Pers Ubiquit Comput (2014) 18:1893–1900
DOI 10.1007/s00779-014-0794-z

ORIGINAL ARTICLE

Secured access control for vehicles in RFID systems on roads

Yanfei Lu · Xin Li · Xing Wei · Tao Jing ·
Wei Cheng · Yan Huo

Received: 1 March 2014 / Accepted: 29 April 2014 / Published online: 17 September 2014

Abstract Vehicle access control systems exist everywhere in our daily life. However, the simple permit-based verification method is not sufficient for the critical departments such as banks and courts, which need to check not only the identity of the vehicles, but also the vehicle route before reaching the restricted area, as the vehicles can have the access permit if and only if they have traveled along the pre-defined routes. To meet the route-tracking requirement, we proposed a novel access control systems based on the radio frequency identification systems on roads. Particularly, we designed a key cloaking method and a route encryption algorithm so that the access control system can be protected against the attackers from both outside and inside. The analytical results demonstrate that our proposed algorithm can successfully reduce the threat of some malicious attack, such as side-channel attack.

Y. Lu · X. Li · X. Wei · T. Jing · Y. Huo
School of Electronics and Information Engineering,
Beijing Jiaotong University, Beijing, China
e-mail: yflu@bjtu.edu.cn

X. Li
e-mail: 12120097@bjtu.edu.cn

X. Wei
e-mail: 12120152@bjtu.edu.cn

T. Jing
e-mail: tjing@bjtu.edu.cn

Y. Huo
e-mail: yhuo@bjtu.edu.cn

W. Cheng (✉)
Department of Computer Science, Virginia Commonwealth
University, Richmond, VA, USA
e-mail: wcheng3@vcu.edu

Keywords Vehicle access control · RFID systems on roads · Route encryption

1 Introduction

In many environments, vehicles need to get permissions to access restricted areas. Courts, banks, and military departments usually ask the drivers to show their IDs or passes at the entrances, and the vehicles are also required to have specific decals or tags. However, it is not sufficient for only checking the permits in the cases, where the monitoring of the vehicle route is also essential. For instance, any detour or delay of a bank note transport car may indicate possible problems such as attacks from insiders.

The existing real-time vehicle-tracking systems are primarily built based on GPS, which is technically ready, but has many defects such as low position accuracy and unavailability in tunnels. In addition, the current access control system cannot handle the problems caused by duplicated permits and insincere drivers.

Therefore, a successful vehicle access control system should meet the following two criteria:

- *Unalterable access permit* The system must be able to distinguish the authorized vehicles from the unauthorized vehicles and the compromised vehicles.
- *Vehicle whole route tracking* The system must be able to track the route and verify the integrity and the truthfulness of a reported route.

In order to meet the criteria, we propose to design a secured vehicle access control system based on RFID system on roads (RSR) [1], which can localize vehicles via reading the radio frequency identification (RFID) tags deployed on the road surface. A typical RFID system consists of a RFID reader and several RFID tags. An RFID tag has a small storage space, which can be used to store its unique ID and the customized information such as the tag's location. A RFID reader can acquire the information from the tag when they are proximate. Due to the small size and the low cost of RFID tags, RFID systems provide a scalable and economic way for managing massive objects in a variety of applications, e.g., inventory management, logistics, and object tracking. RFID systems have also been widely adopted for ETC and parking garages access in the current transportation systems, but has never been used for whole route tracking. To the best of our knowledge, this paper is the first one to study the problem of vehicle route tracking in RSR. Specifically, the main contributions of this paper are summarized as follows:

1. We propose an access control system that can track the vehicle route in RSR.
2. We propose a key cloaking method to protect the key from insincere drivers.
3. We propose a route encryption algorithm to protect the integrity and the truthfulness of the route.
4. We analyze the security of the proposed algorithm against several typical attack models.

The rest of this paper is organized as follows. Section 2 briefly summarizes the most related works. The architecture of the proposed access control system is presented in Sect. 3. The key cloaking method for replacing the traditional single-vehicle–single-key system and the route encryption algorithm is proposed in Sect. 4. Section 5 analyzes the security of the proposed algorithms. Finally, the paper is concluded in Sect. 6.

