Secure Multicast Transmission Scheme for Overlay Networks

K.pavya

Assistant Professor & Computer Science & Bharathiar University
India

Abstract:
Secure multicast transmission schemes are used to transfer data to a set of nodes. Membership in secure multicast groups is dynamic and requires multiple updates in a single time frame. Storage cost and rekeying cost are considered in the secure multicast transmission. The system manages long standing members and shortly lived members separately. Long standing members need to store smaller number of keys than short-lived members.

The system manages variable storage levels for key management. Hierarchical key management algorithm is used to manage group key values. The RSA and Advanced Encryption Standard (AES) algorithms are used for the communication security. The system manages membership addition and removes operations. The key management scheme is not optimized for overlay networks, End node based multicast transmission is not optimized, Traffic overhead is high and Transmission and listen mode energy levels are not managed problems are identified from the existing security models.

The secure multicast transmission supports key management under multicast groups. The storage and key revocation operations are managed by the system. The system is enhanced to manage keys under overlay networks. The traffic and energy control mechanisms are integrated with the system. The system is designed to manage storage and key revocation process. Multicast group and key management operations are integrated in the system. The system is enhanced to manage group keys under overlay network environment. The key management messages are controlled in the system.

Keywords— multicast transmission, key revocation, Group key exchange, Overlay network, Advanced Encryption Standard

I. INTRODUCTION:

A. OVERLAY NETWORKS

An overlay network is a computer network which is built on the top of another network. Nodes in the overlay can be thought of as being connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network.

The multicast group construction and key management system is designed to handle multicast group communication with security. The key values are maintained under the wireless nodes. The network is extended using overlay models. The overlay network is constructed with the support of end nodes. The end node is used to extend the coverage of the network. The key values are exchanged between the nodes using the end nodes. The storage and communication aspects are considered in the key management process. The system is designed with the following specific objectives.

- To construct the overlay networks with wireless nodes
- To establish base station and end node based connections
- To verify the neighbor nodes in periodical intervals
- To maximize the coverage of the wireless network base station
- To build the multicast groups under the overlay networks
- To prepare the group key for each multicast group
- To handle key revocation process on node join and leave situations
- To manage communication and storage overheads

II. LITERATURE SURVEY

Group key exchange (GKE) protocols provide participants with a shared secret key which can be further used to achieve confidentiality and authentication in different group applications. Various group key exchange protocols are focused on their security arguments concerning the resistance against different types of attacks [1]. The following protocol issues are compared for the system. (i) protocols with heuristic security arguments based on informally defined security requirements and (ii) protocols that have been proven secure in one of the existing security models for group key exchange. The system is focused on various informally defined security requirements and currently known formal security models for group key exchange protocols. The main security requirements that is most relevant for the following analytical survey. The description is done along the lines. The main contributions of the system are as follows:

- The family of key management algorithms for efficiently distributing the new group key when multiple users are revoked from the group. The storage at the group controller is linear and the storage at the users is logarithmic in the size of the group. Some popular algorithms are members of this family.
- Some techniques are used to reduce the number of keys stored by the users and the group controller. Two key assignment techniques are constructed using one-way hash functions. The key assignment techniques can be used to add users to the group and to provide preferential treatment to long standing users in the group. The applicability of the algorithms is analyzed with scenarios where users have varying requirements or capabilities.
- A hybrid key management algorithm is composed by combining the algorithm with an existing solution. Such a combination is useful when users have varying computational requirements.

The group key management systems are focused to provide security for mobile ad-hoc network nodes. The current system is focused to provide key management scheme for the overlay networks [2]. The overlay network nodes are communicated with the base station and neighbor nodes. The key values are distributed across the network area. The storage levels for the nodes are considered in the key list management process. The system reduces the key storage overhead. The members join and leave operations initiates the key distribution process. The system uses the RSA and Advanced Encryption Standard (AES) algorithm.

