International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Implementation of Fast Transmission to Remote Cooperative Groups: A New Key Management Scenario in Wireless Sensor Networks

P. Harikrishna[1], K. V. Srinivasa Rao[2]

[1]PG Student, Department of CSE Prakasm Egineering College, Kandukur, Andhrapradesh, India

[2]Associate Professor, CSE Department, Prakasam Engineering College, Kandukur, Prakasam (Dt), India

Abstract: ***The difficulty of effectively and securely broadcasting to a remote cooperative group happens in many freshly appearing networks. A foremost dispute in developing such systems is to over whelm the obstacles of the potentially restricted connection from the assembly to the sender, the unavailability of a completely trusted key generation center, and the dynamics of the sender. The novel, living key administration paradigms cannot deal with these trials effectively. In this paper, we circumvent these obstacles and close this gap by suggesting a innovative key administration paradigm. The new paradigm is a hybrid of customary broadcast encryption and assembly key agreement. In such a scheme, each constituent sustains a single public/secret key two. Upon seeing the public keys of the members, a isolated sender can securely broadcast to any proposed subgroup selected in an publicity hoc way. Following this form, we instantiate a scheme that is verified protected in the standard form. Even if all the no proposed constituents collude, they will not extract any helpful data from the conveyed messages. After the public assembly encryption key is extracted, both the computation overhead and the connection cost are independent of the group dimensions. Furthermore, our scheme facilitates easy yet efficient member deletion/addition and flexible rekeying schemes. Its powerful security against collusion, its unchanging overhead, and its implementation friendliness without relying on a fully trusted administration render our protocol a very under taking solution to many applications***.

Keywords: Ad hoc networks, broadcast, cooperative computing, access control, information security, key management

1. Introduction

Remote cooperative groups using encrypted transmission. Examples can be found in access control in remote group communication arising in wireless mesh networks, mobile ad hoc networks, vehicular ad hoc networks, etc. WMNs have been suggested as a promising low cost approach to provide last-mile high-speed Internet access. A typical WMN is a multi hop hierarchical wireless network. The top layer has high-speed wired Internet entry points. The second layer is made up of stationary mesh routers serving as the multi-hop backbone to connect to each other and Internet via long range high-speed wireless techniques.

The bottom layers include a large number of mobile network users. The end users access the network either by a direct wireless link and through the chain of other peer users leading to a nearby mesh routers; then the router further connects to remote users through the wireless backbone and Internet. Security and privacy issues are of utmost concern in pushing it to the success of WMNs for their wide deployment and for supporting service oriented applications. For instance, a manager on his way to holiday may want to send a confidential email to some staff of her company via WMNs, so that the intended staff members can read the email with their mobile devices (laptops, PDAs, smart phones, etc.). Due to distributed nature and intrinsically open of WMNs, it is essential to enforce access control of sensitive information to cope with both eavesdroppers and malicious attackers. A MANET system is made up of wireless mobile nodes. These nodes have wireless communication and networking characteristics. MANETs have been proposed to serve as an effective networking system which facilitating data exchange between mobile devices even without fixed infrastructures. In MANETs, it is important to support group-oriented applications, such as audio/video conference and one-to-many data dissemination in battlefield or disaster rescue scenarios. In general, users working for the same goal form a cooperation domain; any particular application or interest in a network may lead to the establishment of a corresponding community. Since communication in wireless networks is broadcast and a certain amount of devices can receive transmitted messages, the risk of non -secured sensitive information being intercepted by the unintended recipients is a real concern. For instance, a commander may issue secret commands to soldiers in battlefield via satellite-to-MANET communication. Consequently, efforts to secure the group communication in MANETs are essential.

