JACET Journal of Advances in Computer Engineering and Technology, 2(2) 2016

An efficient solution for management of pre-distribution in wireless sensor networks

Asghar Dolatabadi[1], Hamid Haj Seyyed javadi[2]

Received (2016-04-24)
Accepted (2016-07-05)

***Abstract* — A sensor node is composed of different parts including processing units, sensor, transmitter, receiver, and security unit. There are many nodes in a sensor unit. These networks can be used for military, industrial, medicine, environmental, house, and many other applications. These nodes may be established in the lands of enemies to monitor the relations. Hence, it is important to consider conservation of communications, declaration, and key removal. The locations of nodes are not usually defined in the networks. When a secure connection is required they can be used by symmetrical or asymmetrical encodings. A node can just make secure connection, if they are in same radio range or have a common key. In dynamic wireless sensor networks compared with static networks the sensors are moveable and can be added or removed. This research makes an attempt to investigate the challenges of key management for encoding. It also tries to solve other remained problems in this field. Therefore, distribution and key management schemes supplying security and operational requirements of sensor networks are examined in fuzzy clustering and suitable protocol for key management.**

***Index Terms* — distribution key, dynamic wireless sensor networks, pre-distribution key, fuzzy system, head cluster selection.**

I. INTRODUCTION

Wireless system was developed in 1980s but it was not supplied to the public and engineers for their applications. This technology used to be covered for many years due to security, quality, high costs, and some weaknesses. After many years, the technology was revolutionized and is now used with sensors as a connection between physical world and information systems. The focus of this research is on the management of key in wireless sensors and pre-distribution algorithms. The purpose of this study is to investigate the pre-distribution key methods and to evaluate their weaknesses and strengths[1].

In this research, the main focus is on many kinds of key management methods in wireless sensor networks[2], particularly key pre-distribution algorithms. This is because of the fact that these methods have lower computational and communicative loads. The main objective of this research is to investigate some of the key pre-distribution methods and evaluation of the weaknesses and strengths. We have, then, presented a hybrid mechanism to make pre-distribution of the keys in wireless sensor networks. This method has improved a integration scheme as a method of pre-distribution. After this evaluation, we have evaluated the applicability of the suggested methods in real environment and regulated network parameters to get desired values for efficiency evaluation parameters. Some of the parameters are scalability, unification, and memory and energy consumption. Then, the lower boundary has been extracted to examine the radio ability of the nodes so that it allows the network to continue its operation. In case of application of the suggested key in a real network, it has to

1- Department of Computer, Buinzahra Branch, Islamic Azad University, Buinzahra, Iran
2- Department of Mathematics and Applications, Shahed University, Tehran, Iran (hamid.h.s.javadi@gmail.com)

be unified and secure. It is clear that these key management schemes have different advantages and disadvantages. With the huge number of these schemes, it would be so difficult by a typical user to compare them for selection of the most proper protocol.

Other issues include those relevant in specific applications such as health care networks [3], the problem of security attacks [4], anomaly detection [5]. WSN's face multiple threats and these include: communication attack; denial of service attack; node compromise; impersonation attack; and protocol-specific attack

II. CONCEPTS

A fuzzy concept is a concept of which the boundaries of application can vary considerably according to context or conditions, instead of being fixed once and for all. This means the concept is vague in some way, lacking a fixed, precise meaning, without however being unclear or meaningless altogether. It has a definite meaning, which can become more precise only through further elaboration and specification, including a closer definition of the context in which the concept is used. A fuzzy concept is understood by scientists as a concept which is "to an extent applicable" in a situation, and it therefore implies gradations of meaning. The best known example of a fuzzy concept around the world is an amber traffic light, and indeed fuzzy concepts are nowadays widely used in traffic control systems. The Nordic myth of Loki's wager suggests that concepts which lack a precise meaning or precise boundaries of application cannot be usefully discussed at all. However, the idea of "fuzzy concepts" proposes that "somewhat vague terms" can be operated with, since we can explicate and define the variability of their application, by assigning numbers to it[1].