Mitchel et al. described the notion of key control, i.e., an attack where an adversary tries to influence the resulting value of the computed session group key .Note that opposite to group key distribution protocols, in group key exchange protocols no party should be able to choose the resulting group key on behalf of other participants [3]. Ateniese et al. proposed a related notion called contributiveness that encompasses the fact that all protocol participants must equally contribute to the computation of the group key.

Two different versions of key control and contributiveness are can be currently found in the literature. A weaker form like implicitly considered by Bresson and Catalano assumes honest protocol participants that have biased source of randomness so that a curious adversary can possibly gain extra information and break the AKE-security of the protocol. A stronger version like considered by Bohli et al. assumes malicious participants that try to influence honest participants computing some special value as the resulting group key. Note that according none of the currently available security models for GKE protocols provides definitions concerning key control and contributiveness that consider strong corruptions.

Many group key exchange protocols described in the survey can be seen as extensions of the following two well-known protocols: two-party key exchange by Diffie and Hellman and three-party key exchange by Joux.

The Rivert, Shamir, Adelman (RSA) scheme is a block cipher in which the Plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits or 309 decimal digits.

Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2(n)$; in practice, the block size is k bits, where $2^k < n \leq 2^{k+1}$. Encryption and decryption are of the following form, for some Plaintext block M and cipher text block C

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the value of n. The sender should know the value of e, and the receiver should know the value of d. Thus, this is a public-key encryption algorithm with a public key of KU = { e,u} and a private key of KR ={d,n}.

For this algorithm to be satisfactory for public-key encryption, the following requirements must be met

- It is possible to find values of e, d, n such that $M^{ed} = M \bmod n$ for all $M < n$.

- It is relatively easy to calculate M^e and C^d for all values of $M < n$.
- It is infeasible to determine d given e and n.

The first requirement to find a relationship of the form

$$M^{ed} = M \bmod n.$$

Given two prime numbers, p and q, and two integers n and m, such that n=pq and 0<m<n, and arbitrary integer k, the following relationship holds

$$m^{k\varphi(n)+1} = m^{k(p-1)(q-1)+1} = m \bmod n$$

where φ(n) is the Euler totient function, which is the number of positive integers less than n and relatively prime to n. p, q are prime integers

$\varphi(pq) = (p-1)(q-1)$ the relationship if

$ed = k\varphi(n) + 1$

is equivalent to saying

$$ed = 1 \bmod \varphi(n)$$

$$d = e^{--1} \bmod \varphi(n)$$

That is e and d are multiplicative inverses mod φ(n). According to the rules of modular arithmetic, this is true only if d (and therefore e) is relatively prime to φ(n). Equivalently, gcd(φ(n),d) = 1. The ingredients are the following,

p.q+, [two prime numbers]
(private, chosen)
n = pq (public, calculated)

e, with $\gcd(\varphi(n),e) = 1; 1 < e < \varphi(n)$ (public, chosen)

$d = e^{-1} \bmod \varphi(n)$ (private, calculated)

The private key consists of {d, n} and the public key consists of {e, n}. Suppose that user A has published its public key that user B wishes to send the message M to A. Then B calculates $C = M^e$ (mod n) and transmits C. on receipt of this cipher text, user A decrypts by calculating $M = C^d$ (mod n).

$d = e^{-1} \bmod \varphi(n)$

Therefore,

$ed = 1 \bmod \varphi(n)$

ed is form kφ(n) +1 . but by the corollary to Euler's theorem, given two prime number, p and q, and integers n =pq and M, with 0 < M < n.

$$M^{k\varphi(n)+1} = M^{k(p-1)(q-1)+1} = M \bmod n$$

So $M^{ed} = M \bmod n$,

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n = M \bmod n$$

Key Generation

Select p,q
p and q both prime , p≠q
Calculate n = p x q
Calculate $\phi(n)=(p-1)(q-1)$

Select integer e
$\gcd(\phi(n),e) = 1; 1 < e < \phi(n)$

Calculate d

$d = e^{-1} \bmod \phi(n)$

Public key	KU = {e, n}
Private key	KR = {d, n}

Encryption

Plaintext	M <n
Cipher text	$C = M^e$ (mod n)

Decryption

Cipher text	C
Plaintext	$M = C^d$ (mod n)

This standard specifies the Rijndael algorithm a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in this standard.