2 Related work

Intelligent vehicle access control system has aroused wide public concern. Zhou et al. [2] described a set of vehicle access control systems based on ZigBee wireless technology. Roesner et al. [3] took an approach of user-driven access control, to enable in-context, non-disruptive, and least-privilege permission granting on modern client platforms. Later, Almanza-Ojeda et al. [4] presented a system, by which we can control the accesses of three different parking and can also check the access of each driver using RFID. A hybrid RFID-license plate recognition (LPR) system [5], which is useful to allow entry of vehicles, is designed during Hajj season in Sandi Arabia. Considering the challenges, such as losing or stolen of access cards, Shu et al. [6] introduced a sensory-data-enhanced authentication for access control systems, which were backward-compatible with existing access control systems and significantly increased the key spaces for authentication. There are more work on designing intelligent access control system based on RFID [7] and [8].

More than just checking vehicles' identities in the above work, some special apartments, such as banks and courts, also need to track vehicles and verify the truth of the reported routes in case that they are tampered by insincere drivers. There are three types of methods for protecting the privacy of routes: dummy method, trajectory k-anonymity method, and suppression-based method. The dummy method [9] has the advantages of low computational complexity, low additional load, and easy implementation, but it is vulnerable to the attacks from spatial and temporal target association in poor safety. The k-anonymity method, which is a generalization-based approach to hide true trajectory and protect the privacy, had been used in [10–15]. However, this method is unsuitable for the intelligent vehicle access control systems as it is impossible to find the proper $k-1$ anonymity traces for a vehicle. The suppression-based approach, which can resist hostile attack, was proposed in [16, 17], but it can cause data distortion problems, which make it cannot be applied to the intelligent vehicle access control systems.

To the best of our knowledge, there still doest not exist a method that can protect the route integrity from being tampered while reducing the data distortion. In this paper, we therefore propose a key cloaking method, which can resist most hostile attacks and protect the truth of the reported routes.

Moreover, in most of the current encryption mechanisms, the authentication is based on a single-key and asymmetric encryption. RSA algorithm is the widely adopted asymmetric cryptographic algorithm, but it only focuses on the difficulty of decoding keys without considering the protection of the keys. As a result, it is danger once the keys are intercepted by insiders. To resolve this problem, we introduce the using of faked keys and the user's password to ensure the security of keys. Our method can not only increase the difficulty of key exposure, but also increase the security by requiring password authentication when choosing the keys.

3 System architecture

The access control system proposed in this paper is based on the RSR [1]. RSR consists of RFID tags and RFID readers. In RSR, RFID passive tags are deployed on road surfaces, and RFID readers are installed on vehicles. The reader can obtain the data stored in the tags when the vehicle is passing by. The tag can store its location (latitude and longitude) and road information such as the current direction of the lane, where the tag resides, the lane speed limit, and the local traffic information. By utilizing RSR, the vehicle can accurately locate itself and record its route accordingly. Comparing with GPS systems, which may provide wrong location information when the connections to the satellites are weak, the RFID tags deployed on the road surfaces can ensure the location information accuracy in RSR. As the performance of RSR cannot be affected by the surrounding environments, it is a better choice for localization and tracking in access control systems.

Our access control system consists of the starting center, the authorized vehicles, the authorize users, and the destination center. RFID readers are installed in authorized vehicles, and RFID tags are deployed on road surfaces. The architecture of our system is illustrated in Fig. 1. In the system, the RFID reader records the tag's information when the vehicle passing by and reports the route information to the destination center after arriving at the control gate so that the destination center can verify the vehicle route.

Specifically, the vehicles need to first register at the starting center before departing for the destination center. The starting center distributes a key and a group of faked keys to an authorized vehicle through the key cloaking method, which can protect the key from insincere drivers. The starting center also sends the vehicle information and the key to the destination center. The vehicle reads the tags and records the location information, which is encrypted by the keys. When the vehicle arrives at the destination center, it sends out its collected encrypted location information (the route) to the destination center.

