OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

A Novel Key Management Paradigm for Broadcasting to Remote Cooperative Groups

Murala Lavanya[1], T. Sukanya[2]

[1] M. Tech (CSE), MVR College of Engineering and Technology, A.P., India.

[2]Asst. Professor, Dept. of Computer Science & Engineering, MVR College of Engineering and Technology, A.P., India.

Abstract: *A Mobile Ad Hoc Network(MANET) is a system made up of wireless mobile nodes. These MANET nodes have wireless communication and networking characteristics. MANETs have been proposed to serve as an effective networking system facilitating information 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 disaster or battlefield rescue scenarios. In the above group oriented communication scenarios, the common problem is to enable a sender to securely transmit secret messages to a remote cooperative group. A solution to the above problem must meet several constraints. First, the sender must be remote and can be dynamic. Second, the message transmission may cross various networks including open insecure networks before reaching the intended recipients. Third, the data communication from the group members to the sender may be limited. Also, the sender may wish to choose only a subset of the overall group as the intended recipients. Furthermore, it is hard to resort to a fully trusted third party to secure the overall communication. In contrast to the above constraints, mitigating features are that the group members are cooperative and the secret communication among them is local and efficient. This paper exploits these mitigating features to facilitate the remote access control of group-oriented communications without relying on a fully trusted secret key generation center.*

Keywords: *Broadcasting, Group communication, Key Management, MANET, VANET.*

I. INTRODUCTION

Mobile Ad Hoc Networks(MANETs) [1] are planned to function good networking system facilitating data exchange between mobile devices without fixed infrastructures. It's most important to support group-oriented applications, audio and video conference and one-to- many data dissemination in disaster or battlefield rescue scenarios. Wireless network communication is broadcast and a certain amount of devices can receive transmitted messages, the risk of unsecured sensitive data being intercepted by unintended recipients is a real concerned. So MANET, Vehicular Ad Hoc Network(VANET) [2] having in same near future. This network communication is hard to resort hard to resort to a fully trusted third party to secure the network communication. And then the group members must be cooperative and the communication among them is local and efficiently. An ad hoc network is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing traditional network infrastructure. It is an autonomous system in which mobile nodes connected by wireless links are free to move randomly and often act as routers at the same time. The traffic types in MANETs are quite different from those in an infrastructure wireless network. Figure 1 shows an example MANET.

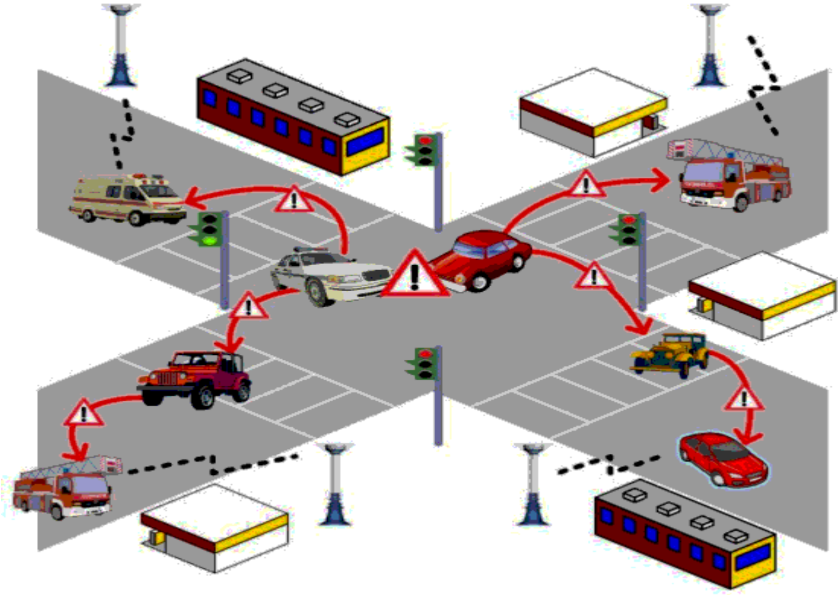

Fig. 1: An example MANET

A Mobile Ad Hoc Network is a type of ad hoc network that can change locations and configure itself on the fly. Because ad hoc networks are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a satellite or cellular transmission. A Mobile ad hoc Network (MANET) is a self-configuring infrastructure network of several mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose". Key Management is the major security concept in group oriented Communications. The existing key management systems can be categorised in to two types depending on the approaches. They are: Group Key Agreement and Key Distribution systems. Presently both of these concepts are active research areas and they have huge repositories of literature.

