Secure Transmission Over Remote Group: A New Key Management Prototype

K.Sudha, J.Prem ranjith, S.Ganapathy,
M.TECH, Assistant Professor, Christ Engineering College, Pondicherry,

B.TECH, Christ Engineering College, Pondicherry,

B.TECH, Christ Engineering College, Pondicherry,

Abstract
The problem of efficiently and more secure broadcasting to a remote co-operative group occurs in many newly emerging networks. The most challenging in devising such systems is to overcome the problems of the potentially limited communication from the group to the sender, the un-avail of a fully trusted key generation center, and the dynamics of the sender. The present key management paradigms can't deal with this problem effectively. In this paper, we circumvent these obstacles and fill this gap by proposing a novel key management paradigm. The new paradigm is a hybrid of traditional broadcast encryption and group key agreement. In such a system, each member maintains a single public/secret key pair. Upon seeing the public keys of the members, a remote sender can securely broadcast to any intended subgroup chosen in an ad hoc way. Following this model, we instantiate a scheme that is proven secure in the standard model. Even if all the non-intended members collude, they can't obtain any useful information from the transmitted messages. After the public group encryption key is extracted, both the computation overhead and the communication cost are independent of the group size. Furthermore, our scheme facilitates simple yet efficient member deletion/addition and flexible rekeying strategies. Its strong security against Collusion, its constant overhead, and its implementation friendliness without relying on a fully trusted authority render our Protocol a very promising solution to many applications.

Keywords:
Access control, ad hoc networks, broadcast, cooperative computing, information security, key management.

1. Introduction

In recent development, WMNs have been recently suggested as a promising low-cost approach to provide last-mile high-speed Internet access. A typical WMN is a multihop hierarchical wireless network. The top layer consists of high-speed wired Internet entry points. The second layer is made up of Stationary mesh routers serving as a multihop backbone to connect to each other and Internet via Long-range high-speed wireless techniques. The bottom layer includes a large number of mobile network users. The end-users access the network either by a direct wireless link or through a chain of other peer users leading to a nearby mesh router; the router further connects to remote users through the wireless backbone and Internet.

Internet Security and privacy issues are of utmost concern in pushing 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 e-mail to some staff of her company via WMNs, so That the intended staff members can read the e-mail with their mobile devices (laptops, PDAs, Smartphone's, etc.). Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce access control of sensitive information to cope with both eavesdroppers and malicious attackers.

MANETs have been proposed to serve as an Effective networking system 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 mission 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 unsecured sensitive information being intercepted by 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 group communications in MANETs are essential.

2. Related work

MOST network applications are based upon the Client–server paradigm and make use of unicast Packet delivery. Many emerging applications, on the other hand,

Manuscript received January 5, 2015
Manuscript revised January 20, 2015

are based upon a Group communications model [1][2]. In particular, they require packet delivery from one or more authorized sender(s) to a large number of authorized receivers. In the Internet, multicast has been used successfully to provide an efficient, best effort delivery service to large groups. We envision that deployment of network applications requiring group communications will accelerate in coming years. As a result, securing group communications[8], i.e., providing confidentiality, authenticity, and integrity of messages delivered between group members, will become a critical networking issue in the near future.

While the technical issues of securing unicast communications for client–server computing are fairly well understood, the technical issues of securing group communications are not. Conceptually, since every point-to-multipoint communication can be represented as a set of point-to-point communications, the current technology base for securing unicast communications can be extended in a straightforward manner to secure group communications.

3. Our Approach

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 (e.g., by retrieving them from a public key infrastructure that is widely available in existing network security solutions), 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 jointly decrypt the secret session key and hence the encrypted message[6]. 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 interaction 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.

First, we formalize the problem of secure transmission to remote cooperative groups, in which the core is to establish a one-to-many channel securely and efficiently under certain constraints. 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 intragroup 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.

Table.1, Diffe-hellman for key exchange between Alice and bob

Alice				Bob		
Secret	Public	Calculates	Sends	Calculates	Public	Secret
a	p, g		$p,g\longrightarrow$			b
a	p, g, A	$g^a \bmod p = A$	$A\longrightarrow$		p, g	b
a	p, g, A		$\longleftarrow B$	$g^b \bmod p = B$	p, g, A, B	b
a, s	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, s

Here are the calculation steps followed in this algorithm that make sure that eve never gets to know the final keys through which actual encryption of data takes place.

