A Key Management Scheme based on Cluster Grouping Structure for Mobile Networks

Feng Xiaorong[1, a], Lin Jun[2,b] and Jia Shizhun[3,c]

[1] Software Quality Testing Engineering Research Center, China Electronic Product Reliability and Environmental Testing Research Institute, Guangzhou, Guangdong

[2] Software Quality Testing Engineering Research Center, China Electronic Product Reliability and Environmental Testing Research Institute, Guangzhou, Guangdong

[3] Software Quality Testing Engineering Research Center, China Electronic Product Reliability and Environmental Testing Research Institute, Guangzhou, Guangdong

[a]fengxr@ceprei.com [b]linjun@ceprei.com, [c]jiasz@ceprei.com

Keywords: cluster grouping, mobile network, elliptic curve cryptography, key management

Abstract. In according to elliptic curve cryptography algorithm, the paper put forward a kind of ECC key management scheme based on logic cluster grouping structure for mobile networks. The mobile nodes are divided according to cluster classification, and then, each cluster is logically divided into multiple groups. The communication key is shared within groups and the cluster header is in charge of each group's key on real time. Mobile nodes communicate with cluster header through shared private key within groups so as to ensure about the security of communication. Key exchange protocol based on ECMOV is adopted for all nodes to participate in the group key construction, while a specific period is designed to update the key, which would effectively avoid key leakage. Analysis illustrates that the proposed scheme can effectively reduce the security risks during key exchanges in communication, which is suitable for intelligent mobile terminal platform with limited resource.

Introduction

As the mobile Internet technology is developing fast, the mobile applications based on intelligent mobile terminal platform increase gradually and the number of software applications is quite striking. However, the security risks induced by Apps have not got a good solution and the attack level on network intrusion by hackers are getting more and more serious, which brings in negative impact for both developers and users. Thus software security issues specific to mobile applications have gradually become a hot spot. Security vulnerabilities in mobile Internet authentication and encryption make it possible for hackers to decode the keys in minutes rather than hours. Therefore, software security reinforcement and certification has become very necessary.

At present, IEEE802.1 X adopts EAP Authentication Protocol (Extensible Authentication Protocol) of PPP (Point - to - Point Protocol) Protocol proposed by IETF can be extended. In the authentication scheme, the EAP - TLS Authentication mechanism using RSA cryptosystem can provide mutual authentication and key management. The security assurance is on the foundation of the integer factorization complexity, where the algorithm complexity could achieve exponential level. RSA key management needs to meet the binary length of more than 1024, where the realization cost is higher. The security feature of Elliptic Curve encryption system (Elliptic Curve Crypto system, ECC) is based on the Elliptic Curve discrete logarithm problem (ECDLP) and the algorithm complexity could satisfy ample exponential, which makes it possible to achieve higher safety with shorter and cipher key than RSA.

Due to the limited hardware processor execution efficiency on the intelligent mobile terminal equipment, the computational capability, memory, and network bandwidth compared with traditional mobile Internet network has certain disadvantages. While, in dealing with security reinforcement and authentication technology for mobile applications, it is necessary to choose a suitable encryption scheme for intelligent mobile terminal embedded platform. Early research illustrates that the computational complexity of public key cryptosystem is too high, which could not be applied to intelligent mobile terminal platforms with limited resources. However, recent studies have shown

that the public key encryption system can be used in the mobile Internet, and ECC encryption system is one of the important research hotspot.

In this paper, a new kind of ECC key management scheme based on logic cluster grouping structure in mobile Internet network environment is put forward. On the foundation of EAP - TLS authentication protocol, the proposed method induces ECMOV key exchange protocol in combination with elliptic curve cryptosystem. Analysis illustrates that the proposed scheme can effectively reduce the communication energy consumption on the premise of security insurance, which is suitable for intelligent mobile terminal platform with limited resource.

