and roadside equipment. Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

2) Smart Phone Ad hoc Networks (SPANs) leverage the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smart phones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure.
3) Internet based mobile ad hoc networks (iMANETs) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes.

1.2 Related work

The major security concern in group-oriented communications with access control is key management. Existing key management systems in these scenarios are mainly categorise with two approaches referred to as group key agreement or it may be called group key exchange and key distribution systems. Group key agreement 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.

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.

One more cryptography technique is broadcast encryption essential for good key management can be used with above techniques. Broadcast encryption schemes in the literature can be classified in two categories: symmetric-key broadcast encryption and public-key broadcast encryption. In symmetric-key broadcast encryption key server generate secret key and transmission takes place, on other hand in public-key broadcast encryption , key server generate both secret and public-key so in addition to key server anybody can be sender to the group member.

1.3 Contribution

Our contributions are first, we achieve the limitation of secure transmission to ad-hoc groups, in which the core is to establish a one-to-many channel securely. According to 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 intragroup communication, but for a remote sender, it requires the sender to stay simultaneously connected with the group members to exchanging common secret session key before transmitting any data to the group members. On the other hand if we go by using broadcast encryption sender may transmit data to the group member without any communication is required between sender and group member before transmitting any secure content to the group members. If we use this technique its require to have an fully trusted key generation system.

In order to avoid all this limitation, we propose a new key management allowing us to secure and efficient transmissions to remote ad-hoc groups by cryptography technique discussed above. The new approach is a combination of group key agreement and public-key broadcast encryption (Combined Cryptography).

In this cryptography approach, each group member has a public/secret key pair. By knowing the public keys of the members which is retrieved from a public key server that is widely available in existing network, a remote sender can securely broadcast a secret session key to any intended group chosen in an ad hoc way and along with this any message can be encrypted to the intended receivers group with the secret session key.

Only the selected group members can decrypt the broadcasted message to retrieve secret session key that can be used to decrypt the subsequent message from sender to group. In this way, the dependence on a fully trusted key server is eliminated.

2. Problem Statement and System Model

The problem is how to enable the sender to efficiently and securely transmit data with the following constraints.

2.1 It is hard to maintain a key generation system which is fully trusted by all group member and senders in ad-hoc network.

2.2 The communication between the sender and the group member is should be limited.

We address the above problem by formalizing a new key management paradigm referred to as group key agreement-based broadcast encryption.

Each receiver has a public/secret key pair. The public key is certified by a certificate authority, but the secret key is kept only by the receiver. A remote sender can retrieve the receiver's public key from the certificate authority and validate the authenticity of the public key by checking its certificate, which implies that no direct communication from the receivers to the sender is necessary. Then, the sender can send secret messages to any chosen subset of the receivers.
The system architecture is illustrated in Figure on next page.

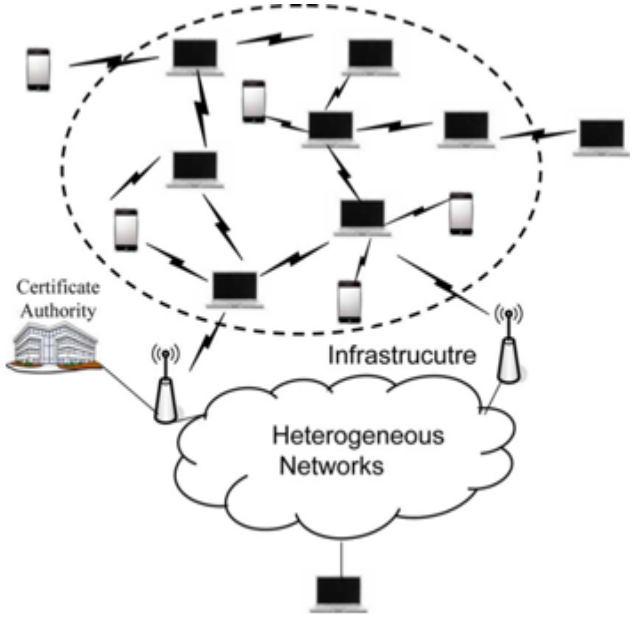


Figure 2: Basic System Model

Following is the algorithm used to implement the cryptography system discussed above.

2.1 Key Generation

This key generation algorithm is run by each user to generate her public/private key pair. We assume that each user's public key is certified by a publicly accessible certificate authority so that anyone can retrieve the public keys and verify their authenticity. This is public key infrastructures have been a standard component in many systems supporting security services. The key generation and the registration to the certificate authority can be done offline before the online message transmission by the sender.

