International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Combinational Approach Using Matrix Based Pairwise Key Establishment and Post Deployment Approach in Wireless Sensor Networks

Shishir Sharma[1], Gajendra Singh Chandel[2]

[1]PG Student, Department of CSE, SSSIST, Sehore

[2]Associate Professor, Department of CSE, SSSIST, Sehore

Abstract: ***Key distribution schemes always played a pivotal role in the security of wireless sensor networks. In this research work we focus mainly on the security aspect of WSN . We have developed a modified key distribution scheme which uses the concepts of post as well as pre distribution scheme and thus hs proved to be a better alternative then the rest of two schemes. Simulation study has been carried out using matlab . The effort turned out to be fruitful s our modified scheme showed less dead nodes per round of data transfer as compared to post deployment scheme.***

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

1. Introduction

Distributed sensor networks have received a lot of attention recently due to its wide applications in military as well as civilian operations. Example applications include targettracking, scientific exploration, and data acquisition in hazardous environments. The sensor nodes are typically small, low-cost, battery powered, and highly resource constrained. They usually communicate with each other through wireless links.Security services such as authentication and key management are critical to secure thecommunication between sensor nodes in hostile environments. As one of the most fundamental security services, pairwise key establishment enables the sensor nodes to communicate securely with each other using cryptographic techniques. However, due to the resource constraints on sensor nodes, it is not feasible for them to use traditional pairwisekey establishment techniques such as public key cryptography and key distribution center(KDC).

Instead of the above two techniques, sensor nodes may establish keys between eachother through key predistribution, where keying materials are predistributed to sensor nodesbefore deployment. As two extreme cases, one may setup a global key among the networkso that two sensor nodes can establish a key based on this global key, or assign each sensornode a unique random key with each of the other nodes. However, the former is vulnerableto the compromise of a single node, and the latter introduces huge storage overhead onsensor nodes.

Eschenauer and Gligor proposed a probabilistic key predistribution scheme recently forpairwise key establishment [Eschenauer and Gligor 2002]. The main idea is to let eachsensor node randomly pick a set of keys from a key pool before the deployment so that anytwo sensor nodes have a certain probability to share at least one common key. Chan et al.further extended this idea and developed two key predistribution techniques: a q –composite key predistribution scheme and a random pairwise keys scheme [Chan et al. 2003]. Theq -composite key predistribution also uses a key pool but requires two nodes compute apairwise key from at least q predistributed keys that they share. The random pairwise keys scheme randomly picks pairs of sensor nodes and assigns each pair a unique random key.Both schemes improve the security over the basic probabilistic key predistribution scheme. However, the pair wise key establishment problem is still not fully solved. For the basicprobabilistic and the q -composite key predistribution schemes, as the number of compromised nodes increases, the fraction of affected pairwise keys increases quickly. As a result, a small number of compromised nodes may affect a large fraction of pairwise keys. Thoughthe random pairwise keys scheme does not suffer from the above security problem, given amemory constraint, the network size is strictly limited by the desired probability that twosensor nodes share a pairwise key, the memory available for keys on sensor nodes, and the number of neighbor nodes that a sensor node can communicate with.

In this paper, we develop a number of key predistribution techniques to deal with the above problems. We first develop a general framework for pair wise key establishment based on the polynomial-based key predistribution protocol in [Blundo et al. 1993] and the probabilistic key distribution in [Eschenauer and Gligor 2002; Chan et al. 2003]. Thisframework is called polynomial pool-based key pre distribution, which uses a polynomialpool instead of a key pool in [Eschenauer and Gligor 2002; Chan et al. 2003]. The secretson each sensor node are generated from a subset of polynomials in the pool. If two sensor nodes have the secrets generated from the same polynomial, they can establish a pairwise key based on the polynomial-based key pre distribution scheme. All the previous schemesin [Blundo et al. 1993; Eschenauer and Gligor 2002; Chan et al. 2003] can be considered as special instances in this framework.

