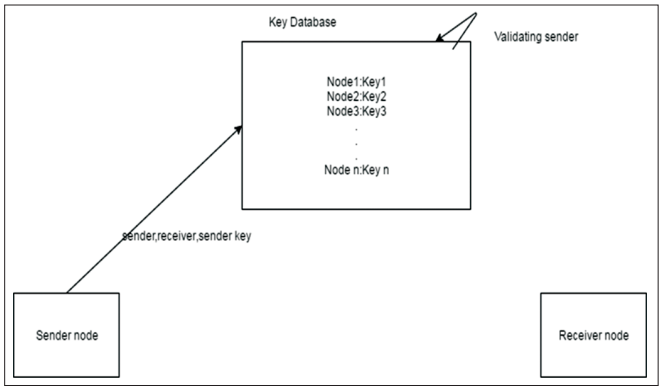
System architecture

Step 1:



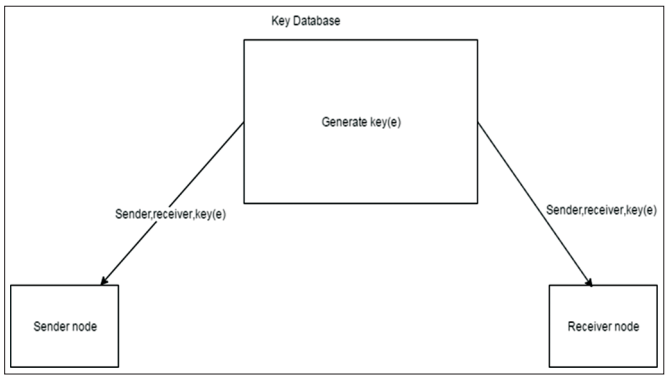
Sender requesting key database for random key by providing its key and receiver node id.

Step 2:



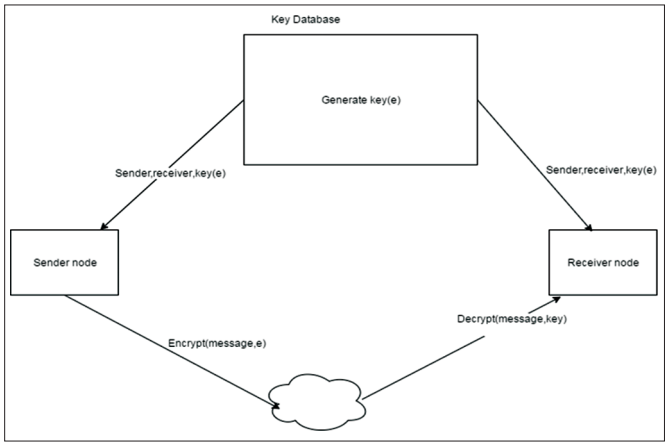
Key database performing validation of sender node.

Step 3:



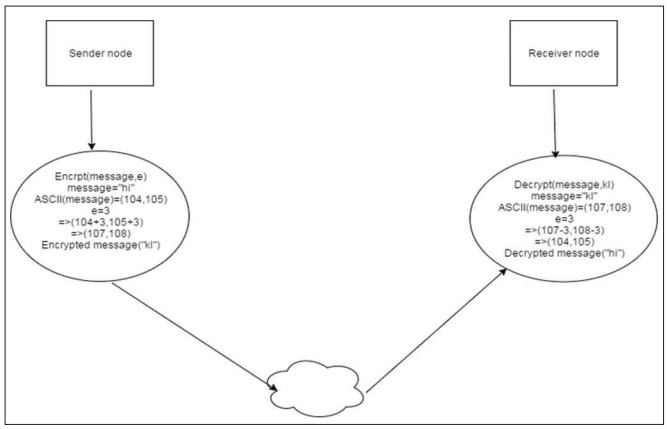
Key database generating random key and sending it to both sender and receiver node.

Step 4:



The path of encryption and decryption.

Encryption:



Nodes performing encryption and decryption function using random key.

