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:-

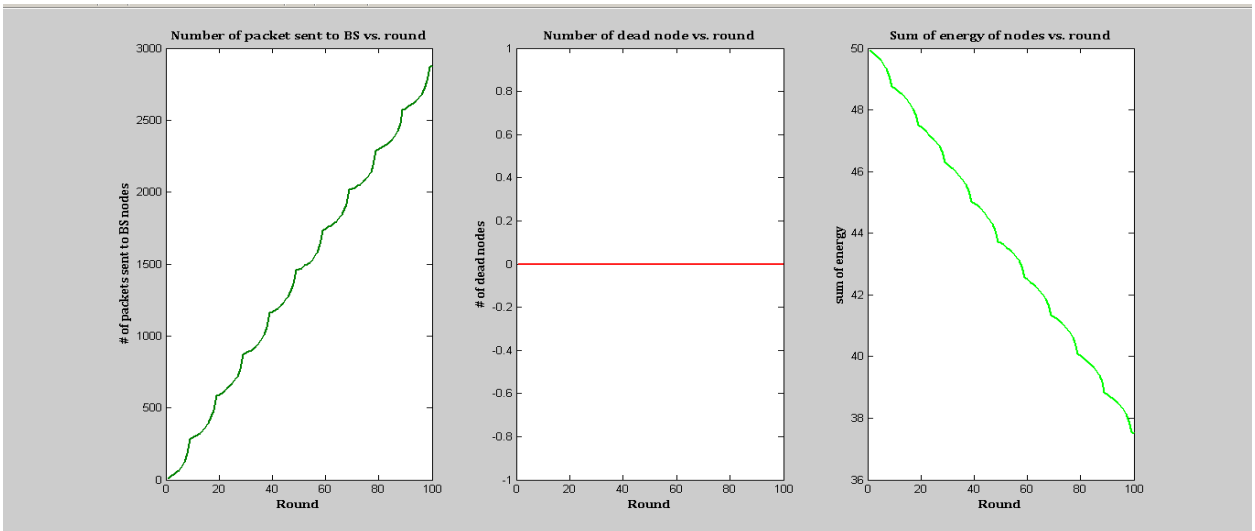

Figure 5.5: Simulations results for modified algorithms for 100 rounds

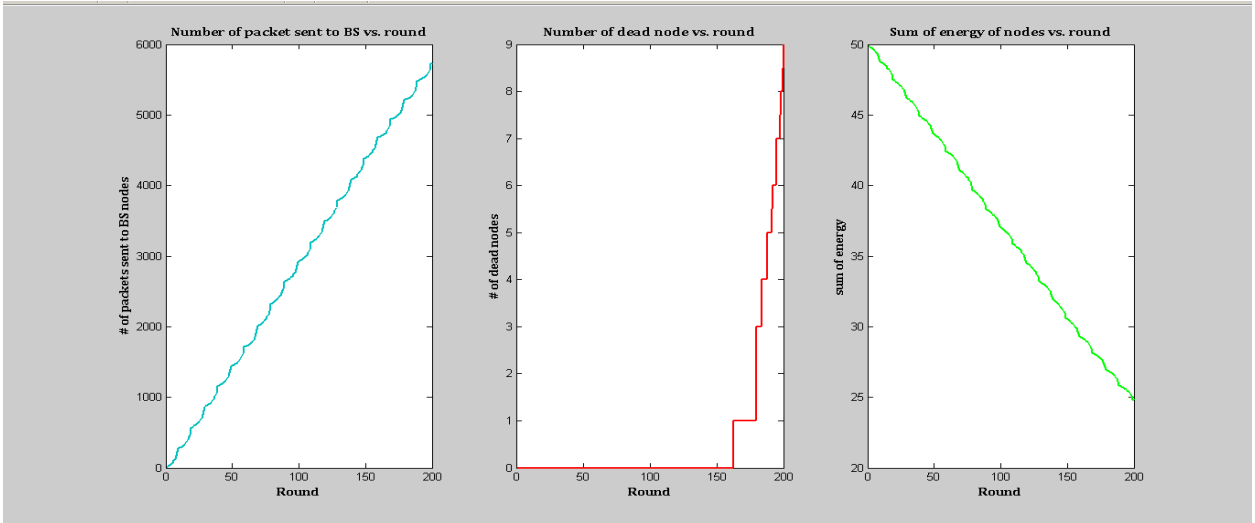