A FLS consists of four main parts: fuzzier, rules, inference engine, and defuzzier. The process of fuzzy logic is explained in Algorithm: Firstly, a crisp set of input data are gathered and converted to a fuzzy set using fuzzy linguistic variables, fuzzy linguistic terms and membership functions. This step is known as fuzzication. Afterwards, an inference is made based on a set of rules. Lastly, the resulting fuzzy output is mapped to a crisp output using the membership functions, in the defuzzi_cation step.

Linguistic variables are the input or output variables of the system whose values are words or sentences from a natural language, instead of numerical values. A linguistic variable is generally decomposed into a set of linguistic terms.

III. METHODOLOGY

In the following, we briefly introduce the basic theory of Fuzzy used in cluster formation of our propositions, and then we give a detailed description of the proposed approaches.

There are many techniques for decoding[6-7]. Standard encoding algorithm (RSA) is used in this research as a symmetric key management method to codify the key values by system functions. This research based on purpose is an applied study. The execution of the scheme is to cover security and management defects[1].

Membership functions are used in the fuzzication and defuzzication steps of a FLS, to map the nonfuzzy input values to fuzzy linguistic terms and vice versa. A membership function is used to quantify a linguistic term.The evaluations of the fuzzy rules and the combination of the results of the individual rules are performed using fuzzy set operations. The operations on fuzzy sets are diferent than the operations on nonfuzzy sets.

In this section we describe our key management approach. Our approach is a post-deployment key management scheme which deal scalability and flexibility issues and is resistant to node capture attacks.

in this research, we have used a key management system to decode message after receiving the cluster node by the private key. Thus, an asymmetric decoding has been used and the number of keys has also been determined by functions. We have attempted to employ an appropriate protocol to make clustering via fuzzy logic and key management protocol. The suggested algorithm of this study would be tested in MATLAB. Hence, to evaluate the security in data transfer, we have also used MATLAB software due to its high accuracy in simulation. The algorithms of this study have also been prepared in MATLAB.

IV. RESULTS

Two parts are of great importance in this paper for key management; 1) clustering, 2) encoding protocol. The first is based on fuzzy logic and the second requires more security.

The suggested fuzzy system of this research is based on selection of nodes. In the fuzzy system, the priorities for selection of nodes are based on the inputs.

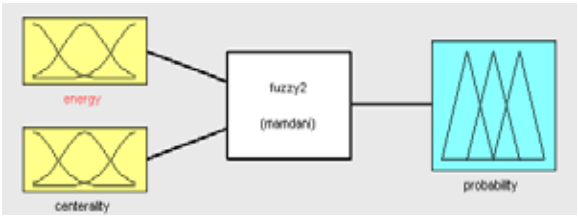

Figure 1 : suggested fuzzy system

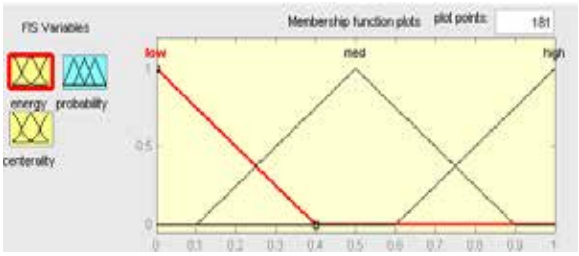

Figure 2: the first input of the fuzzy system

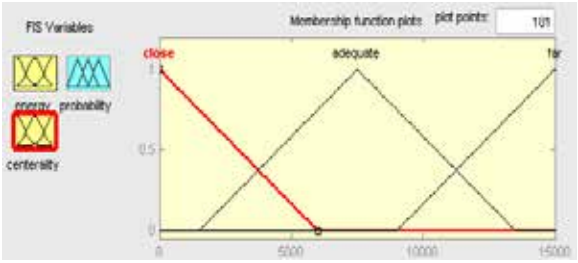

Figure 3: the second input of fuzzy system

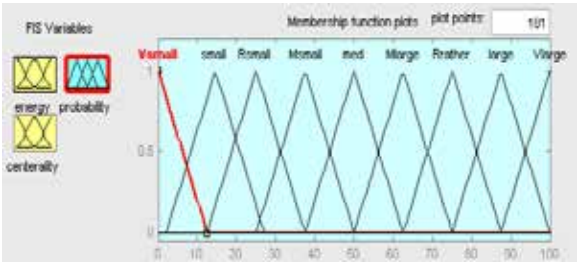

Figure 4: output of the fuzzy system

There are effective parameters for cluster decision maker system. The volume of calculations is based on standard measurements, for example, the traffic volume is 300kb/s. Another criterion is suitable distribution. In this method, t=a node that was not selected in the previous stages can be selectable here. The belonging function can examine the output. The threshold value is 0.5 for the output.