II. Related Work

In a wireless environment, access control is the most fundamental and critical security issue in group oriented communication [3]. Generally, access control can be achieved by applying cryptographic techniques. A shared key, called group key or traffic encryption key (TEK), is used to cipher the group communication data and is distributed to all legitimate group members. Only the members who own this traffic key can access the communication content. The integrity and confidentiality of the group's communication rely on the safety of the group key. Management of the group key thus plays a vital role in the security of group communication [4]. Key management in group oriented communication is very different from that in the point-to-point communication model. In the point-to-point model, the cipher key can be generated by negotiation through protocols such as the Diffie-Hellman key exchange protocol [5] or it can be generated by one side and then sent to another side. However, in group oriented communication, a group may have many receivers, and the efficient generation, regeneration and distribution of the group keys to all receivers is a complicated and challenging task.

A large number of group key agreement protocols have been proposed in the literature. The earlier efforts in [6] focused on efficient establishment of the initial group key. Later studies in [7] enable efficient member joins, but the cost for a member leave is still comparatively very high. A tree key structure has been further proposed and then improved to achieve better efficiency for member joins and leaves [8]. Broadcast encryption is very essential for key management [9] in priced media distribution [10] and digital rights management [11]. Broadcast encryption schemes in the literature can be classified in 2 categories: symmetric-key broadcast encryption and public-key broadcast encryption. In the symmetric-key encryption, only the trusted center generates all the secret keys and broadcasts messages to all users. Hence, only the key generation center can be the sender or the broadcaster. In the public-key encryption, in addition to the secret keys for each user, the trusted center also generates a public key for all the users so that any one can play the role of a sender or broadcaster .

III. PROPOSED WORK

1. System Model

In this paper, we create nodes and made ad hoc network. Each and every node has to generate both public and secret key. And allocate a certificate authority person to provide the certificate for public key during data transmission but he does not have secret key, receiver only have that single secret key. The remote sender can retrieve the receiver's public key for checking and validate through the certificate authority. The potential receivers are linked together with the efficient local connections. Using communication infrastructures, they can also join to the heterogeneous networks. Each receiver has a public and secret key pair. The public key is certified by a certificate authority(CA), but the secret key is kept only by the receiver side. A remote sender can get back the receiver's public key from the CA 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 [7]. Then, the sender can send the secret messages to any chosen subset of the receivers. After that officially define the model of the group key agreement based broadcast encryption. Since the heart of the key management is to securely distribute a session key to the intended receivers, it is sufficient to define the system as a session key encapsulation mechanism. Then, the sender can at the same time encrypt any message under the session key, and only the intended receivers can decrypt it. Figure 2 shows our system model.

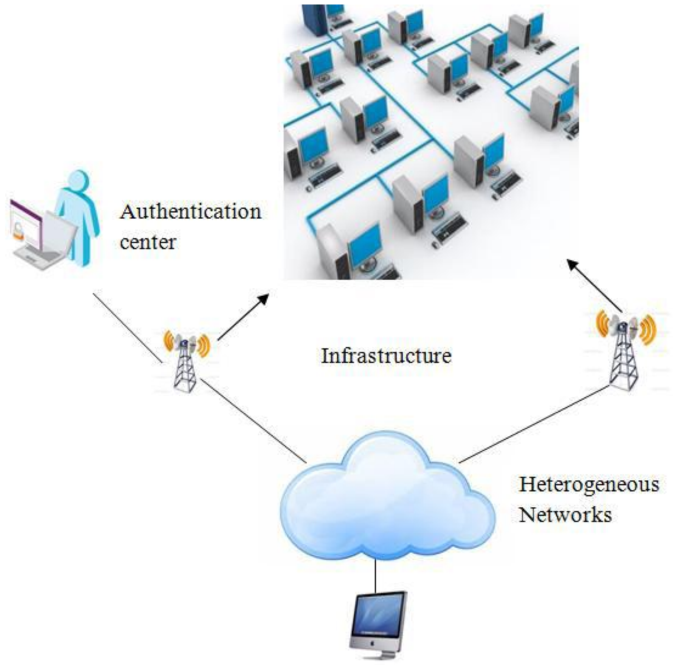

Fig. 2: System Model

2. Key Management

The major security concern in group-oriented communications with access control is the key management. The key management process allowing secure and efficient transmissions to remote cooperative groups by effectively exploiting the mitigating features and circumventing the constraints. In proposed scheme an authentication key is a pair of public and private key and a certificate signed by the base station are pre distributed in each cluster head. The authentication key is used to verify the member sensor node identities. Authentication key is known to all the cluster heads and the base station. The public or 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 of the member sensor node. Public keys are used to verify the certificates of the cluster heads. Authentication key can be calculated by using the following hash function:

