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

A Combinational Advance via Matrix Based Pairwise Key Establishment and Post Deployment Approach in WSN

Shivani Dilwariya [1], Prof. Vijay Prakash Singh[2]

M.Tech Student, Dept. of Electronics and Communication, SSSIST, Sehore, India[1]

Professor, Dept. of Electronics and Communication, SSSIST, Sehore, India[2]

ABSTRACT: Key distribution method has always played a essential role in the security of wireless sensor networks (WSNs). In this investigate work we spotlight chiefly on the security characteristic of WSN . We have urbanized a customized key distribution method which uses the thoughts of post as well as pre distribution method and therefore have demonstrated to be a enhanced substitute then the rest of two methods. Simulation study has been accepted out by means of matlab . The attempt turned out to be fruitful as our customized method illustrated less dead nodes for each round of data transport as compared to post deployment method.

KEYWORDS: Key establishment ,Security, Key prioritization, Mobile sensor networks, Post-deployment knowledge.

I. INTRODUCTION

Distributed sensor networks have established a lot of interest newly due to its large applications in military as well as civilian operations. Example applications comprise targettracking, scientific investigation, and data attainment in dangerous environments. The sensor nodes are characteristically small, less expensive, battery powered, and extremely resource constrained. They typically exchange a few words with each other throughout wireless links.Security services such as verification and key organization are significant to protected the communication among sensor nodes in aggressive environments. As one of the most basic security services, pairwise key establishment facilitates the sensor nodes to exchange a few words firmly with each other using cryptographic methods. On the other hand, due to the resource restrictions on sensor nodes, it is not possible for them to utilize traditional pairwise key organization methods such as key distribution center(KDC) and public key cryptography .

As an alternative of the above two methods, sensor nodes may set up keys among each other during key predistribution, where keying resources are pre distributed to sensor nodes earlier than deployment. As two tremendous cases, one might setup a global key between the system so that two sensor nodes know how to set up a key based on this global key, or allocate every sensor node a single random key with every one of the other nodes. On the other hand, the previous is helpless to the compromise of a particular node, and the later introduces massive storage overhead on sensor nodes.

Eschenauer and Gligor projected a probabilistic key predistribution method newly forpairwise key establishment [Eschenauer and Gligor 2002]. The chief thought is to let every sensor node arbitrarily choose a set of keys from a key pool previous to the deployment so that any two sensor nodes contain a certain possibility to share at least one ordinary key. Chan et al.additional comprehensive this thought and urbanized two key predistribution methods: a q –composite key predistribution method and a random pairwise keys method [Chan et al. 2003]. The q -composite key predistribution too uses a key pool but needs two nodes analyze a pairwise key from at least q predistributed keys that they split. The random pairwise keys method arbitrarily picks pairs of sensor nodes and assign every pair a distinctive random key.Both scheme get better the security over the essential probabilistic key predistribution method.On the other hand, the pairwise key organization difficulty is still not completely solved. For the essential probabilistic and the q -composite key predistribution methods, as the number of compromised nodes enlarges, the portion of affected pairwise keys increases rapidly. As a outcome,a small number of compromised nodes might influence a large portion of pairwise keys. Although the random pairwise keys method does not undergo from

DOI: 10.15680/IJIRCCE.2016. 0404075

the above security trouble, given a memory restriction, the system size is strictly inadequate by the preferred possibility that two sensor nodes contribute to a pairwise key, the memory accessible for keys on sensor nodes, and the no. of neighbor nodes that a sensor node can be capable to exchange a few words with.

In this thesis, we expand a number of key predistribution methods to deal with the above troubles. We first expand a general structure for pairwise key organization based on the polynomial based key predistribution procedure in [Blundo et al. 1993] and the probabilistic key allocation in [Gligor and Eschenauer 2002; Chan et al. 2003]. This structure is called polynomial pool based key predistribution, which uses a polynomial pool in its place of a key pool in [Eschenauer and Gligor 2002; Chan et al. 2003]. The secrets on every sensor node are created from a subset of polynomials in the pool. If two sensor nodes contain the secrets created from the equivalent polynomial, they can set up a pairwise key based on the polynomial based key predistribution method. All the preceding methods in [Blundo et al. 1993; Eschenauer and Gligor 2002; Chan et al. 2003] can be measured as special instances in this structure.