Throughout the remainder of this standard, the algorithm specified herein will be referred to as the AES algorithm [4]. The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256".

The system is focused on contributory group key agreement. Two important trends are combined in group key management: (1) key trees to efficiently compute and update group keys and (2) Diffie – Hellman key exchange to achieve provably secure and fully distributed protocols. The main result is a simple, secure, robust and efficient key management solution, called Tree-based Group Diffie–Hellman (TGDH).

A method is proposed for designing the multicast key management tree for a group of users in a cellular network [5]. Traditional tree-based multicast key management schemes do not consider the effect of the network topology upon the delivery of the rekeying messages, and therefore waste network resources by sending rekeying messages to users who do not need them. This issue is addressed by proposing to match the key management tree to the network topology, thereby localizing the delivery of the rekeying messages and reducing the communication costs.

In a secure group communication system, date privacy can be achieved by a shared group key. Only the authorized members know the group key [6]. But usually group memberships vary over time. Whenever some members join or leave the group, the shared key needs to be changed. Thus there must exist an efficient group key management system to maintain group memberships such that only authorized group members are able to access the group key for that group. At the same time the group key management system must be responsible for generating, updating and delivering the keys to the authorized members.

There are two desirable properties for the shared group key: first, the BAC (backward access control) property, which means that new users should not be able to decrypt past group communications with their new keys; second, the FAC (forward access control) property, which means that the evicted users should not be able to decrypt future group communications with their old keys.

For a group with many users, join/leave requests happen frequently. Since a group key management center needs to send out a lot of re-keying messages to authorized users with limited bandwidth, the bandwidth for re-keying is the biggest bottleneck in current applications [7]. Communication complexity is measured by the number of messages that need to be sent for re-keying in unit time.

There are two kinds of re-keying protocols. One is the individual re-keying protocol, in which the system updates the group key every time a request is received. Another kind of protocol is the periodic batch re-keying protocol, in which the group controller does not immediately perform updating for each request, but waits until several requests have accumulated to perform re-keying.

III. COMPARITIVE STUDY:

The following drawbacks are identified from the existing system.

- The key management scheme is not optimized for overlay networks
- End node based multicast transmission is not optimized
- Traffic overhead is high
- Transmission and listen mode energy levels are not managed

In the proposed system the secure multicast group communication is designed with key revocation and storage management mechanism. The storage space is allocated with reference to the lifetime values. The key values are maintained in different patterns under the nodes. The overlay networks are formed to extend the network coverage. The IP based multicast is switched into end node based multicast mechanism. The system can be used for the following application domains. Multicast group based learning and discussion environment and group based auction process are supported by the system. Group bases service management and trade handling is also provided by the system. Defense and commercial applications are also supported by the system.

Two-Party Key Exchange Protocol

- The protocol proposed by Diffie and Hellman is the earliest key exchange protocol that allows two participants, U1 and U2, compute a secret key k over a public communication channel. Mathematical operations of the protocol are performed in a multiplicative group G where the well-known Discrete Logarithm (DL) problem is believed to be intractable. Let g be a generator of G. Obviously, the resulting shared key has the form k = gx1x2 .
- Each Ui, i ∈ {1, 2} chooses a random X_i ∈ R Zq and sends $Z_i := g^{xi}$ to U3−i.
- Each Ui,i ∈ 2 {1, 2} computes ki := $(z3{-}i)^{xi}$.
- Two-Party Key Exchange Protocol by Diffie and Hellman tic security of k against passive adversaries relies on the Decisional Diffie-Hellman (DDH) assumption. The original Diffie-Hellman protocol does not provide protection against impersonation attacks. A large number of variations has been proposed after the

invention of the protocol to improve its security degree. Mostly all group key exchange protocols considered in the survey can be seen as more or less complex extensions related to this original Diffie-Hellman key exchange protocol.

