A Group Key Management Scheme Based on Random Transmission for VANET

Liang PANG[1, b], Da WEI[1, 2], Qi ZHAO[3], Jianqi ZHU[1, 2, a]

[1]College of Computer Science and Technology, Jilin University, Changchun, 130012, China

[2]Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun, 130012, China

[3]Jilin University, Changchun, 130012, China

[a]email: zhujq@jlu.edu.cn, [b]email:13654408367@163.com

Keywords: VANET Group; Random Transmission; Polynomial; *Hash* Chain

Abstract. Group key management plays an important role in ensuring the safety and reliability of the VANET (vehicular ad-hoc network) over the channel. Through considering the characteristics of VANET communication and topology, a VANET group key management scheme is proposed based on random transmission which is combined with the construction of polynomial and key updating by *Hash* chain. The scheme achieves the random transmission function of group key and the node revocation capability. Moreover, it can ensure the forward and backward and other security attributes of the group key. The results show that the proposed scheme has less communication complexity and better communication performance, also it can suitable for large scale VANET group.

1 Introduction

Secure group communication has been an active research domain in recent years. Since most group communication between vehicles takes place over wide-open expanse of Internet, to encrypt data is a major consideration. Therefore, a group key management scheme needs to be proposed.

The first group key agreement was proposed by Steer et al. in 1988[1]. With the improvement of network technology, the group key management is divided into three basic types: centralized group key management, distributed group key management and decentralized group key management. The centralized group key management has a central organization used for the generation and distribution of key. Guo et al. presented a centralized group key management mechanism for VANET [2]. The distributed group key management divides the group into several sub groups. And each group has a coordinator to manage its own group. Wu et al. proposed a distributed key management based on cipher broadcast [3]. There is no central body in the decentralized group key management and member nodes have the equal status. Guo et al. presented a decentralized group key management by creating hierarchical key tree [4].

However, in VANET environment high mobility of vehicles will result in frequent changes of network topology. And high mobility or stagnation at any moment of vehicles will effect network link based on location to be randomness. Thus typical distributed group key management or centralized group key management can’t be applied to large scale VANET group communication.

In this paper, we proposed a group key management scheme based on random transmission for VANET. The scheme based on random transmission has the following characteristics: (1) Only communication with nearby nodes when sharing data between groups; (2) We can use non group member nodes to transfer message; (3) The message transfer path is adaptive stochastic; (4) Compared with the centralized key management mechanism, the single point failure problem can be avoided effectively; (5) Compared to the typical distributed key agreement mechanism, the number of communication in VANET can be effectively reduced.

We organize the rest paper as follows. In Section 2, we give out group key management scheme. In section 3, we discuss the efficiency of our key agreement. Finally, we conclude the paper.

2 Group Key Management Scheme Based on Random Transmission

In this section, we present detailed method of group key management scheme for VANET. The scheme mainly includes five aspects: system initialization, group key exchange, group key generation, group key distribution and group key update. The overall process is shown in Figure 1.