By instantiating the mechanism in this structure, we further expand two novel pair-wise key pre distribution methods: a random subset assignment method and a hypercube-based method. The random subset assignment method allocate every sensor node the secrets created from a random subset of polynomials in the polynomial pool. The hypercube-based method assembles polynomials in a hypercube space, allocates each sensor node to a exclusive synchronize in the space, and gives the node the secrets created from the polynomials correlated to the resultant coordinate. Based on this hypercube, every sensor node can then recognize whether it can directly set up a pairwise key with a further node, and if not, what middle nodes it can make contact with to indirectly set up the pairwise key.Our examination point to that our new methods have some pleasant features compared among the preceding techniques. In particular, when the portion of compromised protected links is fewer than 60%, known the similar storage constraint, the random separation assignment method provides a significantly high possibility of establishing protected communication among non-compromised nodes than the preceding methods. Furthermore, except the number of compromised nodes allocation a ordinary polynomial go beyond a threshold, compromise of sensor nodes does not direct to the revelation of keys recognized among non-compromised nodes by means of this polynomial.

In the same way, the hypercube-based method also has a number of attractive properties. Initial,it assurances that any two nodes can set up a pairwise key while there are no compromised nodes, supplied that the sensor nodes can exchange a few words with each other. Next, itis flexible to node compromise. Still if a number of sensor nodes are compromised, there is still a high possibility to re-establish a pairwise key among non-compromised nodes. Third,a sensor node can directly establish whether it can set up a pairwise key by another node and how to calculate the pairwise key if it can. As a outcome, there is no communiqué overhead throughout the detection of directly communal keys. valuation of polynomials is necessary to the planned methods, because it affects the presentation of calculating a pairwise key. To decrease the calculation at sensor nodes, we present an optimization method for polynomial valuation. The fundamental idea is to calculate numerous pieces of key fragments over some particular finite fields such as F28 + 1 and F216 + 1 and concatenate these fragments into a regular key. A pleasant property supplied by such finite fields is that no separation is required for modular development. As a consequence, valuation of polynomials can be achieved efficiently on low price processors on sensor nodes that do not have separation directions. Our investigation designates that such a scheme only to some extent declines the uncertainty of the keys.

II. ALGORITHM FOR ACCOMPLISHMENT OF KEY PRE DI STRIBUTION METHOD

The basic algorithms for key predistribution method for matrix based scheme can be written as below:-

1. Select ‘N’ independent key seeds chosen as s_1 , s_2, s_3, …..$s_{N.}$
2. Suppose their id’s be id_1,id_2,id_3,id_4,id_5,id_N
3. Consider a matrix h as per [1].
4. Generate a lambda x lambda matrix as per [1].
5. Compute matrix A as per [1].
6. Create keys and transmit keys to every node.
7. Every node will then broadcast packets to BS via other nodes according to matrix A and by the help of keys stored.
8. Since keys are distributed and broadcasted to every nodes in progress this technique is called as key pre distribution.