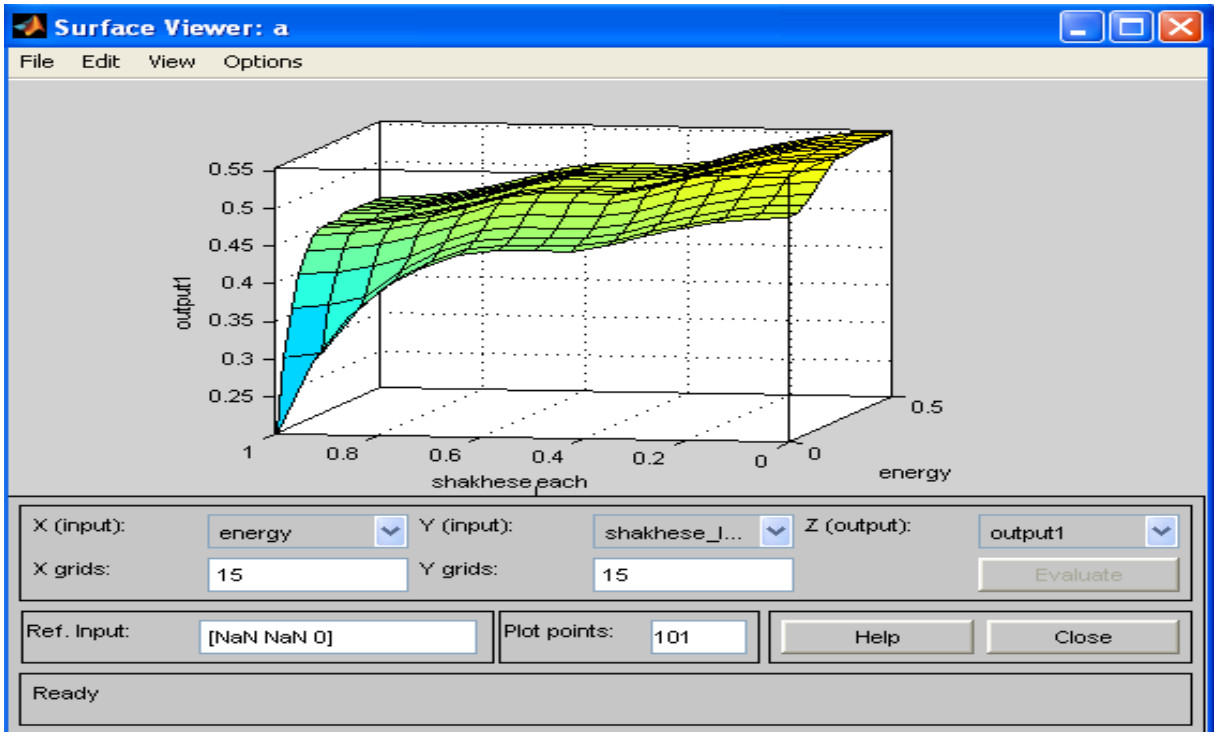

Figure 5: fuzzy graphs

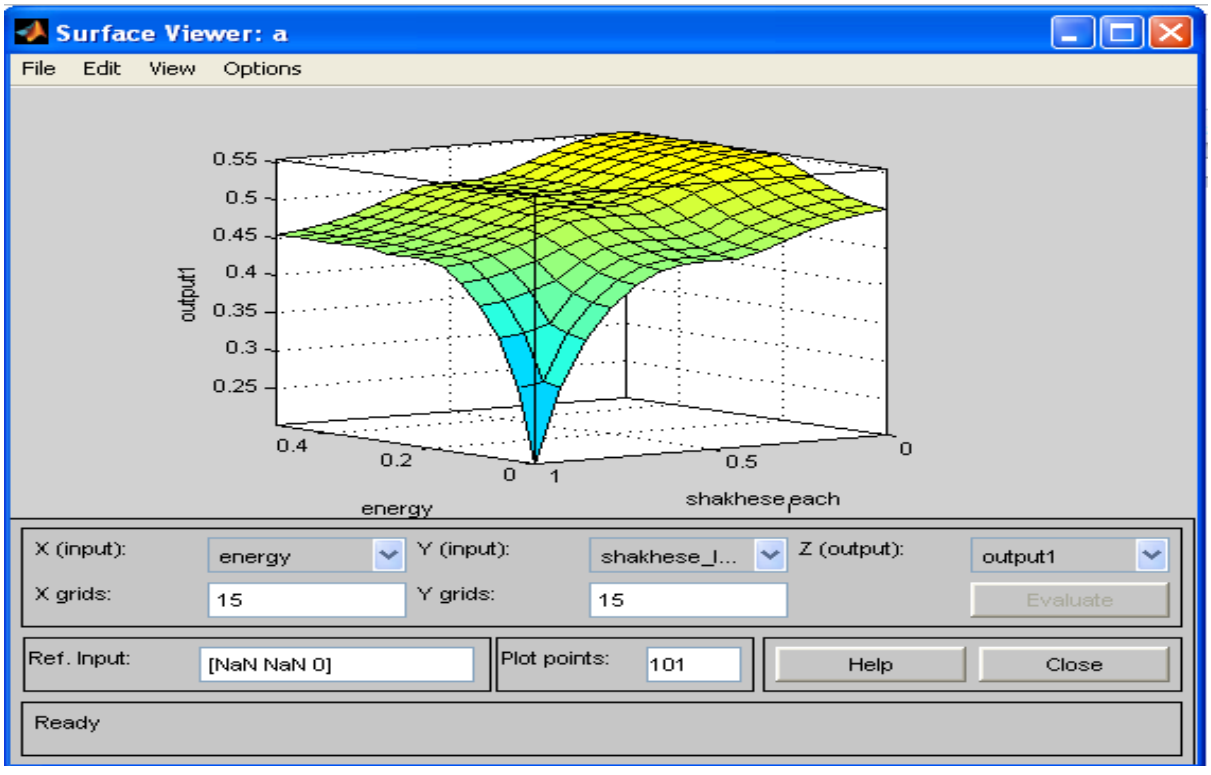

Figure 6: designed fuzzy graphs

The simulation with 10 nodes and 2 head clusters are arranged so that the locations of nodes are determined randomly but the head clusters are determined constantly. In this simulation, there are 10 active nodes and the nodes are constant in every 20 stages. In this simulation, the selection for servers is considered to be 3 as the best head cluster in terms of fuzzy. Fuzzy algorithm is compared with head cluster Leach algorithm. Therefore, execution of the simulation gives the following results.

There are two improvements in the accuracy and ability of this system compared with the previous ones. These improvements made in the key management systems through this research are traffic load improvement and energy improvement. Traffic volume is computed by random functions and traffic load is also calculated by all the data transmitted from between the nodes.