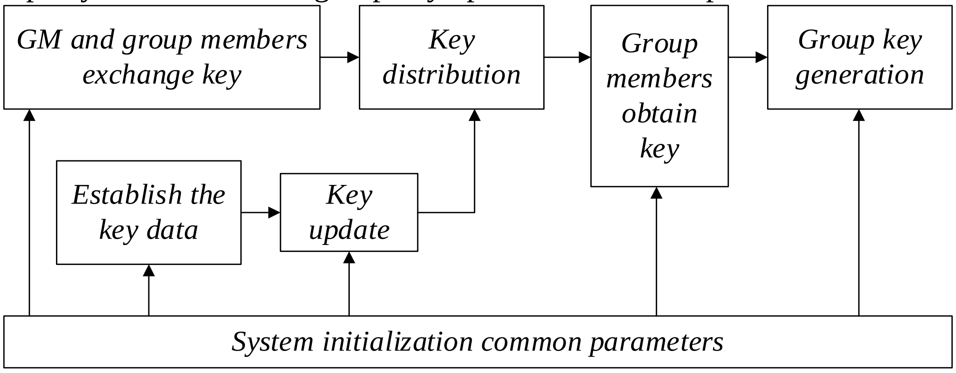

Fig 1. Process of group key management scheme

2.1 System Initialization

The symbol definition is given out of the scheme shown in Table 1. Vehicle node V_i accesses network, registers and applies for $Cert(V_i)$ from CA (Certificate Authority). After the application has been approved by CA, the $Cert(V_i)=\{Sig_{CA}(PK_{V_i} \| ID_{V_i}), PK_{V_i}, ID_{V_i}, PK_{CA}\}$ will be sent to V_i. $Sig_{CA}(PK_A \| ID_A)$ represents digital signature from CA to data. After more than one vehicle access network, $V_i \ldots V_n$ compose $Group_s=\{GM_s, V_i \ldots V_n \mid i,n,s \in N\}$. V_i communicates with GM_s by RSU (Road Side Unit). GM_s selects nodes to participate into the collection $U_{neg}=\{V_{neg} \mid V_{neg} \in Group_s\}$ according to nodes' online time and L_{ii}. L_{ii} represents recent assessment value of OBU (On board Unit). GM_s verifies $Cert(V_i)$ and agrees prime finite fields F_q with V_i. $F^+{}_q$ is cyclic group of qth-order addition, the bit length of q is $b=(log_2q+1)/2$, g is $F^+{}_q$'s generator. Message authentication code algorithms are defined as $MAC_A(\bullet)$ and $MAC_B(\bullet)$. Export key function is $KF(x)=H(X \| j)$, j represents counter.

Table 1. Symbol definition of scheme

Symbol	Symbol definition	Symbol	Symbol definition
$Group_s$	*Vehicle Group S*	M_T	*Key message*
V_i	*Vehicle Node* V_i	$List_{Add}^{T-1,T}$	*Member increment list*
$Cert(V_i)$	V_i *certificate*	$List_{sub}^{T-1,T}$	*Member decrement list*
GM_s	*Group Manager*	L_{List}	*Key chain length*
s_{GM_s}	GM_s *private key*	K_L	*Hash chain*
P_{GM_s}	GM_s *public key*	$Key_S^{T_{seq}}$	T_{seq} *group key*
s_{V_i}	V_i *private key*	$T_K^{\min}$	*Minimum update cycle*
P_{V_i}	V_i *public key*	V_{dele}	*Node to be deleted*
k_S^i	*Key factor*	T_K^{frc}	*Force update cycle*
K_s^T	*Key data*	$B_S^{T_{seq}}$	*Apply for broadcast*
ID_V^i	V_i *Node identifier*		
$List_S^T$	*T cycle members*		

2.2 Group Key Exchange

In this section, group key exchange is based on the mBPR model [5]. Assuming that the private and public key of GM_s are $(s_{GM_S}, P_{GM_S} \mid P_{GM_S}=g^{s_{GM_s}} \bmod q)$, the private and public key of V_i are $(s_{V_i}, P_{V_i} \mid P_{V_i}=g^{s_{V_i}} \bmod q)$. In this formula, $\gcd(s_{GM}, q-1)=1$ and $\gcd(s_{V_i}, q-1)=1$. The process of group key exchange between GM_s and V_i is as follows:

(1) V_i selects a random $a_i \in Z_q^*$ and sets $r_i = P_{V_i}{}^{a_i} \bmod q$. V_i selects $k_i \in Z_q^*$ and computes $s_i = g^{-k_i} r_i^{s_{V_i}} \bmod q$ and $t_i = (1 - s_{V_i}) a_i + s_{V_i}{}^{-1}(k_i - s_i) \bmod (q-1)$, sends r_i, s_i, t_i to GM_s;

(2) GM_s executes the same process as (1) and sends r_{GM}, s_{GM}, t_{GM} to V_i;

(3) GM_s receives r_i, s_i, t_i data and computes $(P_{V_i})^{t_i} = r_i^{(1-s_{V_i})} g^{(k_i - s_i)} \bmod q$. If $(P_{V_i})^{t_i} s_i g^{s_i} = r_i$, computes $k_S^i = (r_i)^{s_{GM} a_{GM}} \bmod q$. Otherwise, taking a renegotiation;

(4) Vi executes same process as (3), and computes $k_S^{GM} = (r_{GM})^{s_i a_i} \bmod q$. The key factor $k_S^i = k_S^{GM} = g^{a_i a_{GM} s_{V_i} s_{GM}}$ is shared among all the vehicles in the group.