Key management scheme based on elliptic curve encryption

Elliptic curve cryptography system can achieve high security with lower system consumption and communication delay which is especially suitable for the limited computing power and communication bandwidth. At present, the existing literature has presented a key management scheme with no secure channel. The formation of ECC key management scheme is based on elliptic curve discrete logarithm of the algorithm complexity, and in combination with threshold key management mechanism. However, in this scheme, the safety distribution of each node in the encryption transmission does not take into account. Researchers also proposed a key management scheme with three layers trust structure. The mobile nodes are divided into three categories including authentication center, service nodes and ordinary nodes. In according to the elliptic curve encryption algorithm, the service node is responsible for the key generation and distribution, and the certification center is in charge of management service nodes. Research showed that the safety management right of the service node is too high, which is easy to be used by malicious attackers and poses security threats.

Cluster grouping topology structure for mobile nodes

On the basis of common network structure of wireless sensor network, in this paper, the mobile nodes in the Internet network are designed with cluster grouping structure, which are grouping within the cluster, and set up each group as a unit for key management. In each group, the ordinary nodes submitted data directly to the cluster headers. The maximum number of nodes each group contained is set with t. Each group and the cluster head nodes share a pair of public and private keys. Other nodes except from the cluster headers within group negotiate a pair of public and private key. The group public key and private key are stored by cluster headers.

In each cluster, all the nodes only communicate with cluster headers for data transmission. Cluster grouping is designed with logical structure, which is not related with the exact location of the communication nodes. The mechanism of new nodes added to cluster is the same with mobile nodes joined to the mobile network. A communication cluster is specified with N nodes, thus the length of the cluster is set as N_{group_id}, and operations related with key creations and updates are implemented within group. The cluster grouping network topology structure for mobile node is shown in Figure 1.

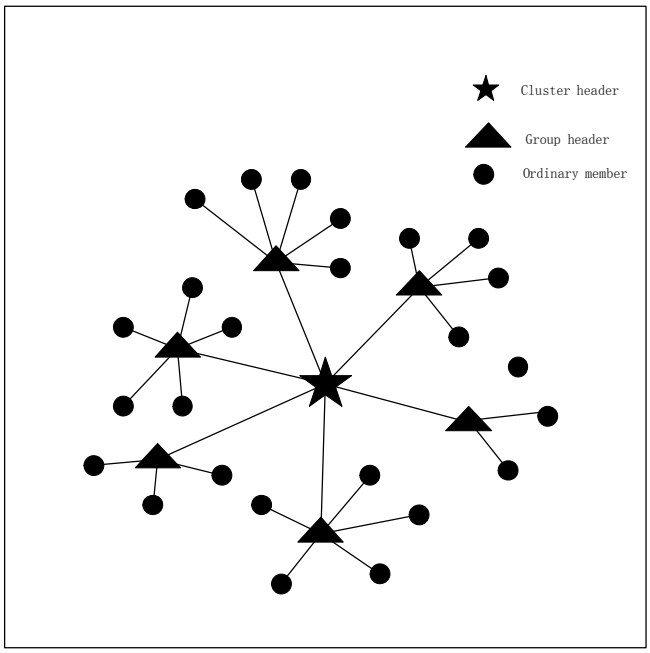

Figure 1 mobile node cluster grouping network topology structure

Elliptic curve encryption mechanism

Elliptic plane curve is determined by Weierstrass equation. Assume that the elliptic curve is $EP(a,b)$ and point G is a base point on the elliptic curve. We select two private key k_a and k_b for Node A and Node B, where K_a and K_b are the corresponding public key. Message is mapping to a point CM on $EP(a,b)$ curve after encryption by Node A. The symmetry encryption achieves agreement between Node A and Node B in message transmission. When in Node A and Node B communication, a random integer is generated, and Node A sends cipher text CM to Node B in according to $CM=\{rG,K_m+rK_b\}$. Node B decrypts the cipher text with $K_m+rK_b-k_b*rG=K_m+r*k_bG-k_b*rG=K_m\}$ and after the inverse mapping plain text would be received. The public transport parameters only include $\mathrm{EP(a,b)}$ K_a, K_b and G which ensures about the safety in process of transmission.