Three-Party Key Exchange Protocol

- Joux proposed the following efficient key exchange protocol designed for three participants. The protocol uses a bilinear map e : G1 × G1 ! G2 where G1 is an additive group of prime order q and G2 a multiplicative group of the same order, e.g., G1 is a subgroup of the group of points on an elliptic curve E over a finite field, G2 a subgroup of a multiplicative group over a related finite field, and ˆe is an appropriate pairing on E. Also, an element P 2 G1 with e(P, P) 6= 1G2 should be publicly known. The protocol between U0, U1, and U2 proceeds as follows. Obviously, at the end of the protocol each user computes
- Each Ui chooses xi 2R Z_q and broadcasts yi := xiP to all other users.
- Each Ui computes ki := ˆe(y(i+1)mod 3, y(i+2)mod 3)xi .
- Three-Party Key Exchange Protocol by Joux the group key k = ˆe(P, P)x0x1x2 . The protocol requires only one communication round. Although not explicitly, the semantic security of the protocol against passive adversaries is based on the Bilinear Diffie-Hellman (BDH) assumption. Joux' HGI Network and Data Security Group Technical Report 2006/03 8 protocol does not provide any form of authentication.

Relationship between Group Key Exchange Protocols

- Regardless of the separation into group key exchange protocols with heuristic security arguments and protocols with security proofs in the available security models. Some of the protocols included in the survey have certain similarities.
- The protocols can be considered as modifications of the static group key exchange protocol proposed by Burmester and Desmedt. These protocols are characterized by the constant number of communication rounds and are, therefore, scalable for large groups. Some of these protocols derive the group key from bases whose discrete logarithms are outputs of an additive cyclic function.
- The protocols in can be considered as modifications of the static group key exchange protocol proposed by Ingemarsson, Tang, and Wong. Most of these protocols derive the group key from bases whose discrete logarithms are outputs of a symmetric multiplicative function. In Particular, from the value of the form gx1···xn where g is a generator of a cyclic group G where the DL problem is believed to be intractable, and every xi, i 2 [1, n] is a private exponent of participant Ui. This form can be seen as a "natural" extension of the two-party Diffie-Hellman key exchange protocol described above.
- The protocols derive the group key from a value obtained by an iterative application of the two-party Diffie-Hellman protocol. The earliest protocol of this class was proposed by by Steer, Strawczynski, Diffie, and Wiener. Most of the protocols of this class arrange participants into a logical binary tree structure which is either linear or balanced. In general, each user is logically assigned to a leaf node of a binary tree T. The system uses labels hl, vi to uniquely identify a node of a tree where l 2 {0, dT } is a corresponding level of T, d_T the depth of T, and v 2 N the nodes' position within the level. Note that in linear binary trees the depth dT is linear in the number of participants whereas in the balanced binary trees dT is logarithmic.

The algorithm enables the group controller to deal with heterogeneous set of users that have different capabilities. With this capability, users with high capability can benefit from it, while users with low capability can still participate. The algorithm can provide differential service to users that are long term versus those that are short term. The hierarchical algorithm can be combined with the logical key hierarchy. Such hybrid schemes provide additional options for the group controller to adapt to heterogeneous systems where users have varying requirements and capabilities.