2.3 Group Key Generation

Group key generation is based on the mKY model [5]. V_i selects a random x_i as private key, so the public key is $Y_i = g^{x_i} \bmod q$. The process of setting up the current group key is as follows:

(1) V_i selects a random $a_i \in Z_q^*$, computes $s_i = a_i g^{x_i} \bmod q - (r_i + g^{x_i} \bmod q) x_i \bmod (q-1)$ and $r_i = g^{a_i} \bmod q$. V_i broadcasts $M_i = (seq, r_i, s_i, Cert_i)$ to other U_{neg} members;

(2) At the same time, V_i receives $Mes = \{M_1, \dots, M_{i-1}, M_{i+1}, \dots, M_n\}$ from other members. For example, V_i receives V_j's data M_j and computes $Y_j^{'} = (g^{x_j} \bmod q)^{r_j + g^{x_j} \bmod q} g^{s_j} \bmod q$. If $Y_j^{'} = r_i^{Y_j}$, set $g_i = r_{i+1} / r_{i-1}$. V_i computes $s_i^{'} = x_i - (g_i^{a_i} \bmod q + g^{x_i} \bmod q)(x_i + a_i) \bmod (q-1)$ and $Z_i = g_i^{a_i} \bmod q$, broadcasts $M_i^{'} = (seq, Z_i, s_i^{'}, Cert_i)$. If $Y_j^{'} \neq r_i^{Y_j}$, end computational process;

(3) V_i receives $Mes^{'} = \{M_1^{'}, \dots, M_{i-1}^{'}, M_{i+1}^{'}, \dots, M_n^{'}\}$ from second round and computes $Y_j^{"} = (r_j Y_j)^{Z_j + Y_j} (g)^{s_j^{'}} \bmod q$. If $Y_j^{"} = Y_j$, V_i computes $Y_j^{"} = r_i^{na_i} Z_i^{n-1} Z_{i+1}^{n-2} \cdots Z_{i+n-2}^{0} \bmod q$ to get the key. Otherwise, end computational process.

2.4 Key Distribution Based on Random Transmission

Collection $List_T = \{V_i, V_i \in Group_s\}$ represents the nodes which are to be distributed in circle T. We use K_S^T to distribute the key data based on constructing polynomial.

(1) GM_s queries the collection $K_S^F = \{k_S^1, k_S^2, \cdots k_S^m, m \in N^+, 5 \le m\}$ and constructs the polynomial in finite field F_q : $F_q^1(x) = ((x - k_S^1)(x - k_S^2) \cdots (x - k_S^m) + K^T{}_s) \bmod q$ .Expanding the polynomial based on congruence of number theory:

$$F_q^1(x) = (x^m \bmod q + a_1 x^{m-1} \bmod q + \cdots + a_{m-1} k_S^1 k_S^2 + \cdots + k_S^m \bmod q + K_S^T \bmod q) \bmod q .$$

In this formula, $a_1, a_2 \cdots, a_{m-1}$ is according to the specific key factor parameters to calculate. GM_s computes $K_*^1 = a_{m-1} k_S^1 k_S^2 \cdots k_S^m \bmod q + K_S^T \bmod q$ and expands polynomial $F_q^1(x)$ to $F_q^1(x) = (x^m \bmod q + a_1 x^{m-1} \bmod q + \cdots + K_*^1) \bmod q$. GM_s broadcasts $M_T = \{a_1 | a_2 | \cdots | K_*^1 | q | m\}$;

(2) Vi in the $List_S^T$ receives M_T and constructs the polynomial by the same coefficient: $F_q^{'}(x) = (x^m \bmod q + a_1 x^{m-1} \bmod q + \cdots + K_*^1) \bmod q$.

V_i sets k_S^i as x value into $F_q^{'}(x)$ and records as $K_T = F_q^{'}(k_S^i)$. Now V_i gets key data K_S^T from $Group_s$. The process of key distribution based on constructing polynomial shown in Figure 2.