Key management scheme implementation on mobile node

Node initialization

The process of node initialization is as follows:

(1) Choose an offline trusted center CA, which is in charge of initialization for each node in the network initialization phase;

(2) CA assigned a unique ID tag $node\_id$ for each node and the cluster header allocate cluster ID tag $cluster\_id$ and cluster length ID tag $group\_id$ in establishing cluster grouping topology structure;

(3) CA selects a secure elliptic curve $EP(a,b)$, and chooses a base point G in the plane curve. A specific Hash function is used for message authentication codes;

(4) The pair of communication keys could be obtained through the encryption algorithm. Define the symmetric encryption algorithm $K_c=F(k,P)$, where k is the node's private key and $P=kG$ is the point on the elliptic curve for the node to announce. Based on the characteristics of ECC encryption algorithm $P=kG$ is k times combined operations for base point G. As parameter k is a large integer, solving $P=kG$ equation through discrete logarithm is not feasible in theory, which could guarantee the safety of node initialization.

Establishment and update for group key management

In the proposed model, the logic clustering is a recursive process. While, each new node joins into the network could be regards as applying for joining into the cluster. When the number of mobile nodes achieves cluster length, the group key establishment is made in preparation.

In mobile network, the attacker could decode the encryption by continuous flow analysis in the network encrypted data. In the designed scheme, automatic cyclical key update mechanism is set up, which can effectively avoid such kind of network safety injection. Key update is implemented within each group by cluster headers. Here, we assign specific period value T for key update and when the communication time achieves the cycle time, key update operations would be implemented.

Assume that the specified group identity with ID tag $group\_id$ and the cluster length is $N_{\text{group\_id}}$. $N_{\text{node\_id}}$ is an ordinary mobile node in the cluster. The group key update operation is as follows:

(1) The mobile node $N_{\text{node\_id}}$ sends public message, $public(group\_id, node\_id, K_{node\_id})$, while, $K_{\text{group\_id}}$ is the node's public key. $K_{\text{group\_id}} = k_{node\_id} * G$. Other nodes save the public key after the message reception.

(2) The mobile node will be deleted from the node sets when the previous node receives the public message, and it will be identified as N_{pre}. Select a new node for the next key exchange, which is named as N_{next}. The agreement key transmitted from the previous node is Q and in initialization the agreement key of the cluster header is base point G. $Q = k_{node\_id} * Q$. Let $N_{\text{node\_id}} = N_{next}$ and repeat step 1 and step 2. Finally, the nodes exchange keys on the basis of ECMOV exchange protocol inner groups. If the nodes are null, send message $Message(group_id, node_id, Nodes)$to the next mobile node N_{next}, otherwise turn to step 3.

(3) When perform the step 3 for the first time, the calculated result Q is regarded as the shared group key $K_{\text{group\_id}}$ of cluster communication. Otherwise, select M_1 and M_2 from reply message received by N_{pre} . In accordance with elliptic curve cryptographic decryption algorithm $K_{group\_id} = M_2 - k_{node\_id} * M_1$, shared group key is obtained. Look up the public key K_{pre} of node N_{pre} in memory, select a random integer and generate elliptic curve scalar $M = \{M_1, M_2\}$, while, $M_1 = rG$, $M_2 = K_{group\_id} + r * K_{pre}$. If N_{pre} is null, turn to step 4, otherwise $N_{\text{node\_id}}$ sends message $Reply_key(group_id, node_id, M_1, M_2)$to N_{pre} and repeat step 3.