9 This method has been applied for 100 nodes and for 100 rounds of information packets and the outcome are as below :-

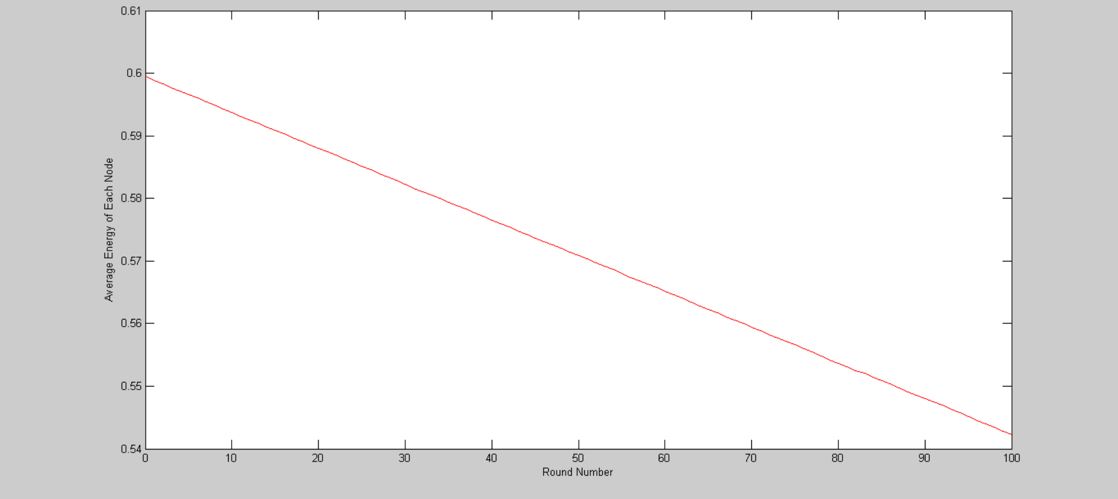

Fig 1. Average energy spent for each round for key predistribution method

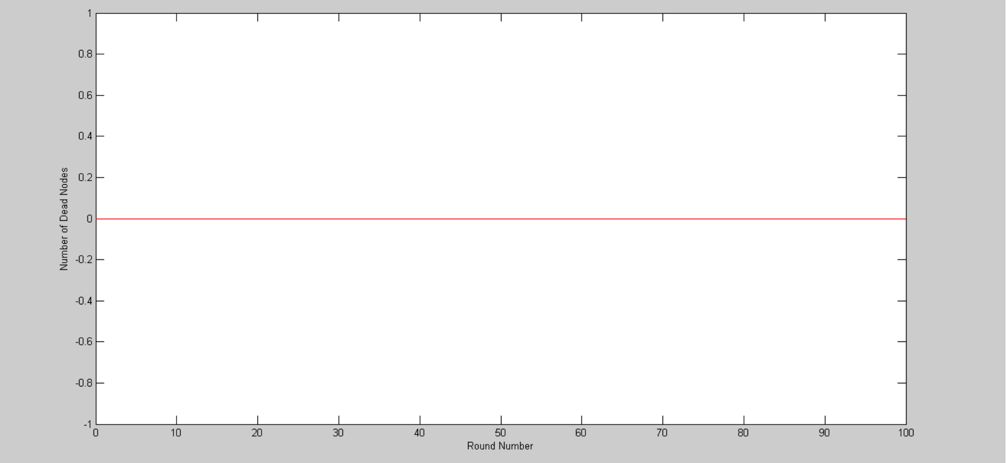

Fig 2. Number of dead nodes per round for key predistribution method

III. **ALGORITHM FOR ACCOMPLISHMENT OF POST DEPLOYMENT INVESTIGATION**

In this technique as per given in [2] basic steps are as below :-

1. ‘m’ key units are created by the scheme in a set of ‘M’ , such that every node can store a maximum of ‘m’ key units.
2. A single id is assigned to every node.
3. Every ‘m’ key units are arbitrarily distributed to every node.
4. Then nodes are positioned physically and their positions are determined by gps and this information is called as their unique position.
5. Previous to distributing keys the positions are also determined arbitrarily and connected with every node.
6. Then every node will conclude the distance among other nodes and subsequently the key will be communal as per [2].
7. Since the keys are not broadcasted as exposed in [1] this technique is referred to a post deployment investigation.

The outcome for this algorithm in provisions of energy and dead nodes per round are given as below:-