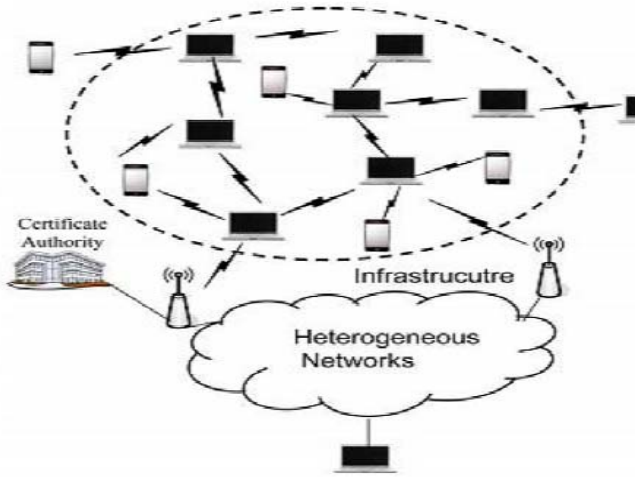


Figure 1: System Model

A VANET consists of on-board units (OBUs) embedded in vehicles serving as mobile computing nodes and road-side units (RSUs) working as an information infrastructure located in critical points on the road. Mobile vehicles form many of cooperative groups in their wireless communications range in the roads, and through roadside infrastructures, vehicles can access other networks such as Internet and satellite communication. VANETs are designed with the primary goal of improving traffic safety and the secondary goal of providing value-added services to vehicles. A substantial body of studies has been devoted to making the primary goal secure and private, by guaranteeing the trustworthiness of vehicle-generated traffic reports and the privacy of vehicles. Very recently, making the secondary goal secure by the securing value-added services in VANETs has been considered. In a particular scenario of this type of applications, only subscribers among an on the-fly cooperative group of vehicles can enjoy/decrypt the value-added services (e.g. multi-player video games) from the remote service providers. Hence, secure group access control is essential to extensively deploy such services in VANETs. A solution to this same problem must meet several constraints. First, sender is remote and can be dynamic. Second, the transmission may cross in various networks including open non -secure networks before reaching the intended recipients. Third, the communication from the group members to senders may be limited. Also, the sender may wish to choose only a subset of the group as the intended recipients. Further, it is hard to resort to a fully trusted third party to get secure communication. In contrast to the above constraints and mitigating features are that the group members are co-operative and the communication among them is local and efficient. This paper exploits these mitigating features for facilitating remote access control of group-oriented communication without relying on a fully trusted secret key generation centre.

2. Related Work

The major security concern in group oriented communications with access control is key management. The existing key management systems used two approaches. One is Group key agreement (or group key exchange by some authors) which allows a group of users to negotiate a common secret key via open insecure networks. Then, any member can encrypt any confidential message with the shared secret key and only the group members can decrypt. And another one is key distribution systems (or the more powerful notion of broadcast encryption). In a key distribution system, a trusted and centralized key server presets and allocates the secret keys to potential users, such that only the privileged users can read the transmitted message. The early key distribution protocol [21] does not support member addition/deletion. Three aspects are important in our contribution. First, we formalize the problem of secure transmission to remote cooperative groups.

3. Contribution

We observe that the existing key management approaches do not provide effective solutions to this problem. On one hand, group key agreement provides an efficient solution to secure intra group communication, but for a remote sender, it requires the sender to simultaneously stay online with the group members for multiple rounds of interactions to negotiate a common secret session key before transmitting any secret contents. On the other hand, broadcast encryption enables external senders to broadcast to non cooperative member s of a preset group without requiring the sender to interact with the receivers before transmitting secret contents, but it relies on a centralized key server to generate and distribute secret keys for each group member.

This implies that:

1) before a confidential broadcast channel is established, numerous confidential uni cast channels from the key server to each potential receiver have to be constructed.
2) the key server holding the secret key of each receiver can read all the communications a n d has to be fully trusted by any potential sender and the group members. Second, we propose the new approach is a hybrid of group key agreement and public-key broadcast encryption. In our approach, each group member has a public/ secret key pair. By knowing the public keys of the members, a remote sender can securely broadcast a secret session key to any intended subgroup chosen in an ad hoc way and simultaneously, any message can be encrypted to the intended receivers with the session key. Only the selected group members can together decrypt the secret session key and hence the encrypted message.

In this way, the dependence on a fully trusted key server is eliminated. Also, the dynamics of the sender and the group members are coped with because the communication between the sender and the receivers before the transmission of messages is avoided and the communication from the group members to the remote sender is minimized. Third, The new key management paradigm and perform extensive experiments in the context of mobile ad hoc networks. In the proposed protocol, after extraction of the public group encryption key in the first run, the subsequent encryption by the sender and the decryption by each receiver are both of constant complexity, even in the case of member changes or system updates for rekeying. As to security, the proposal is shown secure against an attacker colluding with all the no intended members. Even such an attacker cannot get any useful information about the messages transmitted by the remote sender. The proof is given under a variant of the standard Decision Diffie Hellman (DDH) assumption.