(4) After cycle recursion each mobile node in the group gets the same group key $K_{\text{group\_id}}$. Meanwhile, $K_{\text{group\_id}}$ is mapped into integer form $Z_{\text{key\_group\_id}}$ by mobile node $N_{\text{node\_id}}$ and is stored in memory. The group header transmits $K_{\text{group\_id}}$ to cluster header through elliptic curve cryptographic decryption algorithm, thus the cluster get new group keys.

Tthe process of group key establishment and update is shown in Figure 2.

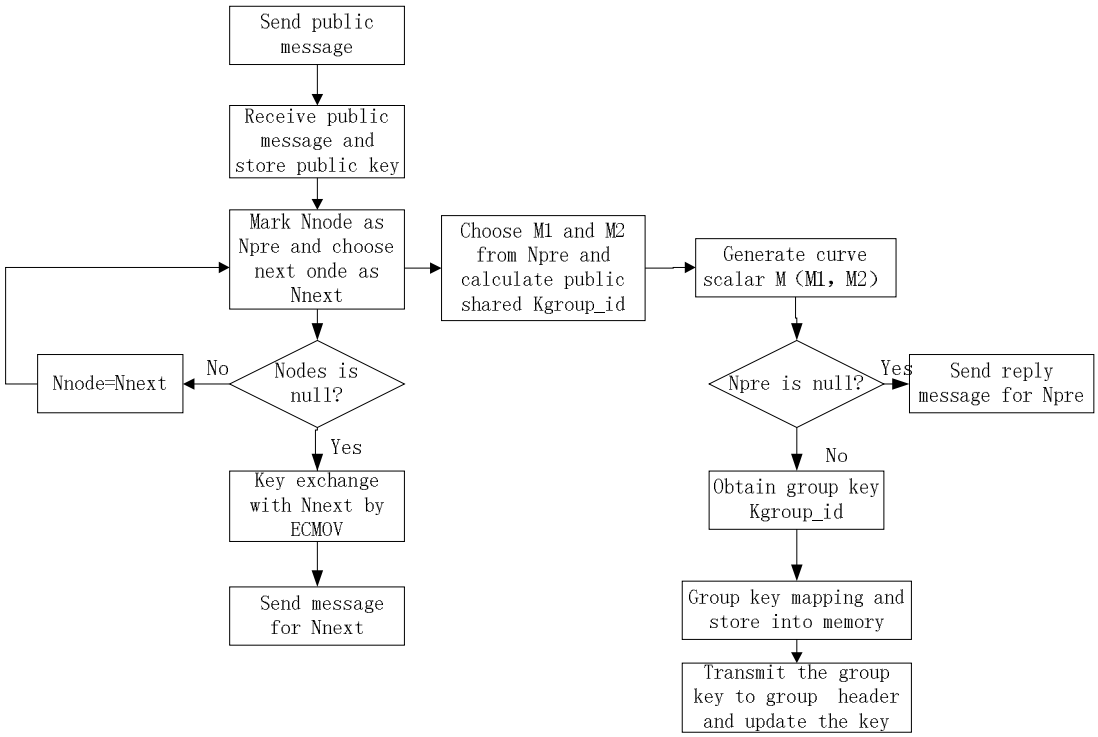

Figure 2 the flow chart of group key establishment and update

Cluster addition

(1) Mobile node N_{node_id} receives multiple broadcast messages sent by cluster headers. Select a cluster header as its own, and apply to joining into the cluster.

(2) When the cluster header receives the entrance application sent from N_{node_id}, it will check the number of nodes allocated in its cluster. Select a group whose number of nodes is less than t as the right cluster. Meanwhile, inform its group number $group\_id$ and group header to the prepared node N_{node_id}. The cluster header notices group header that a new node would add to the group. If $group\_id$ is null, a new group number will be allocated to N_{node_id} and it is regards as the group header. The group header selects a pair of key and transmits it to cluster header through ECC mechanism and the group key is shared with two headers.