Figure 5.6: Simulations results for modified algorithms for 300 rounds

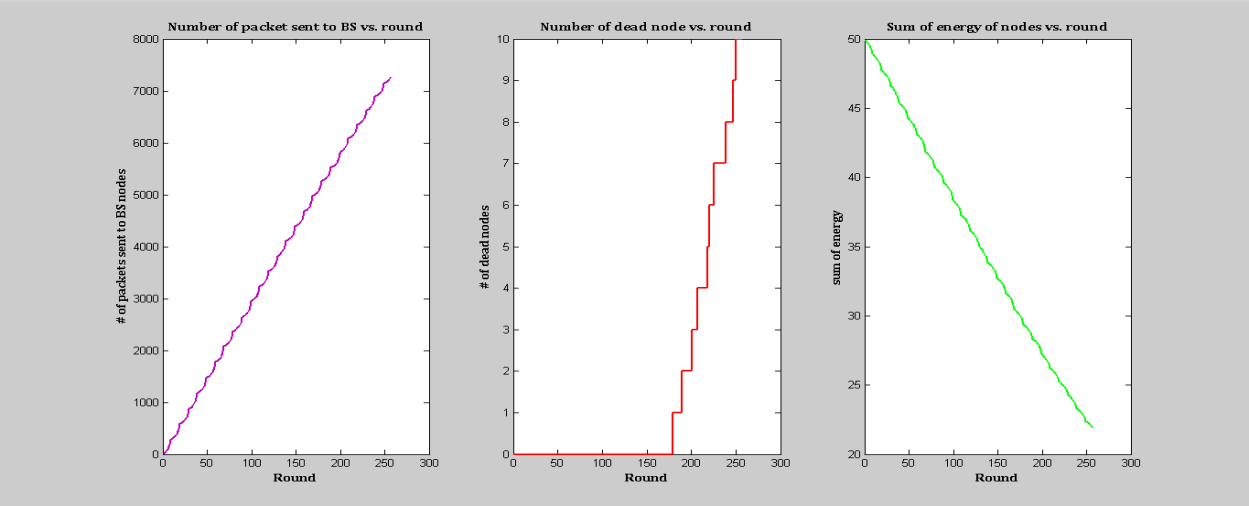

Figure 5.6: Simulations results for modified algorithms for 300 rounds

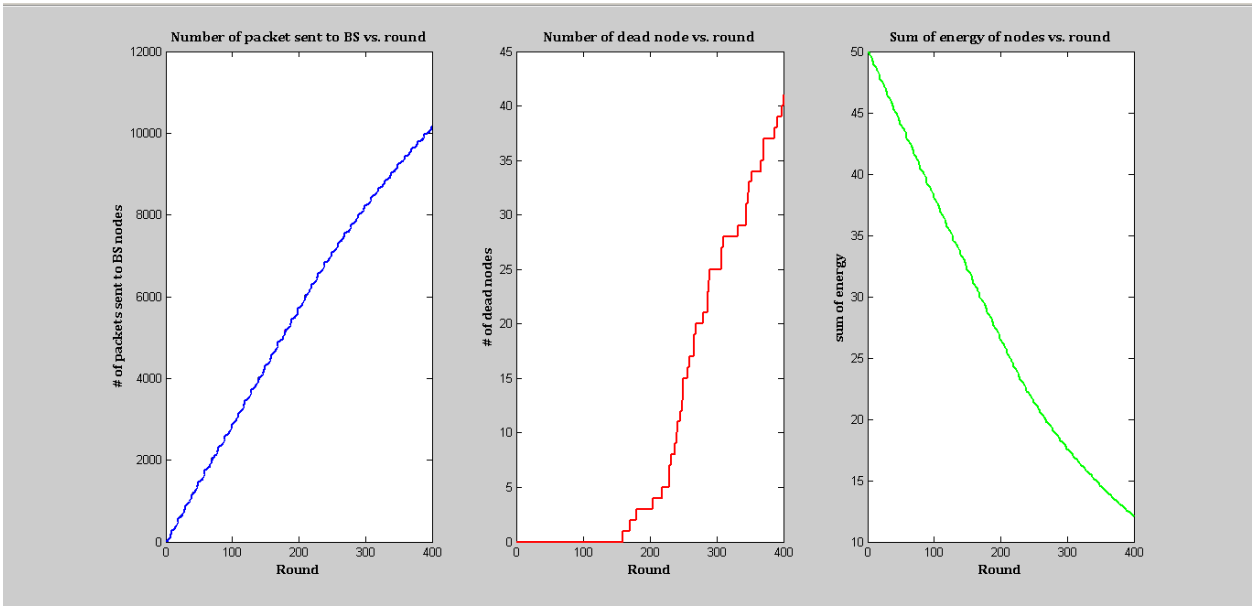

Figure 5.7: Simulations results for modified algorithms for 400 rounds

