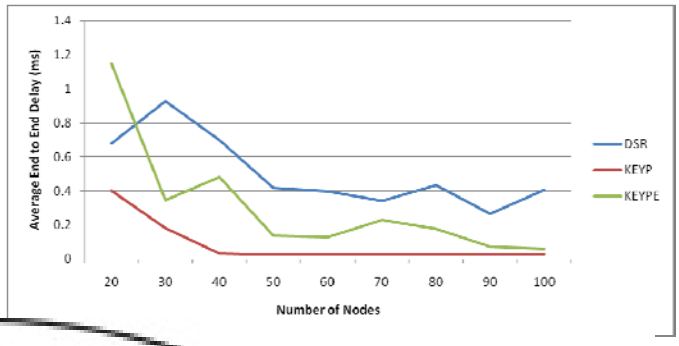
3.4 Key Exchange

In this module the two servers S1 and S2 have received the password authentication information of a client C during the registration, there are several steps for the two servers S1 and S2 to authenticate the client C and establish secret session keys with the client C in terms of parallel computation. The client C randomly chooses an integer r from Zq , computes R and then broadcasts a request message M to the two servers S1 and S2. On receiving M1, the server S1 randomly chooses



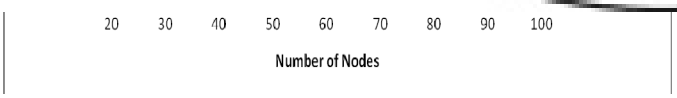


Figure 2: Number of Nodes Vs Packet Delivery Fraction

between network scalability and secure connectivity. We conducted analytical analysis and simulations to compare our new solution to existing ones, the results showed that our approach ensures a high secure coverage of large scale networks while providing good overall performances.

References

[1] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Commun. Surv. Tuts.*, vol. 10, no. 1–4, pp. 6–28, 2008.
[2] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. 2004 IEEE INFOCOM*, pp. 586–597.
[3] S. Ruj, A. Nayak, and I. Stojmenovic, "Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs," in *Proc. 2011 IEEE INFOCOM*, pp. 326–330.
[4] S. A. C¸ amtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 15, pp. 346–358, 2007.
[5] B. Maala, Y. Challal, and A. Bouabdallah, "Hero: hierarchcal key management protocol for heterogeneous WSN," in *Proc. 2008 IFIP WSAN*, pp. 125–136.
[6] W. Bechkit, Y. Challal, and A. Bouabdallah, "A new scalable key predistribution scheme for WSN," in *Proc. 2012 IEEE ICCCN*, pp. 1–7.
[7] S. A. C¸ amtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," Technical Report TR-05-07, Mar. 2005.
[8] S. Ruj and B. Roy, "Key predistribution using combinatorial designs for grid-group deployment scheme in wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 6, no. 4, pp. 1–4:28, Jan. 2010.
[9] M. Doddavenkatappa, M. C. Chan, and A. L. Ananda, "A dualradio framework for MAC protocol implementation in wireless sensor networks," in *Proc. 2011 IEEE ICC*, pp. 1–6.

Author Profile

Maddineni Ramchandra obtained his B.Tech degree from DRK college of Engineering and Technology, Bowrampet and Ranga Reddy District. Currently he is pursuing his M.Tech degree in Digital Systems and Computer Electronics. His research interests are in the area of ADHOC and Wireless Sensor Networks, Advanced Data Communications, VLSI Design, Microcontroller Design, Real Time Operating Systems and Digital System Design.

Mrs.Thoomati Madhavi Kumari obtained B.Tech. in ECE and M.Tech. in Computer Science from JNT University. Presently Mrs. Madhavi is pursuing Ph.D.in Data security for natural languages using FPGA. Mrs. Madhavi joined the faculty of ECE Department of JNU College of Engineering, Kukatpally, Hyderabad as Assistant Professor and served the department for 13 years. Later she was appointed as Assistant Director, UGC-ASC, JNT University, and Hyderabad. She was associated with the implementation of AICTE Sponsored project on computer networks.