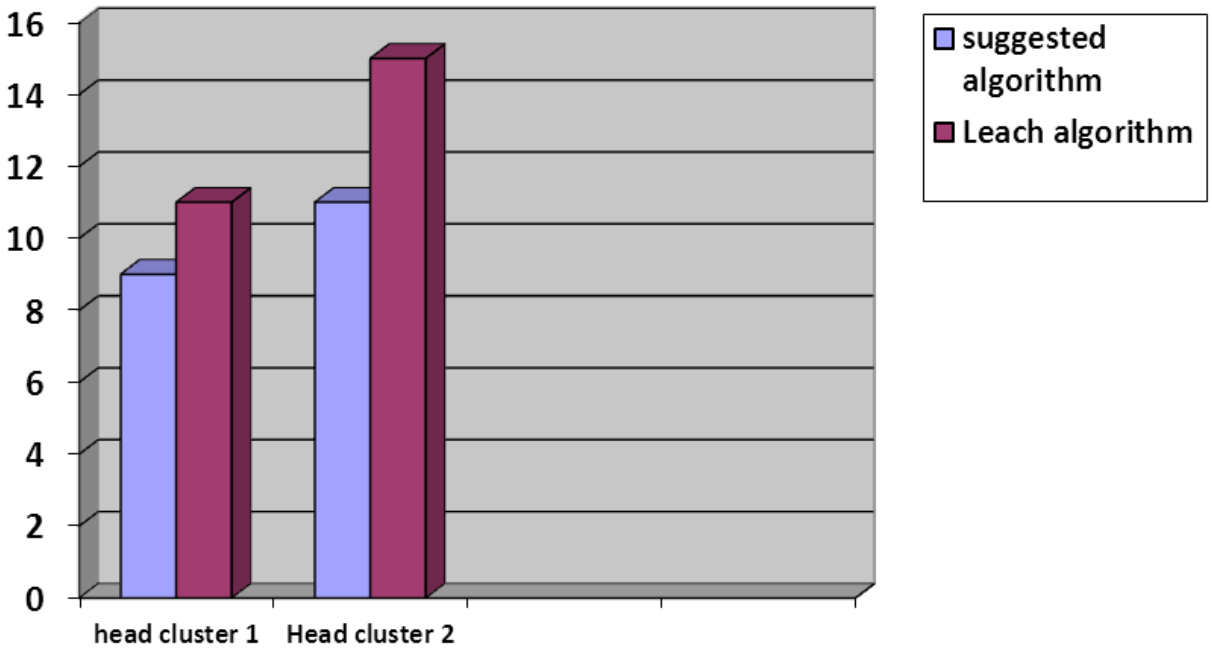

Figure 7: leach algorithm and clusters; this shows traffic and energy (Wat) in vertical axis