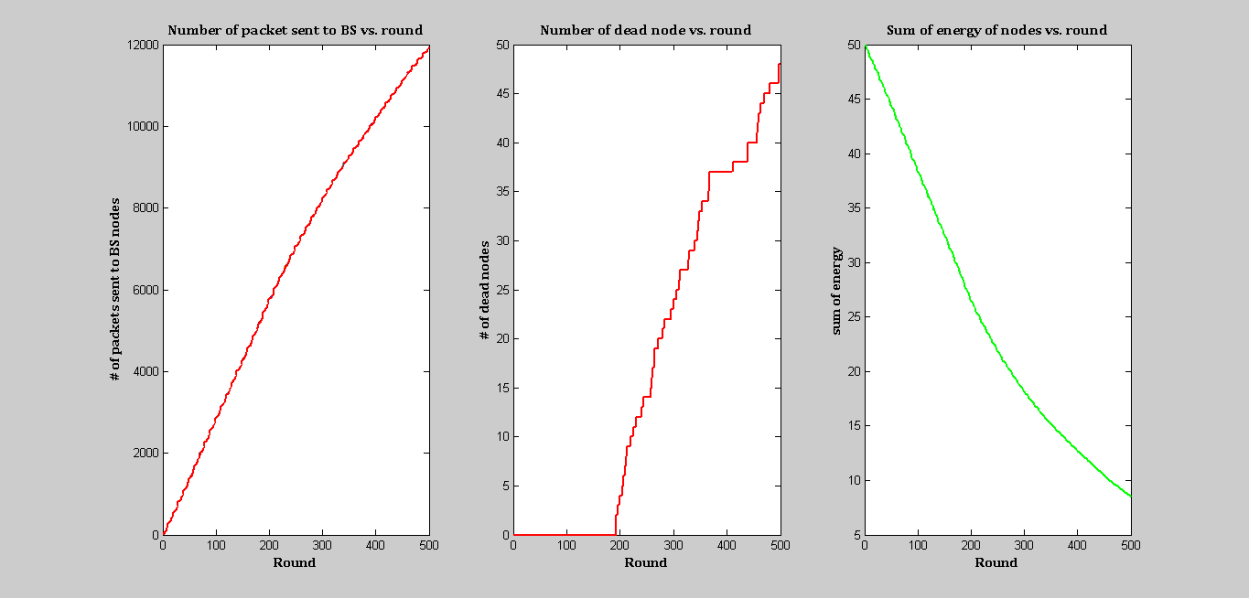

Figure 5.8: Simulations results for modified algorithms for 500 rounds

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 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.