4. Problem Statement and System Model

Problem Statement A group composed of N users, indicated by {u1…uN}. A sender would like to transmit secret messages to a receiver subset S of the N users, where the size S of is n≤N. The problem is how to enable the sender to efficiently and securely finish the transmission with the following constraints.

1) It is hard to deploy a key generation authority fully trusted by all users and potential senders in open network settings.
2) The communication from the receivers to the sender is limited, e.g., in the battlefield communication setting.
3) N might be very large and up to millions, for instance, vehicular adhoc networks.

4) Both the sender and the receiver sets are dynamic due to ad hoc communication.

According to the application scenarios, there are also some mitigating features that may be exploited for solving the problem.

1) n is usually a small or medium value, e.g., less than 256.
2) The receivers are cooperative and communicated via efficient local (broadcast) channels.
3) A partially trusted authority, e.g., a public key infrastructure, is available to authenticate the receivers (and the senders).

5. Key Management

The major security concern in group-oriented communications with access control is key management. The key management paradigm al-lowing secure and efficient transmissions to remote cooperative groups by effectively exploiting the mitigating features and circumventing the constraints. This system is to securely distribute a session key to the intended receivers, it is sufficient to define the system as a session key simultaneously encrypt any message under the session key, and only the intended receivers can decrypt. Member Organization Organize the nodes in the network. Each and every node should managed by Group Manager. Whenever the nodes want to move from one place to another place, they can easily move with the permission of group manager. Any node want to add in the network or group, the group manager should allow the new node in the group. Doing this process, we can easily manage the network members and avoid unwanted nodes. Key Updating Process In this process, whenever happened nodes addition and deletion, the key should rekey in the group and the network. Updating the long-term secret key of a member causes more overhead than updating her session key or her group decryption key, although the long-term secret key update process described is still much more efficient than a completely new run of the protocol.

Key Pre distribution Phase in dynamic key management In proposed scheme an authentication key is a pair of public/private key and a certificate signed by the base station are pre distributed in each cluster head. The authentication key is used to verify member sensor node identities. Authentication key is known to all cluster heads and the base station. The public/private key pair is used to establish pair wise keys among cluster heads. An authentication key and the public key of the base station are pre distributed in each member sensor node. Public key is used to verify the certificates of the cluster heads. Authentication key can be calculated by the following hash function: K Authi=H(I Di‖ KCH Auth)

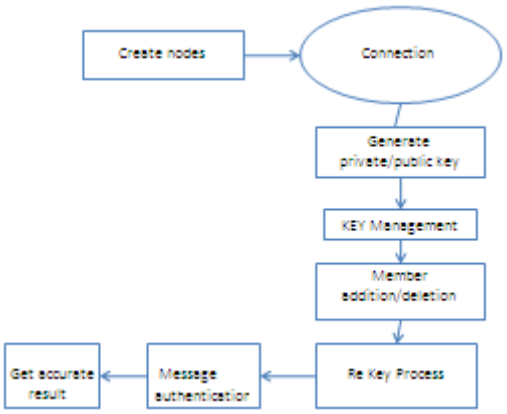
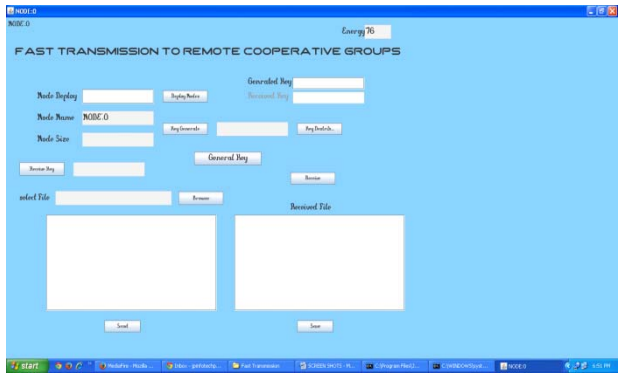
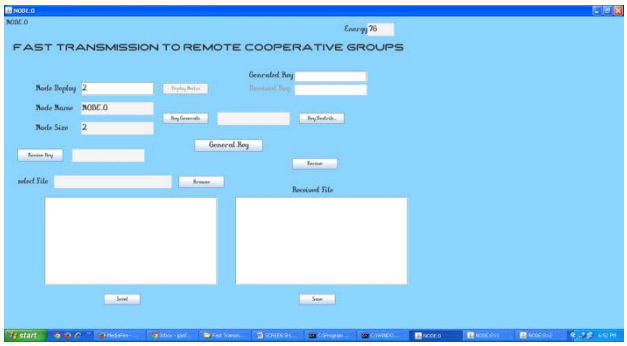


