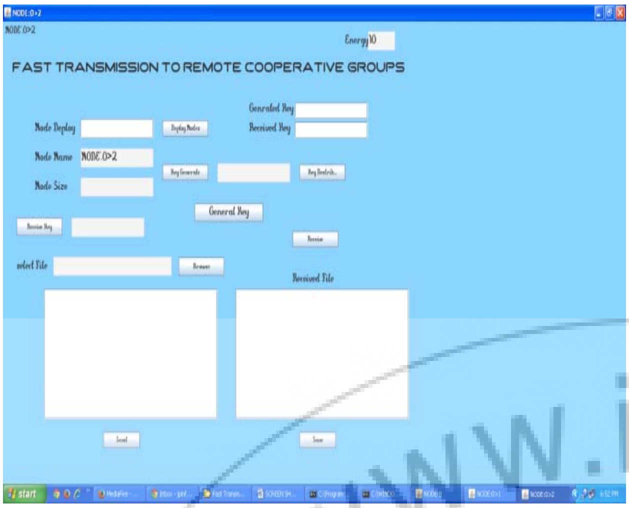

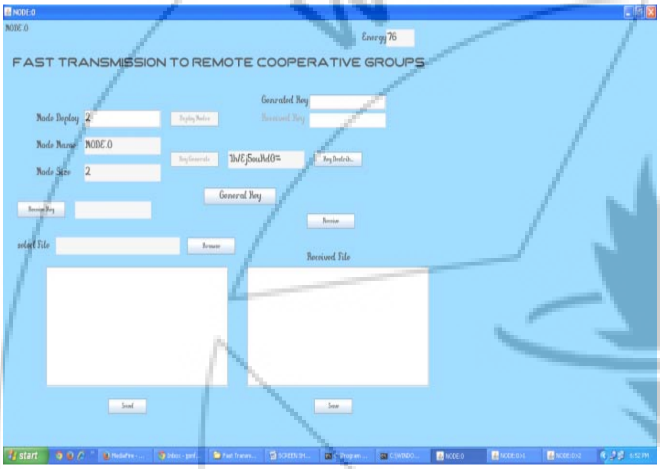

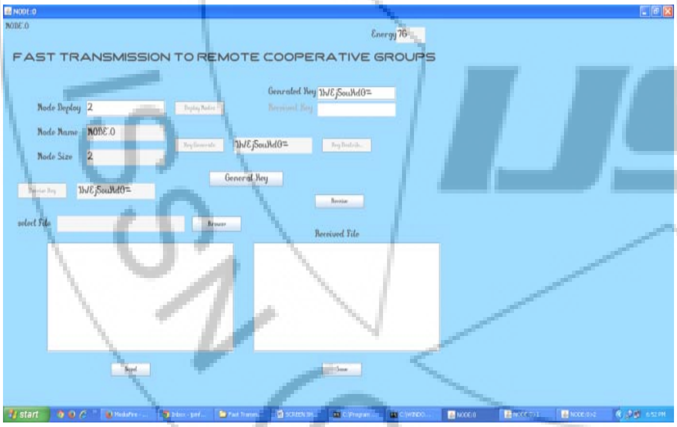

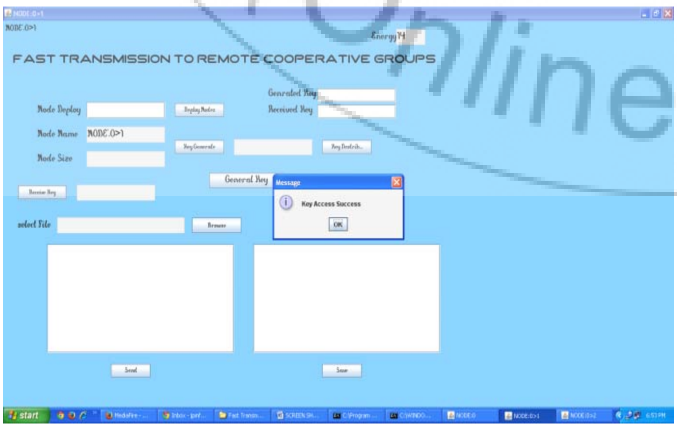

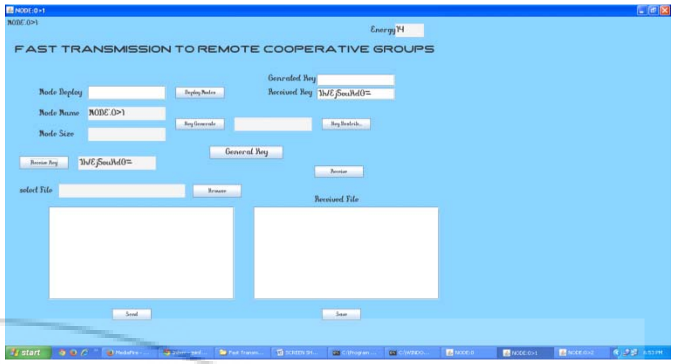

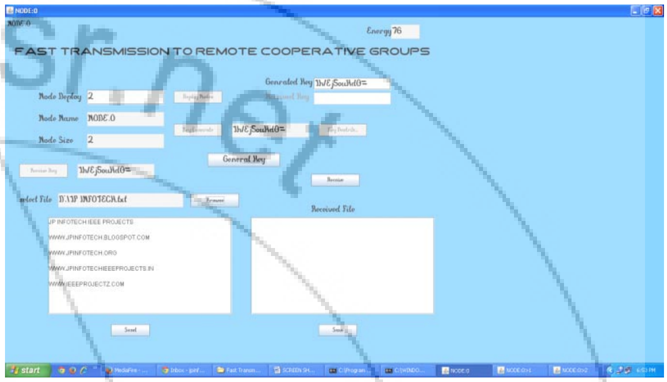

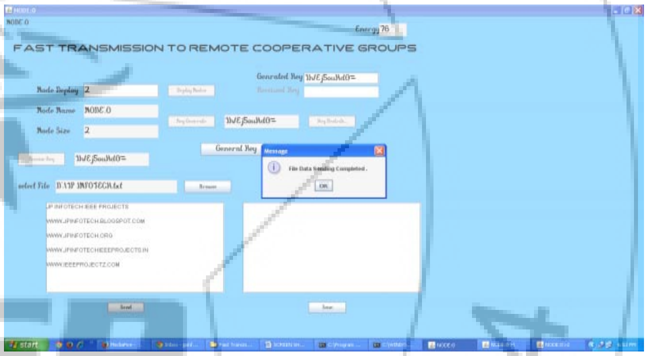

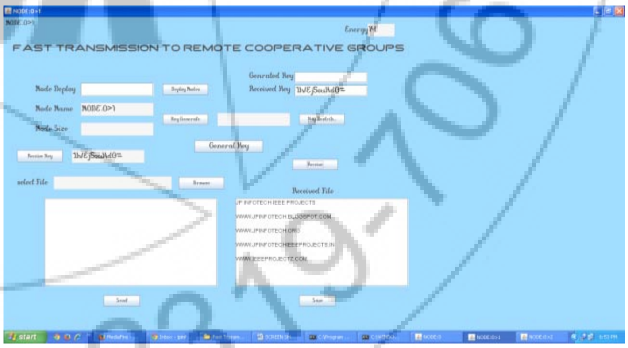

7. Conclusion

We have proposed a new key management paradigm to enable send and leave broadcast to remote cooperative groups with out relying on a fully trusted third party. our scheme has been proven secure in the standard model. A thorough complexity analysis and extensive experiments show that our proposal is also efficient in terms of computation over head and communication. these features render our scheme a promising solution to the group oriented communication with access control in various types of adhoc networks.