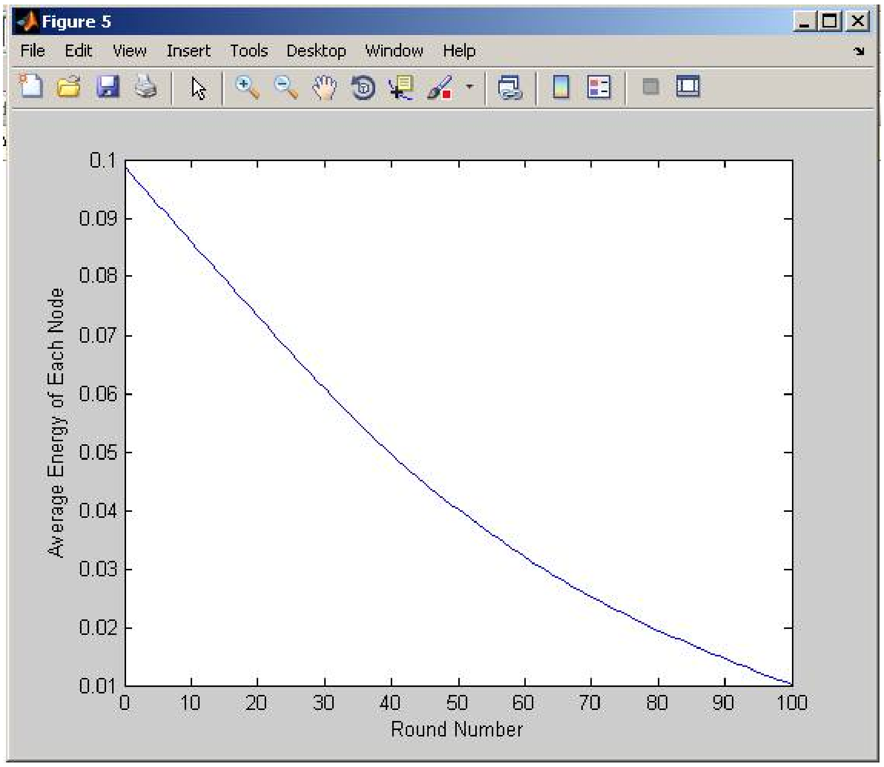

Fig. 3. Average energy spent for each round for post deployment scheme

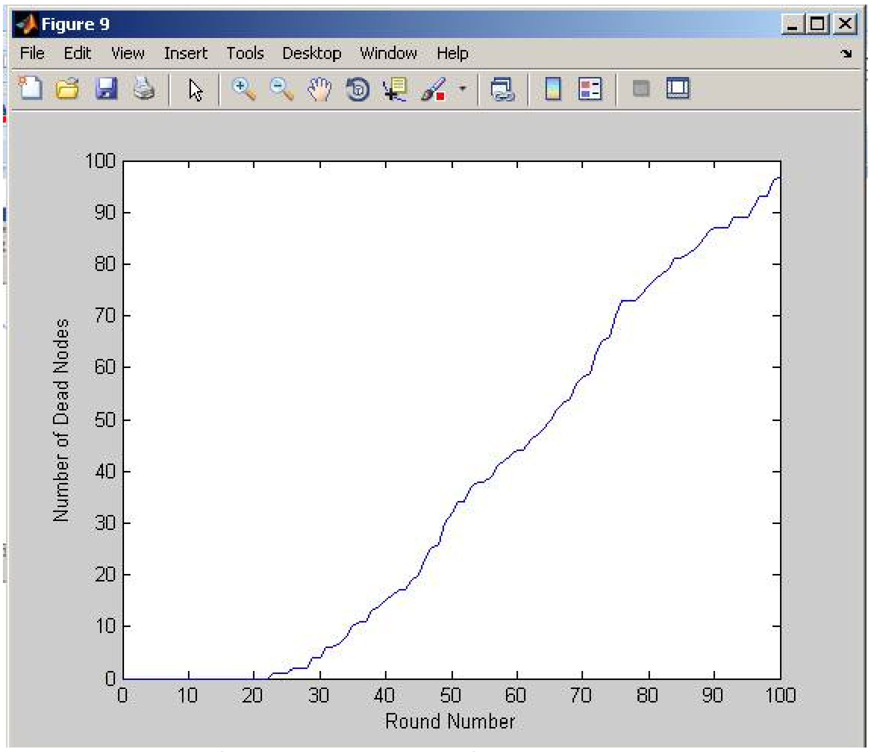

Fig 4. No. of dead nodes per round for post deployment scheme

IV ALGORITHM FOR CUSTOMISED APPROACH

In our work we have mutual the profits of the above two methods and then imitation the whole setup for 100-400 rounds of data transport. The fundamental steps concerned in our advance are as follows:-

1. We have unspecified that the location of nodes are not determined in progress contrary to pre distribution method and thus the position of the nodes are determined by gps except this time the information is transmited to base station.
2. The base station then depending on the position of every node will transmit the key matrix to every node as per in [1].
3. This dispersed common matrix will be used by all the nodes to create further key for communication.
4. Every node then will establish the distance among other nodes as per [2].
5. This information is then used for efficient communication that is the node will not transmit the information, quite the information will be transmited form one node to other like in HWSN.
6. The LEACH clustering approach has been organized for further data transport.
7. Since the message is broadcasted form one node to another the generally dead node incidence is appreciably condensed and hence the data transport gets complete with no overloading the nodes.
8. Various simulation results for the said scheme are as given below:-