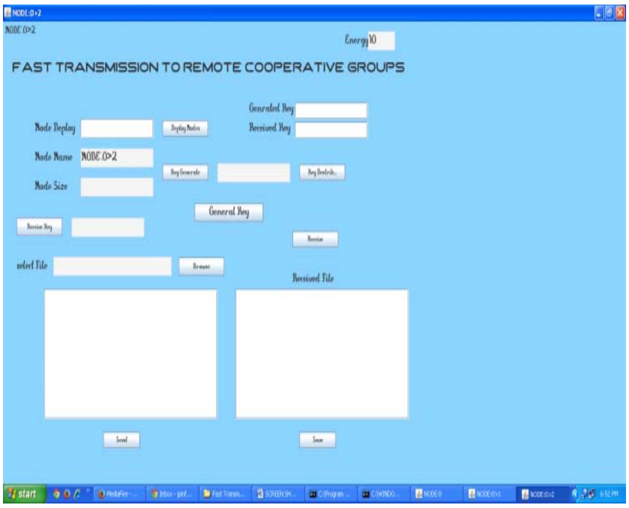
Figure 2: Design flow graph of system

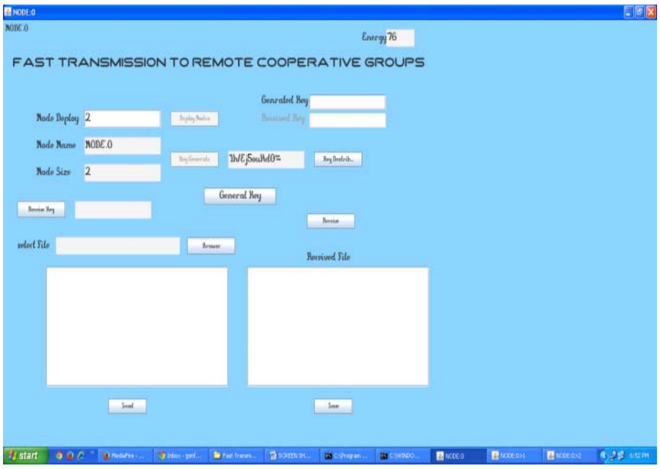
In this process first we create node and then Generate pair wise key .The pair wise key include private and public keys. The cluster head generate key management it will independent on membership addition and deletion of the node. If incase the pair wise key not satisfy the cluster head key generation means the cluster head will intimate to the particular node to perform the rekey strategy. Now the information is authenticated and transfer in secure manner. encapsulation mechanism.