$$KAuthi = H (IDi||KCHAuth)$$

3. Key Generation

The key generation algorithm is run by each user u_i to generate the public and private key pair.The user takes n,N as their inputs and value i as the index to generate (pk_i,sk_i) as their pub-lic,private key pair. The key generation process can be done offline mode before the message transmission starts online.Each user randomly chooses public key P_i which belongs to the group Z_p and gener-ates secret key Si as

$$S_i = g^{Pi}$$

4. Encryption

The encryption algorithm is run by each sender who wishes to start the communication with the group of receivers. Here a secret session key k is generated with which messages can be enciphered and sent to the receivers. Only the intended receivers can decrypt that key and hence the secret message. The secret session key is generated as follows:

- Randomly select r,P_i belongs to Z_p and compute
  $S_{i0} = g^{Pi}, Y_{io} = (S_{i1}/S_{in})^{Pi}, c=g^r$
- Extract the public group encryption key as

  $K = e(S_{i1},S_{i2})e(S_{i2},S_{i3}).....e(S_{in-1}, S_{in})$
- Compute

  $S = Ke(S_{in},S_{i0})e(S_{i0},S_{i1})$
- Compute secret session key

  $k=S^r$
- Broacast the header

$$Hdr = (S_{i0},Y_{i0},c)$$

5. Decryption

The Decryption algorithm is run by all the receivers' in order to decrypt the secret session key hidden in the header part and thereby decrypt the message. The decryption process is explained as follows.

- Each receiver Uij publishes
  $Yij = (S_{ij+1}/S_{ij-1})S_{ij}$
- Each receiver indexed by ij can decrypt the secret session key

  $d = S_{ij-1}^{(n+1)Pij} Y_{ij}^{n} Y_{ij+1}^{n-1} ....Y_{ij-2}$
- By using d each receiver can extract the se-cret session key k by computing

$$k=e(d,c)$$

IV. Conclusion

The difficulty of effectively, efficiently and securely broadcasting to a remote cooperative group happens in many freshly appearing networks. A foremost dispute in developing such network systems is to overwhelm 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 living key administration paradigms cannot deal with these trials very effectively. In this paper, we circumvent these obstacles and close this gap by suggesting a innovative key management paradigm. This novel key management paradigm is a hybrid of customary broadcast encryption and assembly key agreement. In such a scheme, each constituent sustains a single public or secret key two. Upon seeing the public keys of the group members, a isolated sender can securely broadcast to any proposed subgroup selected in an publicity hoc way. Following this form, we instantiate a method that is verified protected in the standard form. Even if all the no proposed constituents collude, then they will not extract any helpful data from the conveyed messages. After the public assembly cipher key is extracted, both the computation overhead and the connection cost are independent of the group dimensions.

REFERENCES

[1] Chansu Yu, y Ben Lee , Hee Yong Youn, ”Energy Efficient routing protocols for mobile ad hoc networks”, Wireless Communications and Mobile Computing, John Wiley & Sons, Ltd, PP-959–973, 2003.

[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] Judge, P., and Ammar, M. (2003). Security Issues and Solutions in Multicast Content Distribution: A Survey. Network, IEEE,Vol. 17(1), pp. 30-36.

[4] Bruschi, D., and Rosti, E. (2002). Secure Multicast in Wireless Networks of Mobile Hosts: Protocols and Issues. Mobile Networks and Applications,Vol. 7(6), pp. 503-511.

[5] Diffie, W., and Hellman, M. E. (1976). Multiuser cryptographic techniques. In Proceedings of the AFIPS, pp. 109-112.

[6] M. Burmester and Y. Desmedt, “A secure and efficient conference key distribution system,” Adv. Cryptol., vol. 950, EUROCRYPT’94, LNCS, pp. 275–286, 1995.

[7] 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.

[8] 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.

[9] M. Abdalla, Y. Shavitt, and A. Wool, “Key management for restricted multicast using broadcast encryption,” IEEE/ACM Trans. Netw., vol. 8, no. 4, pp. 443–454, Aug. 2000.

[10] B. M. Macq and J.-J. Quisquater, “Cryptology for digital TV broadcasting,” Proc. IEEE, vol. 83, no. 6, pp. 944–957, Jun. 1995.

[11] J. Lotspiech, S. Nusser, and F. Pestoni, “Anonymous trust: Digital rights management using broadcast encryption,” Proc. IEEE, vol. 92, no. 6, pp. 898–909, Jun. 2004.