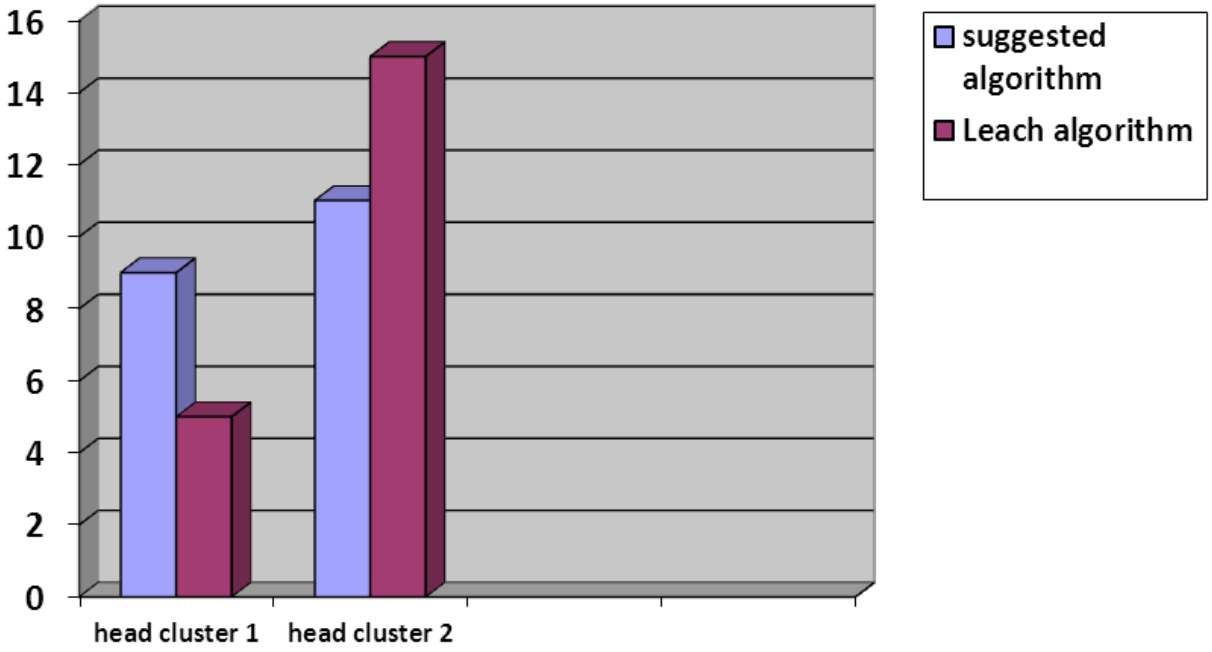

Figure 8: leach algorithm and clusters

Wireless sensor networks are composed of a variety of sensors. Each sensor usually constraints the capabilities such as power, calculations, storage, sensing, and connection[8][9]. Among the variety of public key management models, eclipse curve encoding is based on the algorithms with acceptable advances in performances of the sensor nodes in the networks of loser energy. The public key encodings have better results in 8 bit platforms. Confirmation of identity in such scheme requires high bandwidth and more power. For more efficiency, we can use general encoding keys. In this paper, we have presented a key management system based on encoding by public keys. This scheme can create a suitable level of security in the network. These can be used for the resources in wireless sensor networks based on encoding system using identification in simplified networks. This scheme has also been compared with similar schemes such as s-pksec. There are some kinds of key systems for this solution; these keys are confidential key systems, derivative keys, codifier keys, and settling keys. The confidential key systems use just one key for encoding and decodings. The Data Encryption Standard (DES) is an example of these confidential keys. Key management is often difficult due to many different keys for handling. A method for simplification is to have derivatives of these keys. Another form of the derived keys is use of token as electric calculators. These tokens are usually used to get access to secure computer systems.

As key sending is a drawback in security issues, it is better to use the keys in codified form. Key domain is used to constrain the key fields that are almost locally reserved. Therefore, the keys ranged in domain are transmitted from an area to another. To limit the valid time for the keys a new key can be added for each settling.

Suggested method for relation protocol in key management

The suggested scheme is stated step by step. After clustering and selection of appropriate nodes for key management, operations amongst the nodes of each cluster are as following:

1. before establishment, the base station assigns unique ID and the related Key (K) of each node to them. The ID is written in the memory of the nodes; the key of each node is written in the memory of the head cluster.

2. after establishment, control messages are initially transmitted to all the nodes from the main station. The places are in different levels. The main station makes the level equal to 0. When a node send a message to its neighboring node, it loses the greater message transmitted from the main station. Here the level reaches 1. Thus, the value of each level indicates the number of nodes along the distance to the main station. A sensor node considers all the nodes that their level is one unit lower than their own level as parent node and also all those that their level is higher as child.

3. each sensor node sends its unique ID code to cluster node and registers all the IDs received.

4. the node of sensor i collects its own data. The node sensor adds its own ID to the data. Then, using the ID of parent node (IDi -1), the data are presented as (Data, IDi). The codified message is sent with sensor node of IDi -1 to be hidden. A sensor with IDi -1 and with message IDi(E_{IDi-1}) can use a parent node with IDi -2 for encoding of the message. The message is repeated to the codified message reach the station.

5. the head cluster station receive the de-codified

$E_{ID0}(...E_{IDi-2}(E_{IDi-2}(ID_i, Data)))...)$message. The key k_0 is used as ID_0 for de-coding.

$$D_{K0}(E_{ID0}(...E_{IDi-2}(E_{IDi-1}(ID_i,Data)))...)) = E_{ID2}(...E_{IDi2}(E_{IDi-1}(ID_i,Data)))...)$$

After that, it uses base station with the key k_1 with ID1 for this de-coding.

$$E_{ID2}(...E_{IDi-2}(E_{IDi-1}(IDi,Data)))...)$$
$$D_{K2}(E_{ID2}(...E_{IDi-2}(E_{IDi-1}(ID_i,Data)))...)) = E_{ID2}(...E_{IDi2}(E_{IDi-2}(ID_i,Data)))...)$$

This is repeated until the cluster station receives i data.