The destination center verifies the vehicle's identity and use the correct key received from the starting center to decrypt the received route. The vehicle is authorized to access the restricted area only if the destination center can successfully obtain the route and verify the route's integrity and truthfulness.

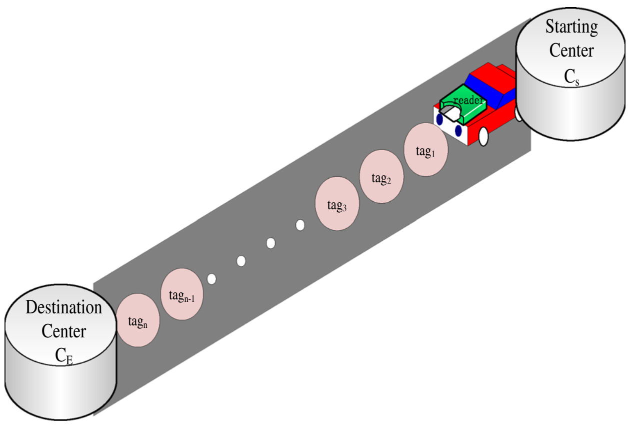

Fig. 1 The system architecture

4 Route tracking and verification

4.1 Key cloaking method

In most of the access control environments, the identification of a vehicle mainly relies on a single security key, which is generated and maintained by the license center (the starting center in our system architecture). Generally, the vehicle is also required to have a copy of the key to pass the gate at the restricted area. Therefore, the security of an access control system is determined by the protection of the key at both the license center and the vehicle. In this paper, we assume that the license center is secure. However, a series of attacks may be occurred to acquire the key from the vehicle. For instances, (1) the key may be captured by attackers during the time of communication. (2) an insincere driver may leak the key. (3) the vehicle may be occupied by attackers. (4) the attackers can masquerade an authorized vehicle.

Accordingly, we consider the above single-vehicle–single-key system is insufficient for guaranteeing the security of an access control system. We therefore design a key cloaking method in this subsection so that the driver or the attackers cannot have the key even if they have the control of an authorized vehicle.

The authorized vehicle, the starting center, and the destination center are denoted as V_A, C_S, and C_E, respectively. The process of initialization for an authorized vehicle before departing from the starting center is illustrated in Fig. 2. The authorized vehicle V_A first sends its identity ID_A to C_S. The starting center then generates a random number R_A to generate a key k_A for the vehicle. k_A is generated through the key-generating function

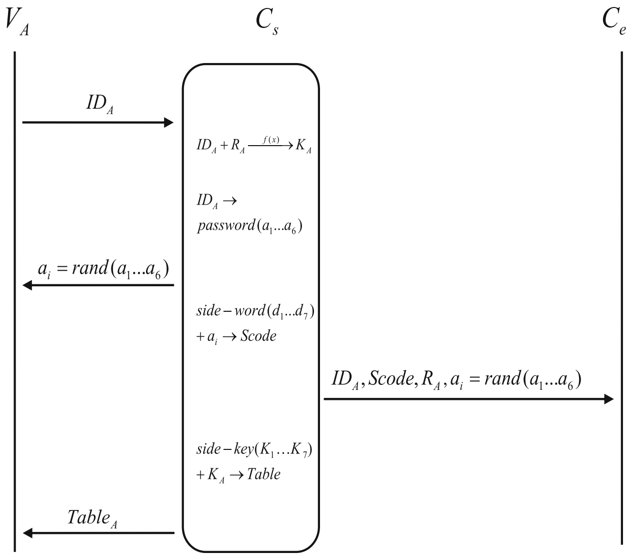
V_A
C_s
C_e
ID_A
$ID_A + R_A \xrightarrow{f(x)} K_A$
$ID_A \rightarrow$
$password(a_1 ... a_6)$
$a_i = rand(a_1 ... a_6)$
$side - word(d_1 ... d_7)$
$+ a_i \rightarrow Scode$
$ID_A, Scode, R_A, a_i = rand(a_1 ... a_6)$
$side - key(K_1 ... K_7)$
$+ K_A \rightarrow Table$
$Table_A$

Fig. 2 The process of initialization before departing from C_S

$f(x)$ $(ID_A + R_A \xrightarrow[\rbrack]{\lbrack} f(x)k_A)$. Note that, the destination center also has the same key-generating function.