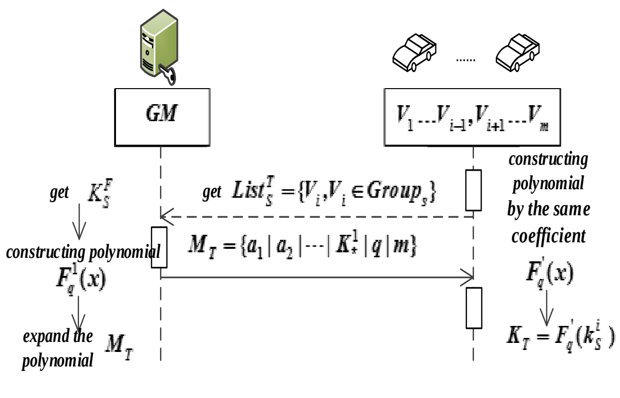

Fig 2. Process of key distribution

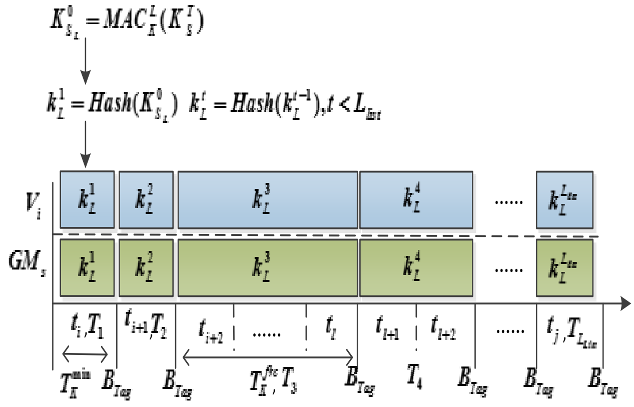

Fig 3.Process of key data update

The nodes got K_T are defined as $U_{chv}=\{V_{chv}^i|V_{chv}^i\in Group_s\}$, conversely the collection is $U_{unch}=\{V_{unch}^i|V_{unch}^i\in Group_s\}$. The process of transmission is as follows:

(1) V_{unch}^i does not obtain K_s^T, then monitors broadcast data nearby itself. If V_{unch}^i does not obtain K_s^T after monitoring for a while, it will randomly connect with other vehicles in the U_{chv} which are close in physical space to apply for the key data;

(2) The vehicle in the U_{chv} receives the application. If the vehicle has already get the data M_T, it will transfer M_T to V_{unch}^i. V_{unch}^i gets M_T and analyzes out key data K_s^T by method mentioned in section 2.4.1. Now V_{unch}^i gets K_s^T and it will be added to U_{chv}. Then V_{chv}^i storages M_T;

(3) If other vehicle V_{unch}^j applies for M_T from V_{chv}^i, V_{chv}^i will transfer M_T to V_{unch}^j.

2.5 Group Key Update

The process of key data update based on *Hash* chain shown in Figure 3.

(1) GM_s selects *Hash* function $\mathrm{H}_{\mathrm{K}}^{\mathrm{L}}(\bullet)$ which is resisted strong collision, selects message authentication code function MAC_K^L and digital signature algorithm $Sig(\bullet)$, computes $L_{List}=T_K^{frc}/T_K^{\min}$ as the length of key. GM_s constructs $B_{para}=\{\mathrm{H}_{\mathrm{K}}^{\mathrm{L}}\|T_K^{\min}\|T_K^{frc}\|Sig\|L_{List}\}$ and broadcasts B_{para} to all the group members;

(2) GM_s divides periodic time series $T_K^{i,j}=\{t_i,t_{i+1},\cdots,t_j|i,j\in N^+\}$ and computes $K_{S_L}^0=MAC_K^L(K_S^T)$, and then distributes $K_{S_L}^0$ to group members. GM_s and V_i compute $K_L=\{k_L^1,k_L^2,\cdots,k_L^{L_{list}}\}$ with $K_{S_L}^0$ by using $\mathrm{H}_{\mathrm{K}}^{\mathrm{L}}(\bullet)$ function, while $t<L_{List}$, $k_L^t=Hash(k_L^{t-1})$;