By instantiating the components in this framework, we further develop two novel pair-wise key pre distribution schemes: a random subset assignment scheme and a

hypercube-based scheme. The random subset assignment scheme assigns each sensor node the secrets generated from a random subset of polynomials in the polynomial pool. The hypercube-based scheme arranges polynomials in a hypercube space, assigns each sensor node to a unique coordinate in the space, and gives the node the secrets generated from the polynomials related to the corresponding coordinate. Based on this hypercube, each sensor node can then identify whether it can directly establish a pairwise key with another node, and if not, what intermediate nodes it can contact to indirectly establish the pairwise key.Our analysis indicates that our new schemes have some nice features compared with the previous methods. In particular, when the fraction of compromised secure links is less than 60%, given the same storage constraint, the random subset assignment scheme provides a significantly higher probability of establishing secure communication between non-compromised nodes than the previous methods. Moreover, unless the number of com-promised nodes sharing a common polynomial exceeds a threshold, compromise of sensor nodes does not lead to the disclosure of keys established between non-compromised nodes using this polynomial.

Similarly, the hypercube-based scheme also has a number of attractive properties. First,it guarantees that any two nodes can establish a pairwise key when there are no compromised nodes, provided that the sensor nodes can communicate with each other. Second, itis resilient to node compromise. Even if some sensor nodes are compromised, there is stilla high probability to re-establish a pairwise key between non-compromised nodes. Third,a sensor node can directly determine whether it can establish a pairwise key with another node and how to compute the pairwise key if it can. As a result, there is no communication overhead during the discovery of directly shared keys. Evaluation of polynomials is essential to the proposed schemes, since it affects the performance of computing a pairwise key. To reduce the computation at sensor nodes, we provide an optimization technique for polynomial evaluation. The basic idea is to compute multiple pieces of key fragments over some special finite fields such as F28 + 1 and F216 + 1 and concatenate these fragments into a regular key. A nice property provided by such finite fields is that no division is necessary for modular multiplication. As a result, evaluation of polynomials can be performed efficiently on low cost processors on sensor nodes that do not have division instructions. Our analysis indicates that such a method only slightly decreases the uncertainty of the keys.

2. Implementation of Key Predistribution Scheme

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

1. Choose 'N' independent key seeds designated as s_1 , s_2, s_3, …..s_N.
2. Let 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. Create a lambda x lambda matrix as per [1].
5. Calculate matrix A as per [1].
6. Generate keys and broadcast keys to each node.
7. Each node will then transmit packets to BS via other nodes according to matrix A and with the help of keys stored.
8. Because keys are distributed and broadcasted to each nodes in advance this scheme is called as key pre distribution.
9. This scheme has been implemented for 100 nodes and for 100 rounds of data packets and the results are as below :-