The algorithms are also suited for overlay multicast applications. In overlay multicast, the end nodes perform the processing and forwarding of multicast data without using IP multicast support. As these tasks result in increased overhead at the end nodes, reducing control traffic is an important problem for overlay multicast. The algorithms reduce the overhead at the end nodes by reducing the number of group key update messages sent by the group controller. These benefits are also desirable in wireless systems which are constrained in battery power. The measurements on wireless network interface cards show that transmission consumes more battery power than reception if the idle listening time of the interface is small. As streaming multicast sessions result in minimal idle time, the energy consumption is dominated by the amount of transmitted data. Thus, in heterogeneous systems which compose of wired and wireless systems, the algorithms can be used to improve battery longevity of wireless systems by reducing the amount of traffic it need to transmit forward.

The multicast group communication with security system is designed for the overlay networks. The wireless nodes are communicated with the support of the base station and the end nodes. The coverage extension is achieved by the end nodes. The overlay communication is secured with personal and group key values. The groups are formed with multicast group mechanism. The system manages the group key and public key values for each node. The storage and traffic factors are considered in the group key management process. The system is designed with the following advantages.

- Efficient data delivery model with security
- Limited storage usage for key management
- Scalability and connectivity is high
- Key revocation period is minimized

IV. PROBLEM DESCRIPTION

The wireless networks are constructed in different ways. The mobile ad-hoc networks, wireless networks and wireless mesh networks. The group communication is carried out with the group members. The node joins and leave operation initiates the key generation and issue process. The key values are maintained under the nodes only. Each node maintains a pair of key values that are node key and group key. The node key value is used to handle node to node communication. The group key value is used to perform communication with in the group members. The system is designed for the overlay networks. The base station and neighbor nodes are used for the communication. The system reduces the storage overheads. The RSA (Rivert, Samir and Adelman) and AES (Advanced Encryption Standard) algorithms are used in the system.

V. CONCLUSION

In the secure multicast transmission scheme a family of algorithms is used to provide a trade-off between the number of keys maintained by the users and the time required for rekeying due to the revocation of multiple users. The algorithms reduce the cost of rekeying. The schemes are based on the use of one-way hash chains that allow one to reduce the number of keys further without increasing the rekeying cost.

The algorithm enables the group controller to deal with heterogeneous set of users that have different capabilities. With this capability, users with high capability can benefit from it. The RSA algorithm is used to manage node to node communication. The Advanced Encryption Standard (AES) algorithm is used to manage group communication with security. The key values are stored in local storages of the nodes. The key values are maintained for the neighbor node only. The group key distributed for the member nodes. The overlay networks are formed with end nodes. The end nodes and base station communication are managed with intermediate nodes. The traffic levels and key storage details are used system analysis.

The system operations are tested under the simulation environment. The system is integrated with the traffic and energy control mechanisms and it supports overlay network multicast process. Storage usage is controlled by the system. Traffic levels are managed by the system. The system reduces the energy levels.

REFERENCES:

1. Dennis Campbell and Center for International Legal Studies “Solutions for Denial of Service Attacks” Publisher: Oxford University Press, USA 2005.
2. Niels Ferguson and Bruce Schneier, “Overlay Networks”, Publisher: Wiley, 2003.
3. Sudip Misra, Isaac Woungang and Subhas Chandra Misra ‘Guide to Wireless Ad Hoc Networks (Computer Communications and Networks)’, Publisher: Springer, 2009.
4. Wenbo Mao “AES algorithm” Publisher: Prentice Hall PTR; 1st edition 2003.
5. Y.-H. Chu, S.G. Rao, S. Seshan, and H. Zhang, “A Case for End System Multicast,” IEEE J. Selected Areas in Comm., vol. 20, no. 8, pp. 1456-1471, Oct. 2002.
6. F. Zhu, A. Chan, and G. Noubir, “Optimal Tree Structure for Key Management of Simultaneous Join/Leave in Secure Multicast,” Proc. Military Comm. Conf. (MILCOM), 2003.
7. http://www.ccs.neu.edu/home/ahchan/wsl/papers/group-key-1-tech-rept.pdf