(3) When group members change or $T_K^{\min}$ is reaches, GM_s triggers key update event and updates $B_{Tag}=\{Group_s|tag|T_{seq}|Sig_{S_{GM}}(Group_s|tag|T_{seq})\}$, T_{seq} is current time period;

(4) V_i receives $k_s^{T_{seq}}$ in the next circle of K_L, uses key derivation function $KF(x)$ to compute $Key_S^{T_{seq}}$ in circle T_{seq}: $Key_S^{T_{seq}}=KF(k_L^{T_{seq}})$ ……………………………………………………(1.1)

When vehicle nodes join in the group, GM_s distributes $k_L^{T_{seq+1}}$ which is in circle T_{seq+1} to G_{new}^S and broadcasts B_{Tag}. The new joined node V_j receives $k_L^{T_{seq+1}}$ and constructs incomplete *Hash* chain $K_L^{T_{seq}}$, computes $Key_S^{T_{seq+1}}$ in circle T_{seq+1} by using formula 2.3. V_i receives B_{Tag} and computes $Key_S^{T_{seq+1}}$ in circle T_{seq+1} by using formula (1.1).

When vehicle nodes leave the group, GM_s sets the new collection $Group_S^{T_{seq+1}}$ in circle T_{seq+1}. GM_s computes $K_L^t=MAC_K^L(k_L^{T_{seq}})$ and distributes K_L^t as new cipher key to $Group_S^{T_{seq+1}}$. V_j in $Group_S^{T_{seq+1}}$ gets $k_s^{T_{seq}+1}$ and computes $Key_S^{T_{seq+1}}$ by using formula (1.1).

3 Scheme Safety and Performance Analysis

3.1 Safety Analysis

In this scheme, group key exchange and generation has already been proved in security based on mBPR [6] model and mKY [6] security model. The node has not exchanged key factor with GM_s can't compute key data. Any node V_i can compute k_s^i with a non-ignorable probability ε, it also can solve high order polynomial problem of Ruffini Abel theorem or large number factorization problem with a non-ignorable probability. So the security of group key is guaranteed.

The described key updating mechanism in this scheme is based on *Hash* chain. *Hash* has the features of unidirectional and resistance to strong collision. Any node has got key data in circle T_{seq} wants to get the key data in its last circle T_{seq-1} is infeasible. In other words, the process of computing a last node from a current node in *Hash* chain is not feasible in the calculation.

When vehicle nodes leave group in circle T_{seq}, GM_s uses the private key to computes message authentication code and tags the key data as abolished. Any node left the group can't get K_L^t by updating. While GM_s redistributes key data based on constructing polynomial, there is no key factor of the node left the group, so it can't recover the key data from the broadcast. Therefore, our scheme can effectively satisfied the forward and backward of the group key in this scheme.

Table 2. Overhead of establishing group key

Scheme	Index		
	Communication	**Calculation**	**Storage**
LKH	$n(U)+B$	......	$GM: 2n-1$ $V_i: \log_2(n)+1$
TR-GKA	$6n(U)$	$(3MUL+(n^2+3n)/2-3)MUL$ $2sig+(2n-2)vsig$	$2n$
LMA	$\mathrm{m}(B)$ $(2k+1)B$	$GM: \mathrm{m}+2k(MUL)$ $V_i: 1(MUL)$	$GM: 3$ $V_i: 2$
Random transmission	$GM: B+n(U)$, $neg: m$ $V_i: random \le n$	$GM: (n^2-n)/2(MUL)+sig$ $V_i: (6+n)(EXP)+n(MUL)$	$GM: n$ $V_i: 1$

Table 3. Overhead of key update by joining notes into the group

Scheme	Index	
	Communication	**Calculation**
LKH	$2\log_2 n(M), 1(U)$	......
TR-GKA	$6n(U)$	$(3MUL+(n^2+3n)/2-3)MUL$ $2sig+(2n-2)vsig$
LMA	$1(SB), 1(U), 2(B)$	$GM: k(MUL)$ $V_i: 1(MUL)$
Random transmission	$GM: B$ $V_i: random \le n$	$GM: 1(HASH)$ $V_i: 1(Hash)$