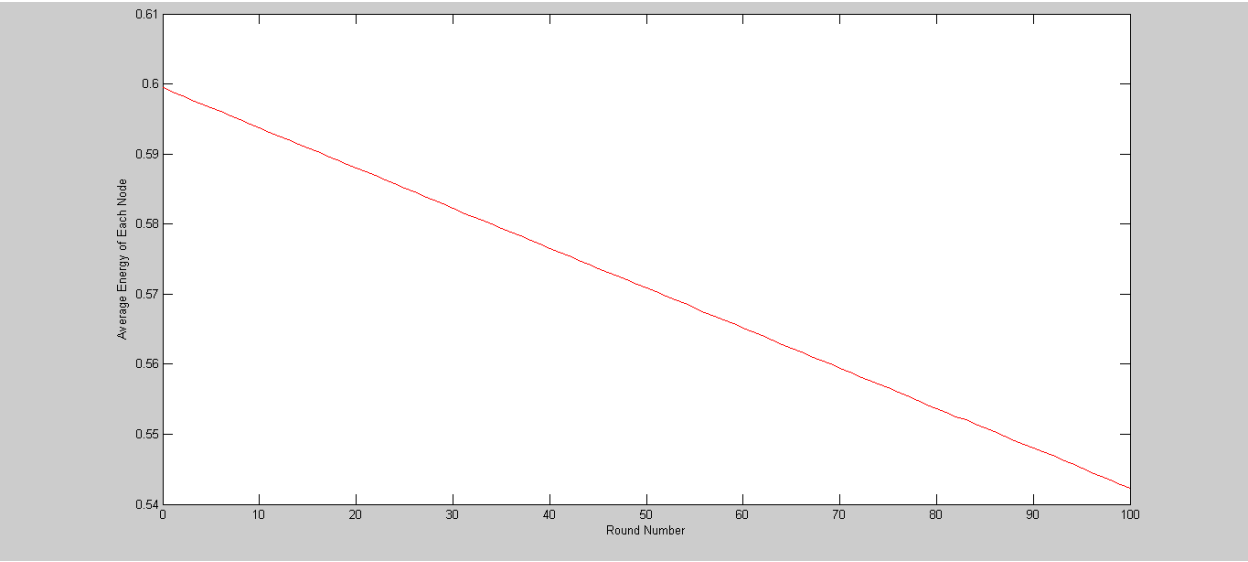

Figure 5.1: Average energy spent per round for key predistribution scheme

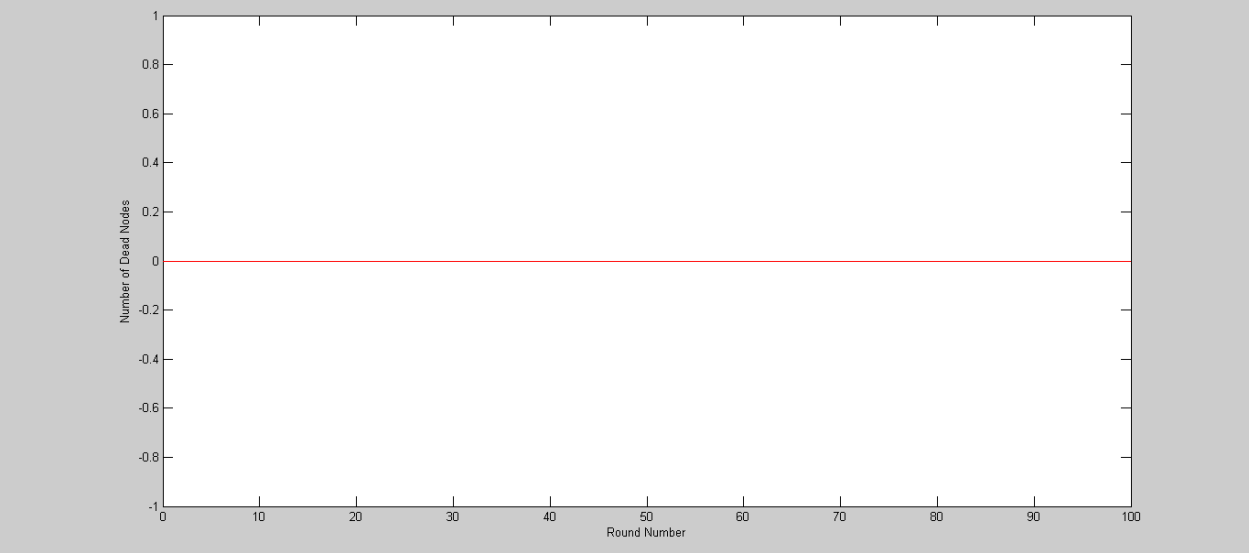

Figure 5.2: No. of dead nodes per round for key predistribution scheme

3. Implementation of Post Deployment Analysis

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

1. 'm' key units are generated by the system in a set of 'M' , such that each node can store a maximum of 'm' key units.
2. A unique id is assigned to each node.
3. Each 'm' key units are randomly distributed to each node.
4. Then nodes are deployed physically and their locations are determined using gps and this information is called as their unique location.
5. Prior to distributing keys the locations are also determined randomly and associated with each node.
6. Then each node will determine the distance between other nodes and then the key will be shared as per [2].
7. Because the keys are not broadcasted as shown in [1] this scheme is referred to a post deployment analysis.