The point of protecting the key from the above four listed attacks is to make the driver be unaware of k_A. To achieve this goal, the starting center takes the following steps during the initialization stage.

1. According to ID_A, C_S generates a password $(a_1a_2a_3a_4a_5a_6)$. Note that the password is different from k_A and the i in a_i can be set according to the system requirement. C_S randomly chooses an a_i from the password. Without loss of generality, we assume that a_2 is the chosen number. Then, C_S sends a_2 to V_A.
2. C_S generates a set of code $(d_1d_2d_3d_4d_5d_6d_7)$. Note that, the j in d_j can be set according to the system requirement, and for any i, j, $a_i \neq d_j$.
3. C_S constructs a $Scode$ based on a_2 and $(d_1d_2d_3d_4d_5d_6d_7)$ as in (1). Note that the position of a_2 in the $Scode$ is random.

$$Scode = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ d_4 & d_1 & a_2 & d_6 & d_7 & d_3 & d_5 & d_2 \end{bmatrix} \quad (1)$$

4. C_S sends the vehicle's identity ID_A, a_2, the $Scode$, and the random number R_A to the destination center C_E, such that C_E can construct the same k_A.
5. C_S generates a set of faked keys $(k_1, k_2, \cdots k_m)$ and put the faked keys together with k_A randomly into a key table $Table_A$.

$Table_A$=

1	k_4
2	k_1
3	k_A
4	k_6
5	k_7
6	k_3
7	k_5
8	k_2

6. C_S sends the $Table_A$ to V_A.

When the vehicle arrive at the destination center, (1) V_A sends its ID_A to C_E as shown in Fig. 3. (2) C_E gets the corresponding $Scode$ according to the received ID_A and sends the $Scode$ back to V_A. (3) V_A find the position of a_2 in the $Scode$ (the position is 3 in our example $Scode$ (1)) and sends the position number to C_E within a required time period. C_E will only consider the vehicle is an authorized one and starts to verify the route if the received position number is the correct one for a_2 in the $Scode$. We summarize the process of key cloaking in Algorithm I.

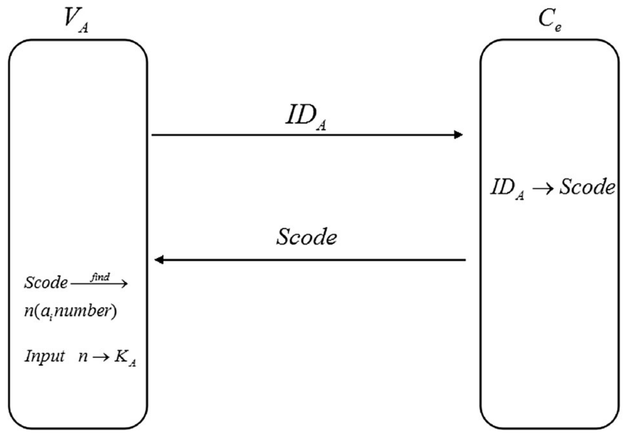

Fig. 3 The process at C_E

Algorithm I: The Key Cloaking Method

```
* Upon Departure:
$C_S$ generates $R_A$, $k_A$, $\{a_1, a_2, a_3, a_4, a_5, a_6\}$, $a_2$,
    $\{d_1, d_2, d_3, d_4, d_5, d_6, d_7\}$, and $(k_1, k_2, \cdots\ k_m)$;
$C_S$ generates $Scode$ and $Table_A$;
$C_S$ sends $a_2$, $ID_A$, $Scode$, and $R_A$ to $C_E$;
$C_S$ sends $a_2$ and $Table_A$ to $V_A$;
* Upon Arrival:
$C_E$ sends $Scode$ to $V_A$;
$V_A$ returns the position of $a_2$ in $Scode$ to $C_E$ within time
    $T$;
if $V_A$ returns the correct position then
    The vehicle is considered to be authorized and $C_E$ start
    to verify the route;
else
    $V_A$ is considered to be illegal;
end if
```

Compared with the simple-vehicle-single-key mode, the proposed key cloaking method can guarantee that V_A has the key table $Table_A$ but has no idea about which key in the table is k_A. Therefore, k_A is protected from the drivers even after the vehicles have arrived at the destination. As a result, the attackers cannot identify the correct key, k_A, even if they can take over the authorized vehicles. In the following subsections, we will introduce the process of route encryption and verification.