Advantage of random key algorithm

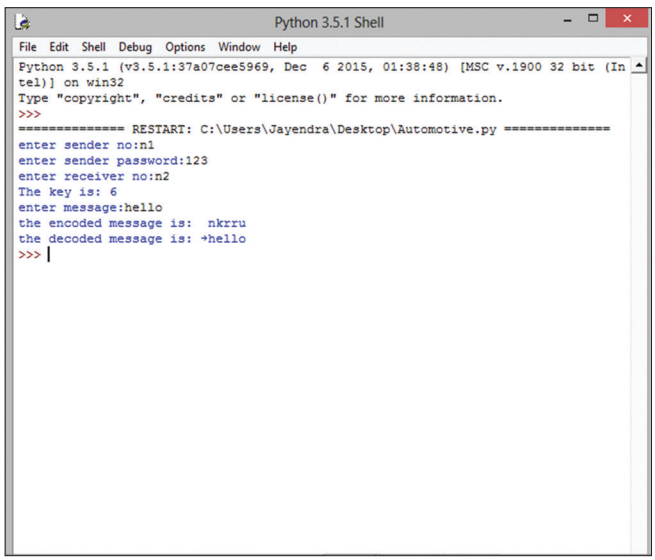
- No need to store key for every node inside local buffer of each node.
- Each key will last for only one transaction. Hence, it is impossible for intruders to hack it.

There is no ambiguity of relationships between nodes.

RESULT AND DISCUSSION

Nodes will be grouped into clusters and CH will be selected based on fitness function. Each cluster may have more than one CH. The data from the environment will be gathered and processed by sensor nodes and send to CH; CH will send it to base station. The information flow between base station and CH is secured through RKEA algorithm. CH will send its node id, password, and base station id to key database. Key database will verify sender and generates the random key and it will be send to sender and receiver.

Result of RKE algorithm:



Description of RKEA output

Sender will send his node's id, password, and receiver's id. Those will be validated by the key database. Once validated, random key will be generated by key database and send it to both sender and receiver. Then sender will perform encryption function using random key and receiver will decrypt the cipher text using the same random key.

EMPERICAL ANALYSIS

When compared with other algorithms such as RSA, data encryption standard, and HASH. RKEA provides a unique feature called "random key." The key will be valid for only one transaction. Like MD5 algorithm, it will also support key range from 8 to 128 bits. The future advancements of RKEA include hashing of key holder file in key database with salt. Perform hashing function for the possible number of times on the passwords to store it safely inside the key database without getting hacked.

CONCLUSION

As the CH changes for specific time intervals, it is impossible for a cluster to get destroyed. The fitness function calculated will give the best CH choice. Encryption of data transfer between clusters head and base station helps to achieve secure data transfer. As the key is generated randomly, the chance of getting hacked is low. No need of storing public and private keys in local database, so overhead will be low. No two transactions share same keys. The future scope of the paper is to encrypt the node key file which is stored in the key database.

REFERENCES

1. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. Elsevier Comput Netw 2002;38(4):393-422.
2. Engelbrecht A. Computational Intelligence: An Introduction. 2nd ed. England: Wiley; 2007.
3. Dai F, Li T. Tailoring Software Evolution Process, 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing; 2007.
4. Abbasi AA, Younis M. A survey on clustering algorithms for wireless sensor networks. Comput Commun 2007;30(14-15):2826-41.
5. Zhou X, Tang X. Research and Implementation of RSA Algorithm for Encryption and Decryption. In: The 6th International Forum on Strategic Technology; 2011. p. 1118-21.
6. Werner-Allen G, Lorincz K, Ruiz M, Marcillo O, Johnson J, Lees J, *et al*. Deploying a wireless sensor network on an active volcano. IEEE Internet Comput 2006;10(2):18-25.
7. Rezaei Z, Mobininejad S. Energy saving in wireless sensor networks. Int J Comput Sci Eng Surv 2012;3(1):23-37.
8. Khemapech I, Duncan I, Miller A. A survey of wireless sensor networks technology. In: PGNET, Proceedings of the 6th Annual Post Graduate Symposium on the Convergence of Telecommunications; 2005.
9. Chong CY, Kumar SP. Sensor networks: Evolution, opportunities, and challenges. Proc IEEE 2003;91(8):1247-56.
10. Hosseingholizadeh A, Abhari A. A neural network approach for wireless sensor network power management. In: Proceedings of 2nd International Workshop on Dependable Network Computing and Mobile Systems; 2009.
11. Anastasi G, Conti M, Di Francesco M, Passarella A. Energy conservation in wireless sensor networks: A survey. Ad Hoc Netw 2009;7(3):537-68.
12. Younis O, Krunz M, Ramasubramanian S. Node clustering in wireless sensor networks: Recent developments and deployment challenges. IEEE Netw 2006;20(3):20-5.
13. Zheng H, Zhou Y. A novel cuckoo search optimization algorithm base on gauss distribution. Int J Comput Inf Syst 2012;8:4193-200.
14. Tawfik AS, Badr AA, Abdel-Rahman IF. One rank cuckoo search algorithm with application to algorithmic trading systems optimization. Int J Comput Appl 2013;64(6):30-7.