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

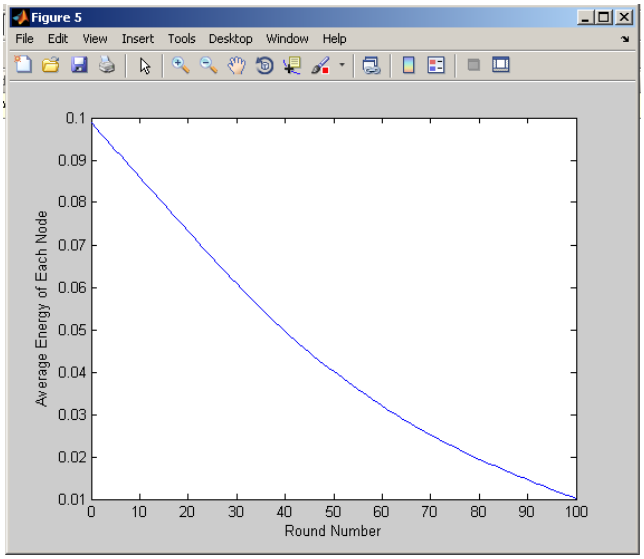

Figure 5.3: Average energy spent per round for post deployment scheme

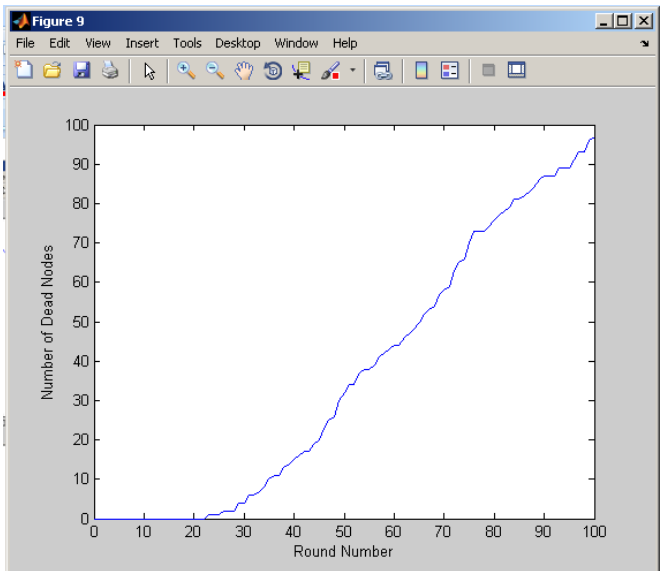

Figure 5.4: No. of dead nodes per round for post deployment scheme

4. A Combinational Approach

In our work we have combined the benefits of the above two schemes and then simulated the entire setup for 100-500 rounds of data transfer. The basic steps involved in our approach are as follows:-

1. We have assumed that the position of nodes are not determined in advance contrary to pre distribution scheme and thus the locations of the nodes are determined via gps but this time the information is relayed to base station.
2. The base station then depending on the location of each node will broadcast the key matrix to each node as per in [1].
3. This distributed common matrix will be used by all the nodes to generate further key for communication.
4. Each node then will determine the distance between other nodes as per [2].
5. This information is then used for effective communication i.e the node will not broadcast the information, rather the information will be relayed form

one node to another as in hierarchical wireless sensor network.

6. The LEACH clustering algorithm has been deployed for further data transfer.
7. Because the information is relayed form one node to another the overall dead node occurrence is significantly reduced and hence the data transfer gets complete without overloading the nodes.