Figure 5 to 8 represents the simulation results for customised algorithm for 100 to 400 rounds

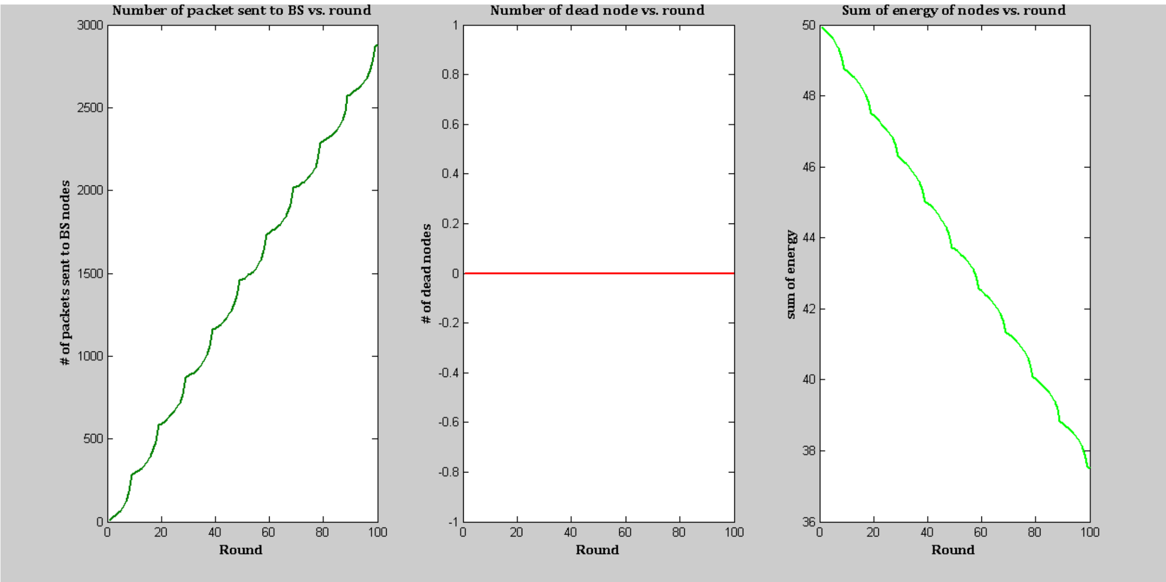

Fig 5. Simulations outcome for customized algorithms for 100 rounds

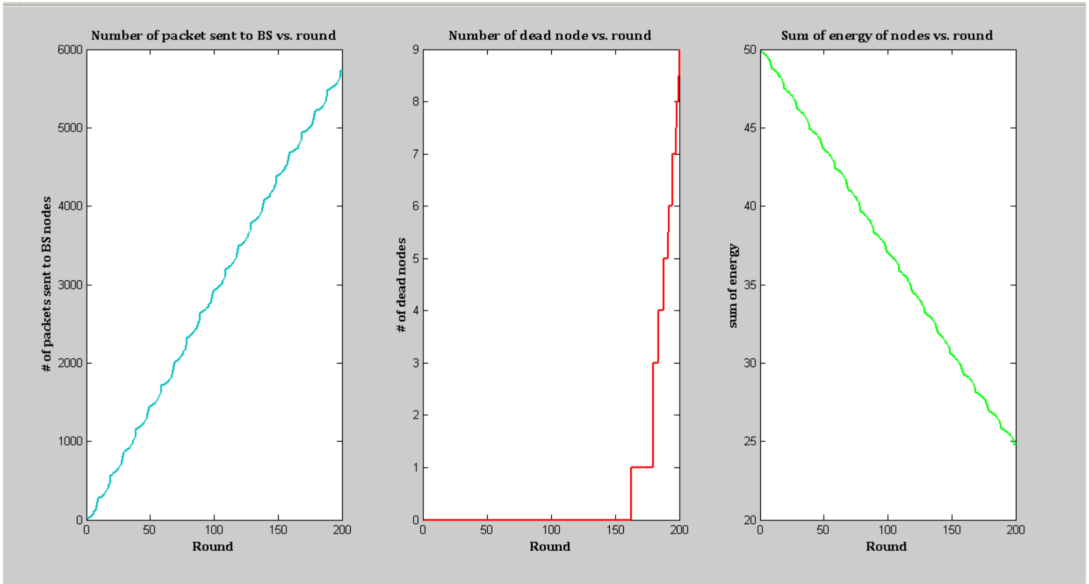

Fig 6. Simulations outcome for customized algorithms for 200 rounds

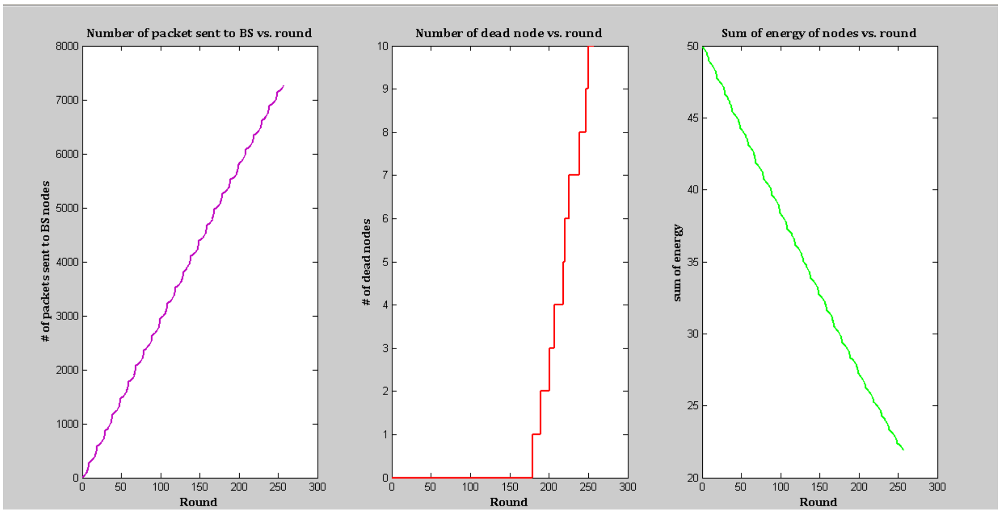

Fig 7. Simulations outcome for customized algorithms for 300 rounds

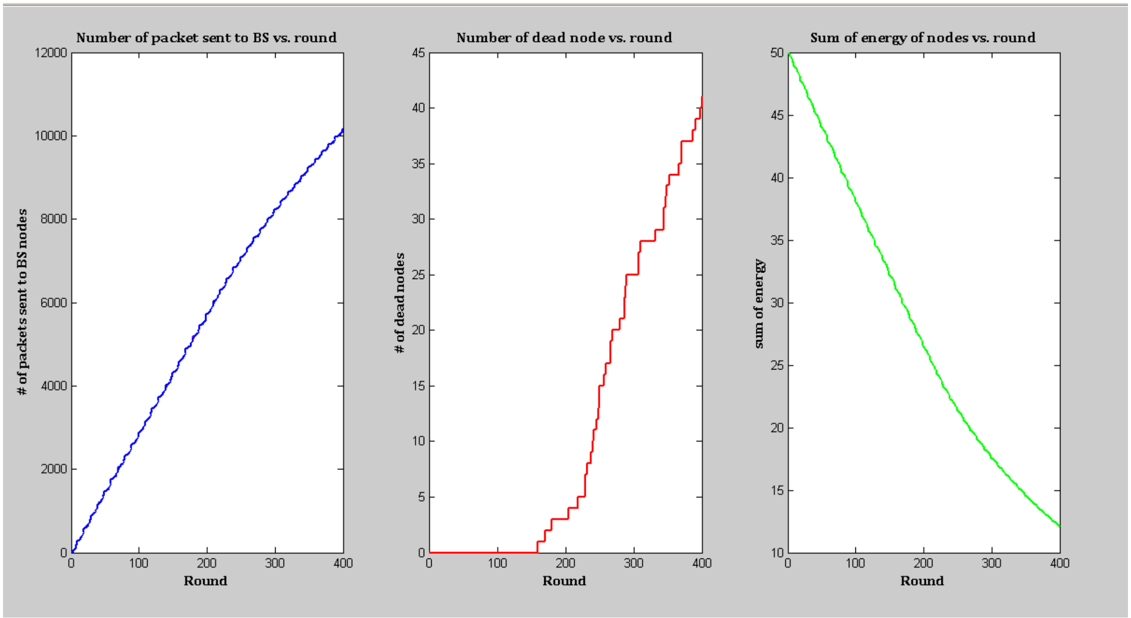

Fig 8. Simulations outcome for customized algorithms for 400 rounds

V. CONCLUSION

In this investigate work, we urbanized a general structure for polynomial pool-based pair wise key predistribution in sensor systems based on the fundamental polynomial-based key pre distribution in [1]. This structure permits study of numerous instantiations of probable pair wise key establishment methods. Based on this structure, we urbanized two definite key predistribution methods: the random subset task methods and the hypercube-based key predistribution method. Our examination of these methods specify that both methods have important advantages over the accessible approaches. The accomplishment and experimental outcome also reveal the practicality and effectiveness in the current generation of sensor networks. Numerous investigate directions are significance investigating. Foremost, we watch sensor node contain low mobility in a lot of applications. Therefore, it can be advantageous to expand position sensitive key predistribution methods to develop the possibility for neighbor nodes to share common keys and at the same decrease the hazard of compromised nodes. Second, it is dangerous to notice and/or withdraw compromised nodes from an operational sensor system.