(3) After receiving group number $group\_id$ and cluster header number N_{group_id}, mobile node N_{node_id} sends message $Apply\ (node\_id, K_{node\_id})$ to cluster header for group entrance.

(4) When group header N_{group_id} receives entrance application, it will add N_{node_id} to its nodes set $Nodes_{group\_id}$. Select a random integer r and extract public key K_{node_id} from application message $Apply\ (node\_id, K_{node\_id})$ sent by N_{node_id}. Meanwhile, send reply message $Response\ (group\_id, rG, K_{group_{id}} + rK_{node\_id})$ to N_{node_id}. The mobile node N_{node_id} will calculate group shared key after getting the response message from cluster header. $K_{group\_id} = M_2 - K_{node_{id}} * M_1$, $K_{new\_group\_id} = K_{node\_id} * K_{group\_id}$. Thus $K_{new\_group\_id}$ is the new group key for inner group communication.

(5) When the group header receives $K_{new\_group\_id}$, it will generate elliptic curve scalar $M = \{M_1, M_2\}$, while, $M_1 = rG$, $M_2 = K_{group\_id} + r * K_{pre}$. Group header broadcasts message within group and other ordinary group members extract group key from the message. So far, all the nodes including cluster header have stored group private key k_{group_id}. Other nodes in the group could obtain $k_{new\_group\_id}$ through message decryption.

The diagram of node joining in the cluster is shown in Figure 3.

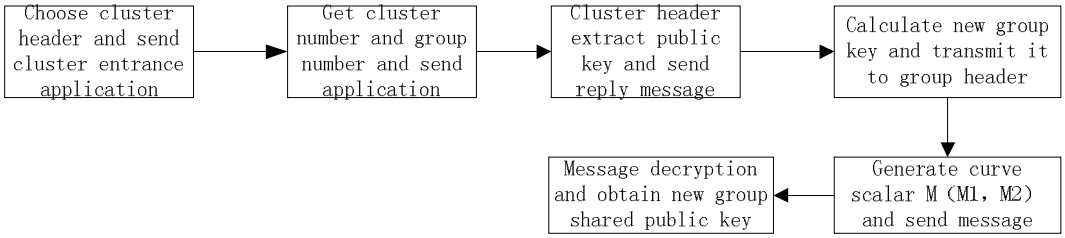

Figure 3 flow chart of mobile node joining in the cluster

Withdrawing from the cluster

When mobile node N_{node_id} withdraws from the exist cluster, it will send quit application to its group header. After receiving the application, group header deletes N_{node_id} from its group member set. Meanwhile, group header informs to cluster header with its nodes number minus one, and then, group key update process will be launched. Cluster header modifies the number of nodes for the group. After key refreshment, the exit node is unable to share the group key and stop communicating with other members within group.

ECMOV key exchange protocol

In grouping cluster topology structure, each node performs key exchange within group. Before key exchange, N_{node_A} and N_{node_B} generate static key (Q_A, d_A) and (Q_B, d_B) through elliptic curve parameters $EP = (q, FR, S, a, b, K, n, h)$. Meanwhile, their temporary keys (R_A, K_{tempA}), (R_B, K_{tempB}) are generated. After obtaining their public key, the two nodes could exchange their symmetry keys through ECMOV agreement.

The scheme of ECMOV protocol is shown as follows:

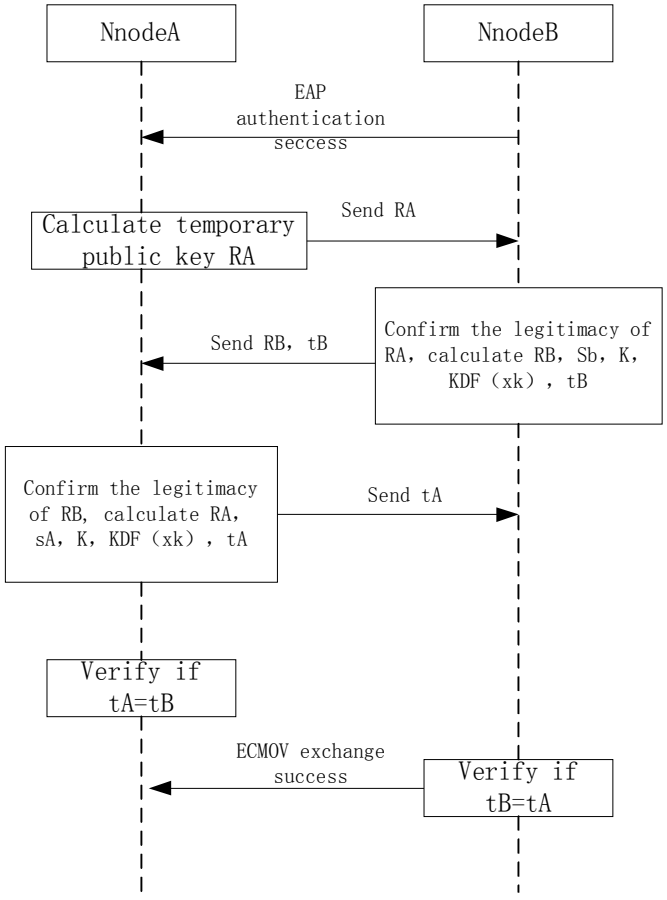

Figure 4 ECMOV flow chart of key exchange

Conclusion

In order to solve the problem about mobile applications in security reinforcement and authentication technology, which requires security encryption, the paper proposes a key management scheme suitable for intelligent mobile terminal embedded platform. The scheme is based on cluster grouping topology structure for mobile nodes, adopts the elliptic curve encryption algorithm, and obtains the communication key through ECMOV key exchange protocol, which can be applied for the mobile network with node random dispersion. The complexity and discrete logarithm encryption with ECC and key exchange within group guarantee the security of group communication. Using cluster grouping topology model of the mobile node makes it reasonable to decompose the key management within group, which shrinks the scope of key exchange, and avoids security risks of the whole network due to a single node network attack, thus improves the security feature of the system. Therefore, the designed key management scheme based on cluster grouping structure for mobile network has a certain theoretical and practical reference value.

References

[1] Pohlig S, Hellman M. An improved algorithm of compuing logarithms over GF(p) and its cryptographic significance[J]. IEEE Trans on Information Theory, IEEE, 1978(1):106-110.

[2] Chuang P J, Chang S H, Lin C S. A Node Revocation Scheme Using Public Key Cryptography in Wireless Sensor Networks [J]. Journal of Information Science and Engineering.2010, 26(5):1859-1873.

[3] Munivel E, Ajit D G M. Efficient Public Key Infrastructure Implementation in Wireless Sensor Networks [C] //International Conference on Wireless Communication and Sensor Computing, 2010.

[4] Sahshan H, Irvine J.An Elliptic Curve Distributed Key Management for Mobile Ad Hoc Networks [C] //2010 IEEE 71st Vehicular Technology Conference, 2010.

[5] Cao Y, Authentication protocol and dynamic key management scheme based on ECC [J]. Mianyang normal university journal 2009，28(5): 86-89.

[6] Tan Zhi Gang, Huang Haiping, Wang Ruzhuang, Sun Lijuan, ECC key management scheme based on grouping within the cluster [J] The computer technology and development,2012,22(2):176-180.

[7] Zhang Y, Liu W, Lou W, Fang Y, Location-based compromise-tolerant security mechanism for wireless sensor networks [J] IEEE Journal on Selected Areas in Communications, 2006, 24(2):247-260.

[8] Amin F, Jahangir A H, Rasifard H. Analysis of Public Key Cryptography for Wireless Sensor Networks Security [C] // Proc of World Academy of Science , Engineering and Technology, 2008:529-534.