2.2 Encryption

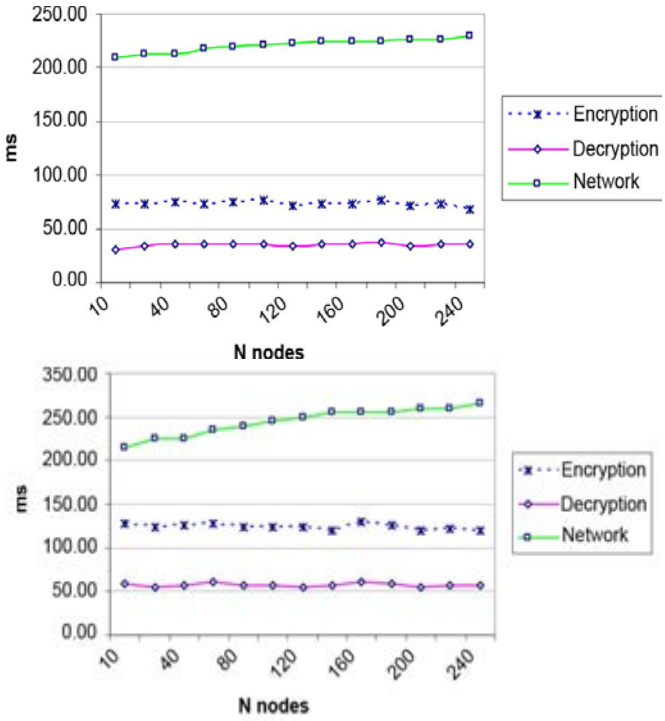
Its run by one who wants to transmit an secure data, content to the group member. Before encrypting data it takes input as public keys of an receiver group member from key generation system also ensure the authenticity of intended receiver's and produce output containing shared secret key, which is broadcasted to the receivers group, which can be used for further decryption by the receiver. The sender can encrypt any message to the receivers with any secure symmetric encryption algorithm, e.g., AES.

2.3 Decryption

This algorithm is jointly run by the intended receivers to extract the secret session key available in encrypted message which is broadcast by the sender. For decryption receiver is using its own secret key. Once receiver is able to extract secret session key, further receiver can easily decrypt the, encrypted messages to the receiver.

3. Result and Discussion

In this section, we encode our new key management cryptography and perform simulations in the context of MANETs. The simulation can be executed on personal laptop with Intel core processor. The experimental results are that the time delay introduced by group decryption is really low. The cost of the encryption to the group grows linearly with the number of the receivers increases. From Figure below, updating a group decryption key or the long-term key of a member has a minimum cost.



In addition to the above remarkable performance, our new key management paradigm has also structural advantages over existing system. Compared to group key agreement, our approach does not require a remote sender to simultaneously stay Online with the receivers. This makes possible the desirable send-and-leave pattern for the senders. Compared to broadcast encryption, our approach does not require a fully trusted key server and is easy to be deployed in practice.

4. Conclusion

We have proposed a new cryptography technique to enable broadcasts to remote ad-hoc groups without relying on a fully trusted key generation system. These features render our scheme a promising solution to group-oriented communication with access control in various types of ad hoc networks. A thorough complexity analysis and extensive experiments show that our proposal is also efficient in terms of computation and communication. Thus The new approach is a combination of group key agreement and public-key broadcast encryption (Combined Cryptography) avoid the dependence on a fully trusted key server and enables secure transmission.

Reference

[1] D. Halevi and A. Shamir, "The LSD broadcast encryption scheme," Adv. Cryptol., vol. 2442, CRYPTO'02, LNCS, pp. 47–60, 2002.

[2] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," Adv. Cryptol., vol. 3621, CRYPTO'05, LNCS, pp. 258–275, 2005.
[3] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," Adv. Cryptol., vol. 1666, CRYPTO'99, LNCS, pp. 537–554, 1999.
[4] J.-H. Park, H.-J. Kim, M.-H. Sung, and D.-H. Lee, "Public key broadcast encryption schemes with shorter transmissions," IEEE Trans. Broadcast., vol. 54, no. 3, pp. 401–411, Sep. 2008.
[5] A. Sherman and D. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Trans. Softw. Eng.*, vol. 29, no. 5, pp. 444–458, May 2003.
[6] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," *Trans. Inf. Syst. Security*, vol. 7, no. 1, pp. 60–96, Feb. 2004.
[7] Y. Sun,W. Trappe, and K. J. R. Liu, "A scalable multi cast key management scheme for heterogeneous wireless networks," *IEEE/ACMTrans. Netw.*, vol. 12, no. 4, pp. 653–666, Aug. 2004.
[8] P. P. C. Lee, J. C. S. Lui, and D. K. Y. Yau, "Distributed collaborative key agreement and authentication protocols for dynamic peer groups," *IEEE/ACM Trans. Netw.*, vol. 14, no. 2, pp. 263–276, Apr. 2006.