It has been revealed in the outcome investigation that the post deployment analysis method given in [2] ahs chief disadvantages in terms of no. of dead nodes per round of data transport , our outcome are enhanced then both the approaches but numerous mathematical models are still require to be prepared , hence this work has to accomplished in the expectations to keep away from any dis ambiguousness in the investigate literature.

REFERENCES

[1] Wireless Integrated Network Sensors, University ofCalifornia, Available: http://www.janet.ucla.edu/WINS.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, andE. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002[3] R. Anderson and M. Kuhn. Tamper resistance - a cautionarynote. In Proceedings of the Second Usenix Workshop onElectronic Commerce, pages 1–11, November 1996.

[4] R. Blom. An optimal class of symmetric key generationsystems. Advances in Cryptology: Proceedings ofEUROCRYPT 84 (Thomas Beth, Norbert Cot, and IngemarIngemarsson, eds.), Lecture Notes in Computer Science,Springer-Verlag, 209:335–338, 1985.

[5] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro,and M. Yung. Perfectly-secure key distribution for dynamicconferences. Lecture Notes in Computer Science,740:471–486, 1993.

[6] D. W. Carman, P. S. Kruus, and B. J. Matt. Constraints andapproaches for distributed sensor network security. NAI LabsTechnical Report #00-010, available athttp://download.nai.com/products/media/nai/zip/nailabs-report-00-010-final.zip,2000.