6. Comparison

To get the public key, each node can just transmit its unique ID to its child node. Thus, this scheme has lower energy consumption relative to security architecture based on asymmetric s-pksec and pair keys. Thus, the s-pksec is more economic than the SSL scheme. Thus, s-pksec is more economical than SSl. The suggested security architecture is based on an encoding system of ID. This is essentially based on

encoding security architecture of the public key. To increase the security in encoding of the public key higher than the private key, it is not required to transfer the public key. They are all reserved in the memory. For key pre-distribution scheme, the key consistency stage is required for universal key distribution. However, it is not necessary in this scheme. In comparison with security architecture, this scheme has lower computation costs. For the designed security architecture, it is not necessary to have two way key alterations. In primary key distribution scheme, each key should have a unique ID and related key for storage. But, in this scheme just one ID can be saved and this has lower costs for storage relative to the pre-distribution.

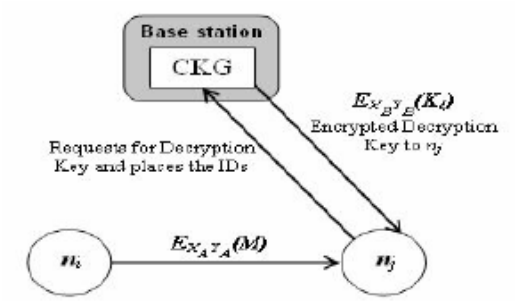

Figure 9: encoding and decoding by node connections

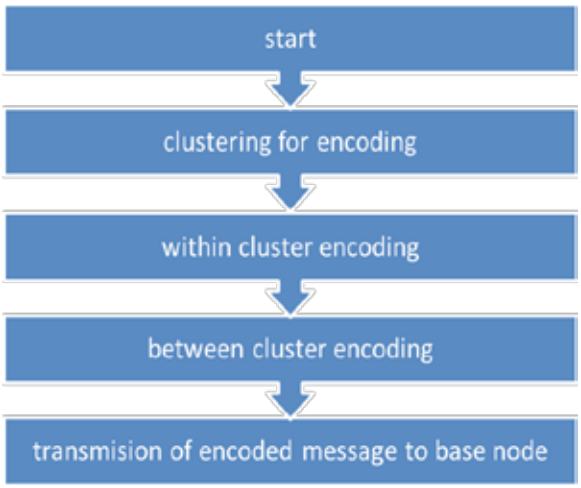

Figure 10: the suggested algorithm in this study

V. CONCLUSION

The scheme is to cover security and management disadvantages. Hence, we have considered a message sending software and executed in MATLAB. By using this platform, we are not limited to a particular platform. A simple security algorithm uses encoding algorithm to conserve information using key management. The suggested approaches in this study are successfully executed to securely transmit the key messages. A new combination of algorithms is suggested in this research for safe message transmit.

REFERENCE

[1] M. Ge, K.-K. R. Choo, H. Wu, and Y. Yu, "Survey on key revocation mechanisms in wireless sensor networks," Journal of Network and Computer Applications, vol. 63, pp. 24-38, 2016.

[2] M. G. Ball, B. Qela, and S. Wesolkowski, "A Review of the Use of Computational Intelligence in the Design of Military Surveillance Networks," in Recent Advances in Computational Intelligence in Defense and Security, ed: Springer, 2016, pp. 663-693.

[3] H. Alemdar and C. Ersoy, Wireless sensor networks for healthcare: A survey. Computer Networks, vol 15, pp. 2688-2710, 2010.

[4] C.Chen and H. Chao, A survey of key distribution in wireless sensor networks, Security and Communication Networks, 2011.

[5] M. Xie et al., Anomaly detection in wireless sensor networks: A survey. Journal of Network and Computer Applications, vol 34, pp.1302–1325, 2011.

[6] M. Simplcio, P. Barreto, C. Margi, and T. Carvalho, "A survey on key management mecha nisms for distributed wireless sensor networks," Computer Networks, vol.54, no.15, pp.2591- 2612, 2010.

[7] N. Islam and M. Moyeen, "An Empirical Study on Key Management Schemes of Wireless Sensor Network," group, vol. 134, 2016.

[8] C. Chen and H. Chao, "A survey of key distribution in wireless sensor networks,"Security and Communication Networks, 2011.

[9] V. Shnayder, M. Hempstead, B.-r. Chen, G. W. Allen, and M. Welsh, "Simulating the power the 2nd international conference on Embedded networked sensor systems, pp.188200, ACM, 2004.