References

[1] Q.Wu, J. Domingo-Ferrer, and U. González-Nicolás, "Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications," IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.
[2] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.
[3] J. H. Cheon, N.-S. Jho, M.-H. Kim, and E. S. Yoo, "Skipping, cascade,and combined chain schemes for broadcast encryption,"IEEE Trans.Inf. Theory, vol. 54, no. 11, pp. 5155–5171, Nov. 2008.
[4] Y.-M. Huang, C.-H. Yeh, T.-I. Wang and H.-C. Chao, "Constructing Secure group communication over wireless ad hoc networks based on a virtual subnet model," IEEE wireless Commun., vol. 14, no. 5, pp. 71–75, Oct. 2007.
[5] Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecture for multi-hop wireless mesh networks," IEEE J. Sel. Areas Commun, vol(1). 24, no. 10, pp. 1916–1928, Oct. 2006.
[6] M. Naor and B. Pinkas, "Efficient trace and revoke schemes," inProc.4th FC, 2001, vol. 1962, pp. 1–20.[19] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcastencryption with short ciphertexts and private keys,"Adv. Cryptol., vol.3621, CRYPTO'05, LNCS, pp. 258–275, 2005.
[7] Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, "Secure group communication using robust contributory key agreement,"IEEE Trans. Parallel Distrib. Syst., vol. 15, no. 5, pp. 468–480, May 2004.
[8] J. Lotspiech, S. Nusser, and F. Pestoni, "Anonymous trust: Digitalrights management using broadcast encryption,"Proc. IEEE, vol. 92,no. 6, pp. 898–909, Jun. 2004.
[9] D. Halevi and A. Shamir, "The LSD broadcast encryption scheme,"Adv. Cryptol., vol. 2442, CRYPTO'02, LNCS, pp. 47–60, 2002.
[10] J. Snoeyink, S. Suri, and G. Varghese, "A lower bound for multicastkey distribution,"Proc. IEEE INFOCOM, pp. 422–431, 2001.
[11] C. K. Wong, M. Gouda, and S. Lam, "Secure group communicationsusing key graphs,"IEEE/ACM Trans. Netw., vol. 8, no. 1, pp. 16–30,Feb. 2000.
[12] M. Steiner, G. Tsudik, and M. Waidner, "Key agreement in dynamic peer groups," IEEE Trans. Parallel Distrib. Syst., vol. 11, no. 8, pp. 769–780,Aug. 2000.
[13] M. Abdalla, Y. Shavitt, and A. Wool, "Key management for restrictedmulticast using broadcast encryption,"IEEE/ACM Trans. Netw., vol.8, no. 4, pp. 443–454, Aug. 2000.
[14] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The versa key framework: Versatile group key management," IEEE J. Sel. Areas Commun., vol. 17, no. 9, p. 1614–1631, Sep. 1999.
[15] B. M. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting,"Proc. IEEE, vol. 83, no. 6, pp. 944–957, Jun. 1995.
[16] M. Burmester and Y. Desmedt, "A secure and efficient conference Key distribution system,"Adv. Cryptal.,vol.950, EUROCRYPT'94, LNCS, pp.275–286, 1995.
[17] A. Fiat and M. Naor, "Broadcast encryption,"Adv. Cryptol., vol. 773,CRYPTO'93, LNCS, pp. 480–491, 1993
[18] I. Ingemarsson, D. T. Tang, and C. K. Wong, "A conference on key distribution system,"IEEE Trans. Inf. Theory, vol. 28, no. 5, pp. 714–720,Sep. 1982.

Author Profile

Mr. P.Hari Krishna received B. Tech. degree in Computer Science and Engineering from JNTUK University, in 2010. Currently he is doing M. Tech. In Prakasam Engineering College, from JNTUK University, Kakinada, India

K. V. Srinivasa Rao received M.TECH degree in Computer Science and Engineering from JNTUA University, and currently heis working as an Associate Professor, Department of CSE in Prakasam Engineering College, Kandukur, India.