Table 4. Overhead of key update by revoking notes out of the group

Scheme	Index	
	Communication	**Calculation**
LKH	$2\log_2 n(M)$	......
TR-GKA	$6n(U)$	$(3MUL+(n^2+3n)/2-3)MUL$ $2sig+(2n-2)vsig$
LMA	$1(SB), 2(B)$	$\mathrm{m}+k-1(MUL)$
Random transmission	$GM: B+n$, $neg: m$ $V_i: random \le n$	$GM: (n^2-n)/2(MUL)+sig$ $V_i: (6+n)(EXP)+n(MUL)$

3.2 Performance Analysis

In this section, we compare LKH [6] agreement base on logic key tree, TR-GKA [5] agreement and LMA [7] scheme which is similar in structure with this paper. We take the overall number of communication rounds and the calculation of a single node as the main reference.

Assuming that n is the number of group member nodes, m is the number of nodes participated in group key data negotiation. MUL represents point multiplication of elliptic curve, B is global broadcast, *U* is unicast communication of point to point, *EXP* is modular exponentiation, *Hash* represents one-way *Hash* operation, *MAC* is message authentication code operation, *sig* is digital signature, *vsig* is validate of digital signature, *random* is random communication process. The overhead of establishing group key in communication, calculation and storage shown in Table 2.

From table 2, it is clear that our scheme has larger calculation than LMA agreement, *GM* needs polynomial times multiplication, one time digital signature. V_i has the same scale in calculation with TR-GKA agreement needs modular exponential operation. In storage aspect, our scheme is better than LKH agreement and TR-GKA agreement, and at the same level with LMA agreement. It has the same scale with other schemes in communication performance.

When there are vehicle nodes joined or left the group, the key update mode is different from key establishment phase. Overhead of key update by joining notes into the group or revoking notes out of the group shown in Table 3 and 4. From table 3 and 4, our scheme has better performance than other schemes in communication. And when nodes join into the group, our scheme is superior to others in calculation. But when nodes left the group, members that did not leave the group using the method of redistribution in our scheme. So it is more complex than other schemes.

4 Conclusion

In this paper, our scheme based on random transmission is better reflected in safety and communication performance. The key path is depth random of this scheme. When the number of group members increases linearly, the frequency of the communication will grow exponentially in distributed group key management. But communication times still appeared linear growth in our scheme. And propagation delay time is logarithmic growth. Under ideal circumstances, the number of nodes in a single cycle will be exponential growth in this paper. That means group key can quickly cover the key data and be applied to large scale VANET communication requirements.

Acknowledgement

In this paper, the research was sponsored by the National Natural Science Fund (Project No. 61373123 and 61572229).

References

[1] D. Steer, L. Strawczynski, W. Diffie, M. Wiener. “A Secure Audio Teleconference System,” Advances in Cryptology (CRYPTO’88), 1988:520-528

[2] Guo M H, Liaw H T, Deng D J, et al. Centralized group key management mechanism for VANET[J].Security and Communication Networks,2013, 6(8):1035-1043.

[3] Wu Q, Qin B, Zhang L, et al. Fast transmission to remote cooperative groups: a new key management paradigm[J].Networking, IEEE/ACM Transactions on,2013,21(2):621-633.

[4] Ming-Huang Guo, Horng-Twu Liaw, Meng-Yu Chiu, et al. On decentralized group key management mechanism for vehicular ad hoc, networks [J]. Security & Communication Networks, 2016, 9(3):241–247.

[5] Zhang Hua, Wen Qiao-yan, Jin Zheng-ping. Provable Safety Theory and Protocol [M]. Beijing: Science Press, 2012.304-320.

[6] Wallner D, Harder E, Agee R. Key management for multicast: Issues and architectures[R].RFC 2627, 1999.

[7] Cao Shuai, Zhang Chuan-rong, Song Cheng-yuan. Group key management scheme for large mobile Ad hoc network [J]. Application Research of Computers, 2012, 29(4):1420-1423.