[7] H. Chan, A. Perrig, and D. Song.Random keypredistribution schemes for sensor networks. In IEEESymposium on Security and Privacy, pages 197–213,Berkeley, California, May 11-14 2003.

[8] W. Diffie and M. E. Hellman.New directions incryptography. IEEE Transactions on Information Theory,22:644–654, November 1976.

[9] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney. Akey management scheme for wireless sensor networks usingdeployment knowledge. Technical Report, SyracuseUniversity, July 2003. Available fromhttp://www.cis.syr.edu/~wedu/Research/paper/ddhcv03.pdf.

[10] Erd˝os and R´enyi. On random graphs I. Publ. Math.Debrecen, 6:290–297, 1959.

[11] L. Eschenauer and V. D. Gligor.A key-management scheme for distributed sensor networks. In Proceedings of the 9thACM conference on Computer and communications security , November 2002.

[12] J. M. Kahn, R. H. Katz, and K. S. J. Pister. Next centurychallenges: Mobile networking for smart dust. InProceedings of the 5th Annual ACM/IEEE InternationConference on Mobile Computing and Networking(MobiCom), pages 483–492, 1999.

[13] F. J. MacWilliams and N. J. A. Sloane.The Theory ofError-Correcting Codes. New York, NY: Elsevier Science Publishing Company, Inc., 1977.

[14] D. Malkhi, M. Reiter, A. Wool, and R. N. Wright. Probabilistic quorum systems. Information and Computation, (2):184–206, November 2001.

[15] B. C. Neuman and T. Tso. Kerberos: An authentication service for computer networks. IEEE Communications,32(9):33–38, September 1994.

[16] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar.SPINS: Security protocols for sensor networks. In Proceedings of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom) , pages 189–199, Rome, Italy, July 2001.