4.2 Route encryption

In this subsection, we design a disordered route encryption algorithm to prevent the attackers from tampering the reported route.

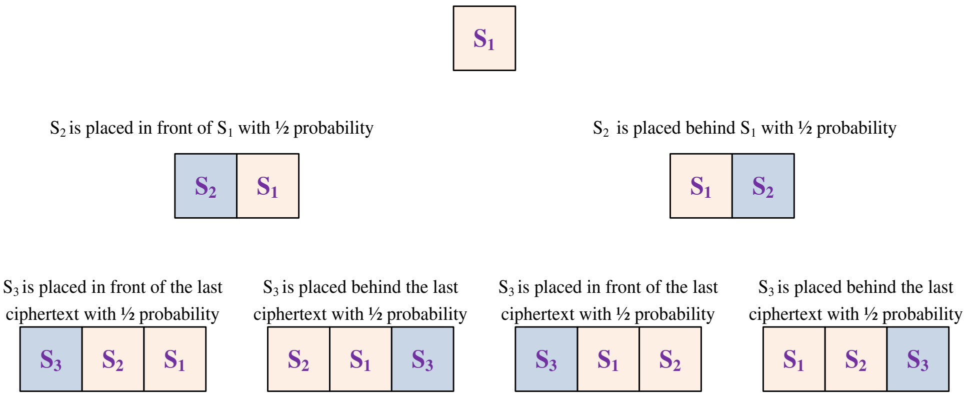
S_1
S_2 is placed in front of S_1 with ½ probability
S_2 is placed behind S_1 with ½ probability
S_2 S_1
S_1 S_2
S_3 is placed in front of the last ciphertext with ½ probability
S_3 is placed behind the last ciphertext with ½ probability
S_3 is placed in front of the last ciphertext with ½ probability
S_3 is placed behind the last ciphertext with ½ probability
S_3 S_2 S_1
S_2 S_1 S_3
S_3 S_1 S_2
S_1 S_2 S_3

Fig. 4 The encryption process

The RFID reader on a vehicle will read the tag's locations and encrypt them automatically when passing by. For each collected tag location, the vehicle encrypts it with the $m + 1$ keys, which are in the key table $Table_A$, respectively. In other words, each location has $m + 1$ ciphertexts. Note that, the vehicle only records the ciphertexts of the route. Without loss of generality, we only introduce the process of encrypting the route with k_A at the followings.

When passing by the first tag t_1, the vehicle uses the key k_A to encrypt the location of t_1 and generates a fixed-length ciphertext s_1. At the time of passing by the second tag t_2, the vehicle uses $s_1 + k_A$ as the new key to encrypt the location of t_2 and generates the ciphertext s_2. By this analogy, s_2 and k_A become new keys to encrypt the location of the third tag t_3 and to generate the ciphertext s_3. As a result, the vehicle has a ciphertext route $S = \{s_1, s_2, \cdots, s_n\}$ after passing by the nth tag.

If the route is simply encrypted as $S = \{s_1, s_2, \cdots, s_n\}$, it is easy for attackers to pair the original tag location with the ciphertext. Then, if the attackers intercepts ciphertext block S, they will capture the hidden k_A by cryptanalysis as we assume that the attackers have all the tag locations.

To solve this problem, we design a disorder placement method to remove the regularity of ciphertext in S as shown in Fig. 4. We first consider the ciphertext s_1 as the base. Then, s_2 is placed before or after s_1 with 1/2 probability, respectively. As a result, there are two possibilities for placing s_1 and s_2. Similarly, s_3 is placed before or after the ciphertext block $\{s_1, s_2\}$ or $\{s_2, s_1\}$ with equal probability. In other words, there are four possibilities for placing s_1, s_2 and s_3. Therefore, for n ciphertexts, the number of possibility for placement is 2^{n-1}.