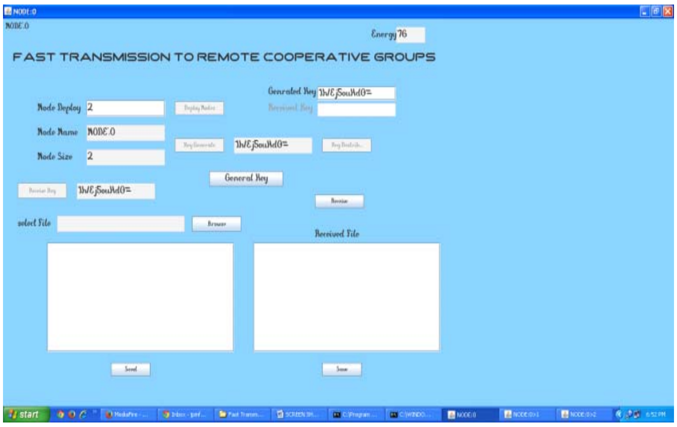
6. Simulation Results

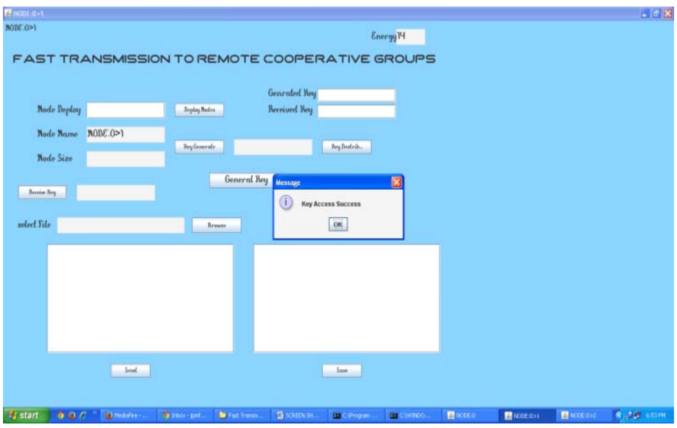


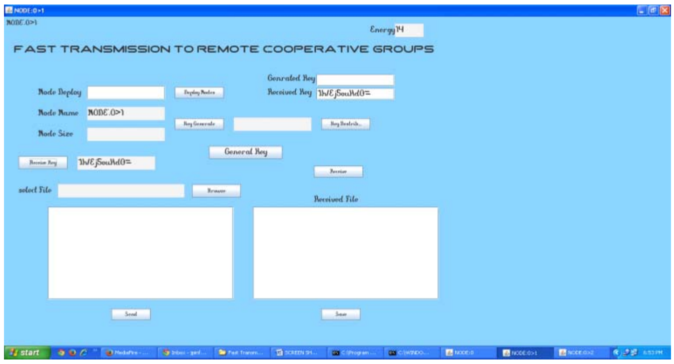


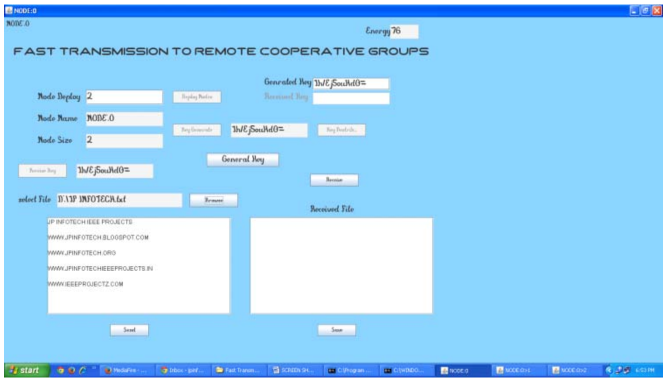


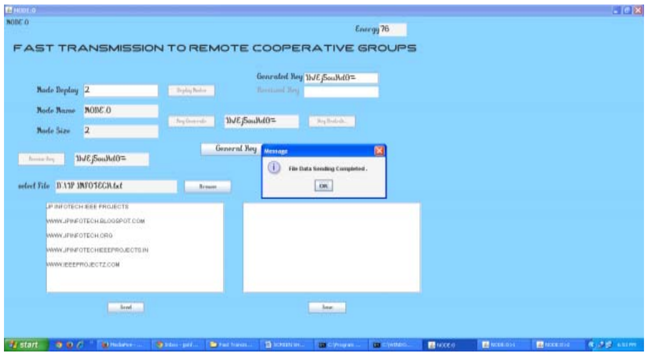


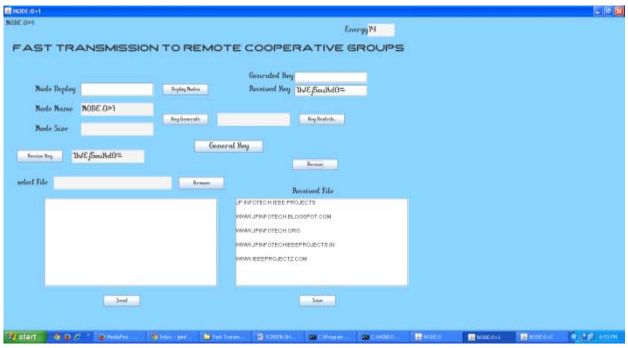












7. Conclusion

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.