- First, both Alice and Bob agree upon a prime number and another number that has no factor in common. Let's call the prime number as p and the other number as g. Note that g is also known as the generator and p is known as prime modulus.
- Now, since eve is sitting in between and listening to this communication so eve also gets to know p and g.
- Now, the modulus arithmetic says that r = (g to the power x) mod p. So r will always produce an integer between 0 and p.
- The first trick here is that given x (with g and p known),it's very easy to find r. But given r(with g and p known) it's difficult to deduce x.
- One may argue that this is not that difficult to crack but what if the value of p is a very huge prime number? Well, if this is the case then deducing x (if r is given) becomes almost next to impossible as it would take thousands of years to crack this even with supercomputers.
- This is also called the discrete logarithmic problem.
- Coming back to the communication, all the three Bob, Alice and eve now know g and p.
- Now, Alice selects a random private number xa and calculates (g to the power xa) mod p =ra. This resultant ra is sent on the communication channel to Bob. Intercepting in between, eve also comes to know ra.
- Similarly Bob selects his own random private number xb, calculates (g to the power xb) mod p = rb and sends this rb to Alice through the same communication channel. Obviously eve also comes to know about rb.
- So eve now has information about g, p, ra and rb.

- Now comes the heart of this algorithm. Alice calculates (rb to the power xa) mod p = Final key which is equivalent to (g to the power (xa*xb)) mod p .
- Similarly Bob calculates (ra to the power xb) mod p = Final key which is again equivalent to (g to the power(xb * xa)) mod p.
- So both Alice and Bob were able to calculate a common Final key without sharing each other's private random number and eve sitting in between will not be able to determine the Final key as the private numbers were never transferred.

Broadcast encryption is used to enable the senders to send the broadcast message to cooperative members of a present Group without need the sender must to interact with the receivers before transmitting secret messages, but it relay on a centralized key server to generate and distribute secret keys for each member in the group[4]. It requires that: 1) before a confidential broadcast message channel is established, numerous confidential separate channels from the key server to each receiver must be constructed 2) the key server contain the secret key of every receivers, it can read all the communications and fully trusted by any sender and the group members also.
It provide the security against collusion Encrypt by the sender and the decrypt by the receiver are both of less complexity and it enable to send-and-leave broadcasts message to remote cooperative groups without fully trusted third party. Even an attacker cannot retrieve any information about the messages transmitted by the sender in the remote group.

4. Key management

The public key is created and certified by a certificate Authority, but the secret key is hold only by the receiver. A sender in a remote group can receive the receiver's public key from the certificate authority and validate the authentication of the public key by verifying its certificate, which provide that no direct communication from the receivers to the sender. Then, the sender can send secret messages to any receivers in a remote group. Authority can be done on the offline before the message transmission by the sender[7][9]. Security policy may affect the stringency of cryptographic requirements, depending on the susceptibility of the environment in questions to various types of attack.
Techniques for distributing public keys
- Authentication trees:
Authentication trees provide a way for making public data to be available with verifiable authenticity, by using a tree structure with a suitable hash function, and authenticating the root value.
- Public-key certificates:
Public-key certificates are a device by which public keys may be stored, distributed or forwarded over unsecured media without danger of undetectable manipulation
- Key separation and threat of key misuse:
The principle of key separation is that keys for different purposes should be cryptographically separated. The threat of key misuse may be addressed by techniques which ensure that keys are used only for those purposes pre-authorized at the time of key creation.
Techniques for controlling use of symmetric keys:
The main technique is the use of control vectors Control vectors provide a method for controlling the use of keys, by combing the idea of key tags with the mechanism of simple key notarization.

5. Optimizations

The pairing is providing some optimizations. These may involve precomputation, and in some storage availability may introduce a problem. We can consider these optimizations in some other ways. If both left-hand and right-hand arguments are, pairing itself can be pre calculated and stored. If the left-hand parameter, its multiples that rise in its multiplication by the variable can be precalculated and it must store in coordinates. We consider no advantage can be taken on right-hand parameter, but only for a Type-1 pairing, symmetry can be move it to the left-hand side and precalculate as before. The protocol on a Type-3 pairing it may be useful for reversing the roles of the left-hand and right-hand parameters in the protocol. Note that if storage is not problem and the left-hand parameter the size of din E (Fpd) is not matter, and so it is no need to use a pairing-friendly curve . It will be advantage to use the pairing which provides the loop reduction, and limited storage need for precomputation by the degree of loop reduction can be achieve. scheme with constant-size cipher texts is a modified version of BGW by the same authors (dubbed BGW2 from now on), which has cipher texts that are double the size of our scheme (i.e., four group elements vs. our two). BGW2 is proved selective CCA secure under BDHE, plus the assumption that a signature scheme used in the construction is strongly unforgivable, which is an assumption of comparable strength as UOWHF.