Obviously, the final ciphertext block S does not have the ordered sequence anymore. Even if the attackers can obtain the whole block S and know each tag's location, it is very difficult to get the key k_A through cryptanalysis, because each tag's ciphertext is hidden in the ciphertext block and the attackers cannot find the corresponding relationship between the ciphertext and the tag location.

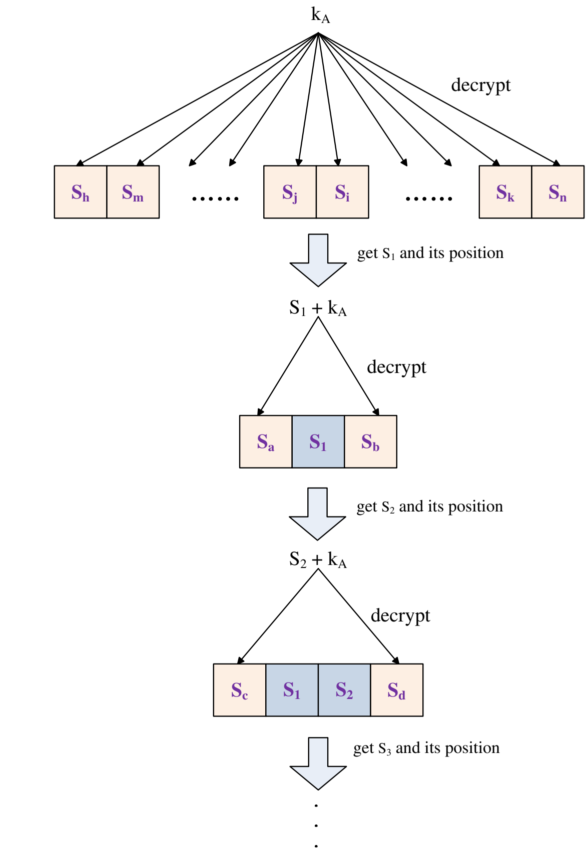
k_A
decrypt
S_h S_m ...... S_j S_i ...... S_k S_n
get S_1 and its position
$S_1 + k_A$
decrypt
S_a S_1 S_b
get S_2 and its position
$S_2 + k_A$
decrypt
S_c S_1 S_2 S_d
get S_3 and its position

Fig. 5 The decryption process

4.3 Route verification

In this subsection, we present the process of route decryption and verification at the destination center.

Once the vehicle passes the authorization test shown in Algorithm 1, it sends all the $m + 1$ encrypted routes to the destination center. C_E uses the key-generation function $f(x)$ to obtain the key k_A according to the vehicle's identity ID_A and the random number R_A received from the starting center. Without lose of generality, we assume S is one of the encrypted route received from V_A.

The destination center C_E divides S into segments based on the pre-defined length of each ciphertext. Note that $S = \{\cdots, s_i, s_j, \cdots\}$ is out of order. Then, C_E tries to decrypt the route by following the process as shown in Fig. 5.

First, C_E uses k_A to decrypt each ciphertext s_k, $(k = 1, 2, n)$, respectively. In the worst case, C_E needs $n \times (m + 1)$ times of decryption attempts to locate the s_1 successfully, which can be decrypted by k_A. Note that, s_1 is the one that has the first tag t_1's location. After t_1 located successfully, C_E uses $s_1 + k_A$ to decrypt the ciphertexts located at both sides of s_1 to obtain t_2. It need at most 2 times of decryption attempts to obtain t_2's location. Similarly, C_E uses the key $k_j = s_{(j)} + k_A$ to decrypt the ciphertext located at the both ends of the ciphertext block $\{s_{j-1}, \cdots, s_j\}$ or $\{s_j, s_{j-1}, \cdots\}$ to obtain the location of t_{j+1}. It also needs at most 2 times of decryption attempts. Accordingly, the destination center needs at most $2 \times (n - 2) + n \times (m + 1)$ decryption attempts to decrypt the whole route.

The destination center compares the decrypted route with the pre-specified route. If the decrypted route has passed the integrity test, the vehicle can access the restricted area.