Various simulation results for the said scheme are as given below:-

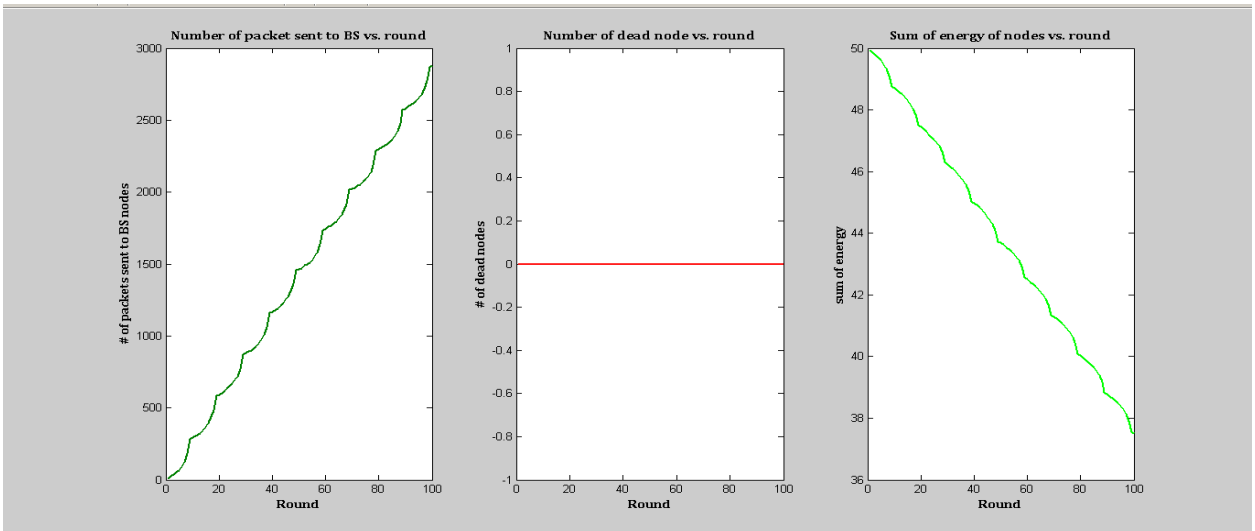

Figure 5.5: Simulations results for modified algorithms for 100 rounds

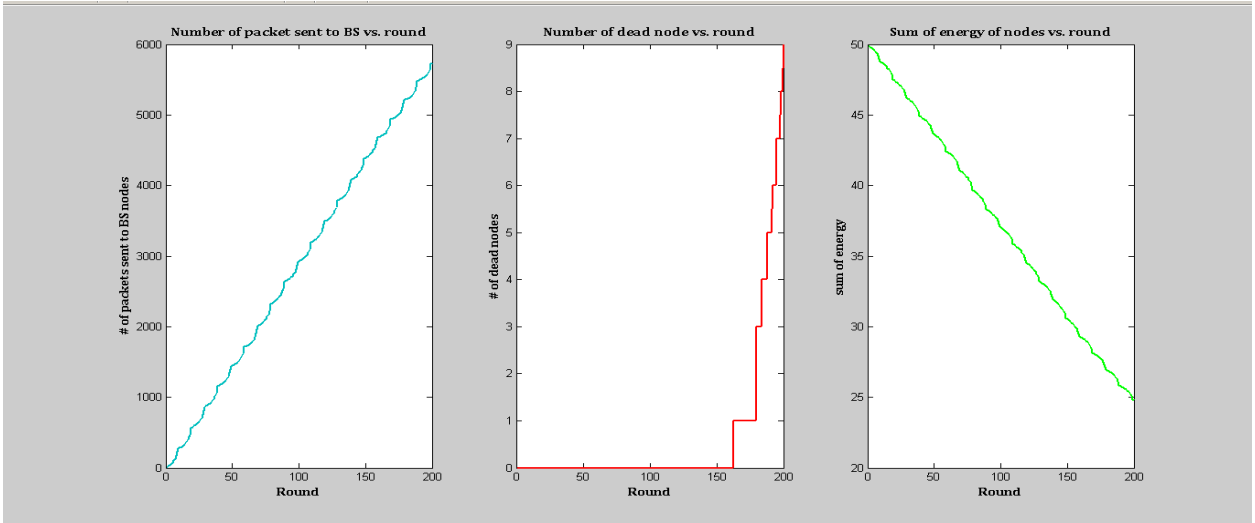

Figure 5.6: Simulations results for modified algorithms for 300 rounds

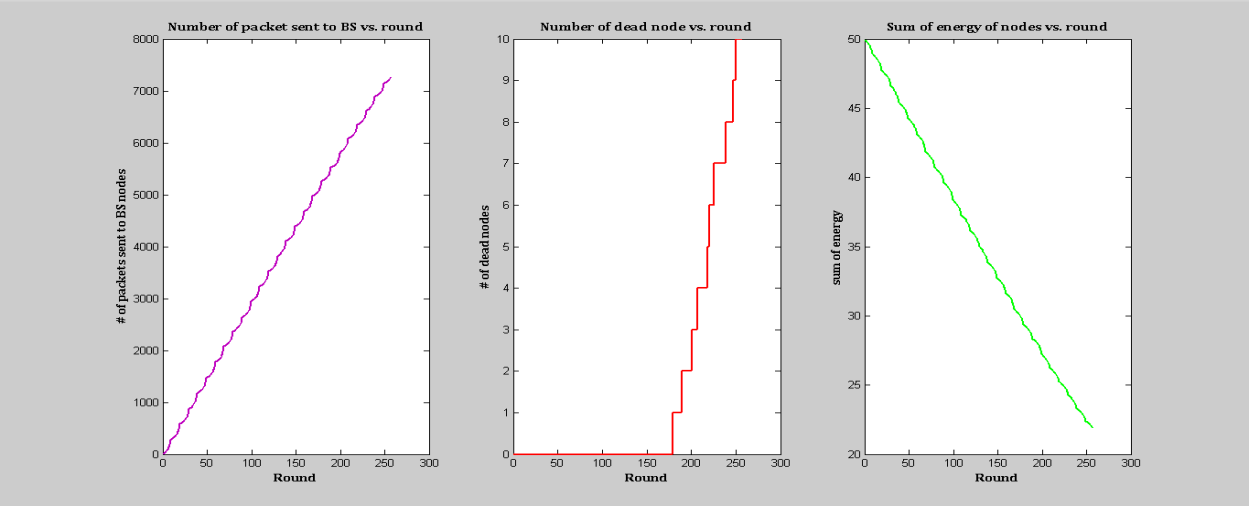

Figure 5.6: Simulations results for modified algorithms for 300 rounds

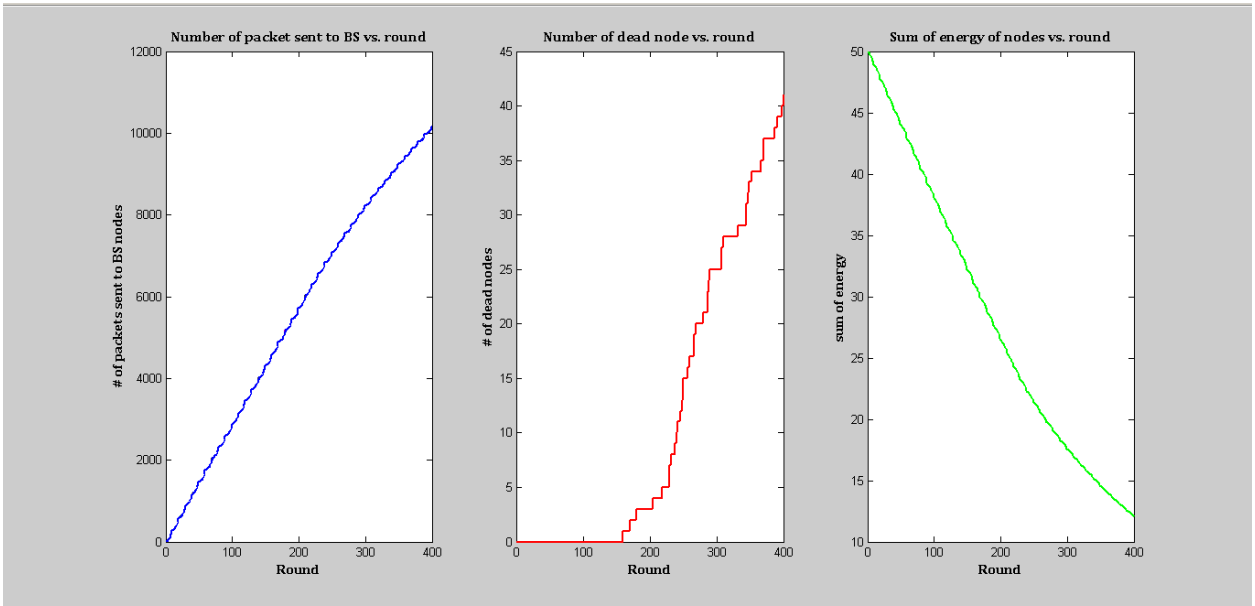

Figure 5.7: Simulations results for modified algorithms for 400 rounds

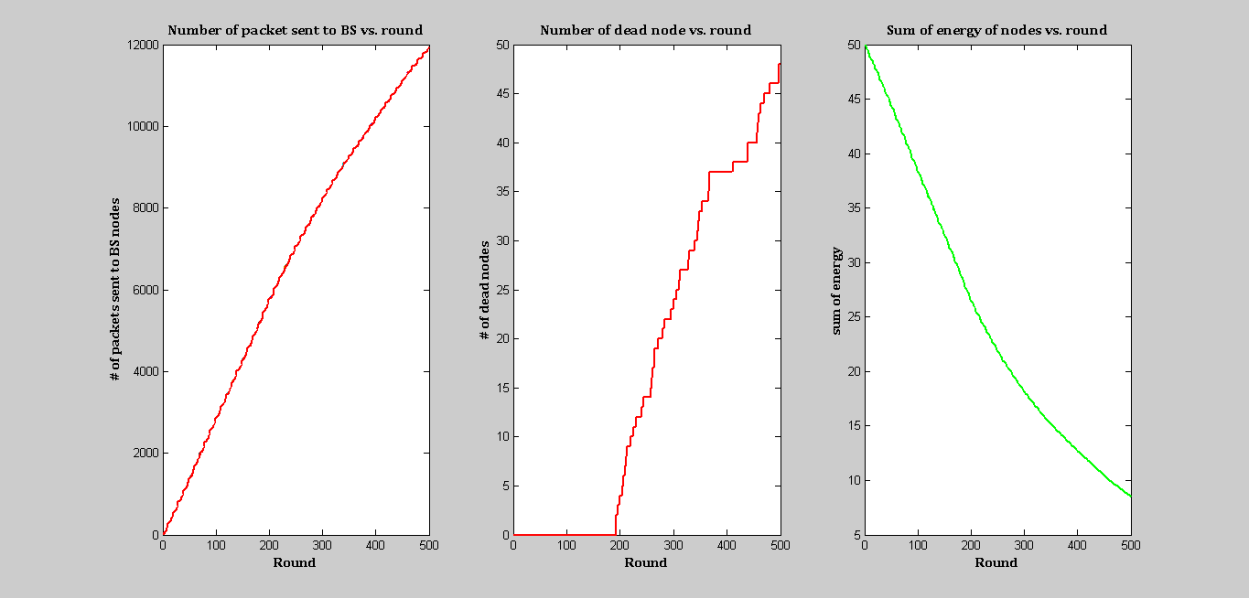

Figure 5.8: Simulations results for modified algorithms for 500 rounds

5. Conclusion

In this research work, we developed a general framework for polynomial pool-based pairwise key predistribution in sensor networks based on the basic polynomial-based key predistribution in [1]. This framework allows study of multiple instantiations of possible pairwise key establishment schemes. Based on this framework, we developed two specific key predistribution schemes: the random subset assignment scheme and the hypercube-based key predistribution scheme. Our analysis of these schemes indicate that both schemes have significant advantages over the existing approaches. The implementation and experimental results also demonstrate the practicality and efficiency in the current generation of sensor networks. Several research directions are worth investigating. First, we observe sensor node have low mobility in many applications. Thus, it may be desirable to develop location-sensitive key predistribution techniques to improve the probability for neighbor nodes to share common keys and at the same reduce the threat of compromised nodes. Second, it is critical to detect and/or revoke compromised nodes from an operational sensor network.

It has been shown in the result analysis that the post deployment analysis scheme given in [2] has major drawbacks in terms of no of dead nodes per round of data transfer , our results are better then both the approaches but several mathematical models are still need to be made , thus this work has to completed in the future to avoid any disambiguousness in the research 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
[3] 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 9th ACM 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.