6. Broadcast Encryption

The basic tree scheme requires only log2 n keys to be stored in each receiver. Therefore it is reasonable to consider schemes with slightly more keys: for populations of several millions, we can afford to keep twice or four times as many keys in a receiver. In order to generate the extra key sets, we start with a "level-degree" profile, which specifies how

many keys each user should hold at each level[9]. For a level with set size , a degree of d implies that each user should belong to extra sets(d-1), in addition to the one basic tree set it belongs to at this level. Thus we need to be able to generate nd/k sets of size , such that each user belongs to exactly d of them. We
Achieve this by randomly permuting the N users times (D-1), and for each random permutation we add the users in positions (i-1)k+1,…….,ik as a set ,for i=1,…….,n/k.

Key Establishment Algorithm

Input: Target set K,
establishment key allocation $\mathcal{S} = \{S_1, \ldots, S_m\}$.

0. $R \leftarrow \emptyset$; $\mathcal{C} \leftarrow \emptyset$
1. **Repeat**
2. $\mathcal{A} \leftarrow \{S_i : \frac{|S_i \setminus R|}{|(K \cap S_i) \setminus R|} \leq f\}$.
3. $A \leftarrow S_i \in \mathcal{A}$ which maximizes $|(K \cap S_i) \setminus R|$.
4. $R \leftarrow R \cup A$; $\mathcal{C} \leftarrow \mathcal{C} \cup \{A\}$.
5. **until** the candidate collection $\mathcal{A}$ is empty.
6. **return** $R, \mathcal{C}$.

To calculate the redundant establishment key allocation over a universe u of size n .then
$t_{max}(s) \geq \lfloor \{\Omega^{\log}_{n} \; {}^{\log n}$, where deg(s)=O(log n)
The required number of keys a receiver needs to store. As we said before, this is typically a small fixed value which we can reasonably model by $log_2 n$ or n^e inverse lower bound, on the number of transmissions. Asymptotically we can obtain the following bound.

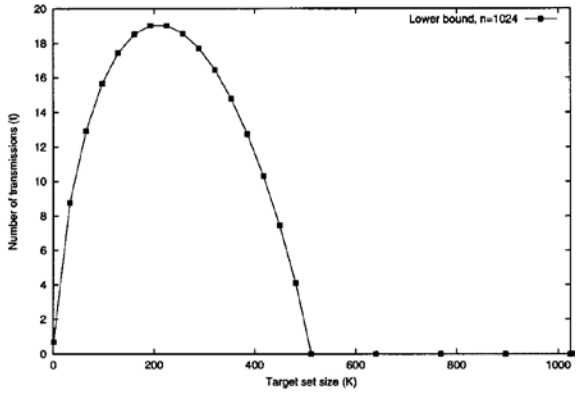

Fig .2. Number of transmission (t) as the function represent to the target set size (k).

7. CONCLUSION

We proposed a new key management paradigm for secure transmission over remote group i.e. to enable add-and-delete broadcasts message to remote cooperative groups without fully third party. Our proposed has been proven by secure in the standard model. Although it provide less complexity and less time take for encryption. These features provide sender to send the message to remote group in more securely and faster way communication.

References

[1] C. K. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," IEEE/ACM Trans. Network., vol. 8, no. 1, pp. 16–30, Feb. 2000.
[2] W. Yu, Y. Sun, and K. J. R. Liu, "Optimizing the rekeying cost for contributory group key agreement schemes," IEEE Trans. Depend. Secure Compute. vol. 4, no. 3, pp. 228–242, Jul.–Sep. 2007.
[3] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short cipher texts)," Adv. Crypto., vol. 5479, EUROCRYPT' 09, LNCS, pp. 171–188, 2009.
[4] R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2007–2025, May 2008.
[5] Y. Mao, Y. Sun, M. Wu, and K. J. R. Liu, "JET: Dynamic join-exit tree amortization and scheduling for contributory key management," IEEE/ACM Trans. Network., vol. 14, no. 5, pp. 1128–1140, Oct. 2006
[6] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: A novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," IEEE Trans. Parallel Distributed System, vol. 21, no. 2, pp. 203–215, Feb. 2010.
[7] Y. Mao, Y. Sun, M. Wu, and K. J. R. Liu, "JET: Dynamic join-exit tree amortization and scheduling for contributory key management," IEEE/ACM Trans. Network., vol. 14, no. 5, pp. 1128–1140, Oct. 2006
[8] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: A novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," IEEE Trans. Parallel Distributed System, vol. 21, no. 2, pp. 203–215, Feb. 2010.
[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.
[12] A. Fiat and M. Naor, "Broadcast encryption," Adv. Cryptol., vol. 773, CRYPTO'93, LNCS, pp. 480–491, 1993.
[13] C. K. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," IEEE/ACM Trans. Netw., vol. 8, no. 1, pp. 16–30, Feb. 2000.