4.4 Randomly chosen tag reading

Supposing we ask the vehicle to read all the tags deployed on the road (in other words, the recorded route is static), the user can attack the system by the following steps. (1) The user gets a correct ciphertext block $S = \{s_1, s_2, \cdots, s_n\}$ from its previous trips. (2) He compare the correct ciphertext with the current block $S' = \{s'_1, s'_2, \cdots, s'_n\}$. If a portion of the ciphertext block is similar, he can infer the two paths used in the same key k_A. (3) the user can report the previous ciphertext block $\{s_1, s_2, \cdots, s_n\}$ to deceive C_E. In summary, the route is prone to be tampered if the user can obtain enough number of correct ciphertext blocks (driving on the same route).

In order to address this problem, we propose to randomly read tags on a tag densely deployed road so that the recorded router can be dynamic. As, the key is generated by combining k_A with the existing ciphertext block, we can have different ciphertext blocks every time when driving on the same route. In addition, randomly reading tags can also reduce the number of ciphertext and the computational complexity of encryption and decryption. On the other hand, the random tag read scheduling should be designed carefully. Two consecutive readings should not be too far away so that we can be sure the vehicle is still on the predefined route, and the number of readings should be sufficient to guarantee the security (the length) of the key.

In this paper, we assume that the tag is deployed in every 10m to deal with the intricacies of urban roads. Additionally, in order to track the vehicle's stopping time at each tag and the travel time between two tags, the reader logs each reading with the time of reading.

5 Algorithm security analysis

The algorithms such as Hash algorithm and Message Authentication Codes (MAC) algorithm can provide data integrity and data origin authentication. Hash functions can map data with different length to the one with a fixed length. They provide a unique relationship between the input message and a smaller hash value. This means that the digital signature provided by hash functions will be different from the original signature once part of the original information is distorted. MAC algorithm is derived from a hash code and generated from the applications such as MD5, SHA-1 and other hash functions.

Although both Hash and MAC can recognize the integrity of the information according to the hash value, the adversaries can get the hash function and get into the control area once it has successfully attacked an authorized vehicle if all the vehicles use the same Hash/MAC algorithm. Assigning different Hash/MAC algorithms to vehicles and keeping changing inner keys are not the best solution as they introduce additional management cost. We therefore come up with an idea of separating keys into two parts and design a novel authorization model based on the dynamic password in this paper.

By separating the user's input from encrypted message, our proposed algorithm can theoretically strengthen the system security and protect the control area from side-channel attack [18]. In traditional authorization, digital signature mostly relies on the sender's secret key. The dynamic password is considered as more secure than static password. To reduce the cost of manage dynamic keys, we introduce the key-generation module to generate a unique key for each authorized vehicle according to the vehicle's identity. By employing this approach, the vehicle only need to provide its identity and the random number to the start center, and the center will generate a unique key for the vehicle accordingly. As the random number changes from time to time, the key is also changed. In addition, as the vehicles carry the key table during the journey instead of a key, the adversary cannot get the correct key from the key table. As the start center and the destination center share the same key-generation function, the vehicle just needs to send its ID and random number to the destination center, and the destination center can get the corresponding key and verify the vehicle's identity.

In order to limit human's motivation and verify the reported route, we propose a novel disordered encryption algorithm. The RFID reader installed on the vehicle records the tag's information when passing by and encrypts it automatically following a certain order. In traditional encryption algorithm, the attacker can get the inner key by cryptanalysis. It means that the attacker can break the regulations and maliciously transform the route into a prescribed one. In our algorithm, as the ciphertext is placed before or after the latest ciphertext randomly, the attackers cannot obtain the original key by cryptanalysis. In other words, the attackers are unable to detour and tamper the route to pass the check.

Compared with the traditional single-vehicle–single-key system, the proposed algorithms can reduce the threat of side-channel attack to the correct key by introducing multi-interference keys and dividing keys into two parts. Our method can avoid the risk of interception in wireless environment, since the password is not exposed to the outside of the vehicle, as the password is not included in communication with the center. Moreover, as the starting center seriatim assigns the password to the user, the user cannot predict what the password is. This avoids human-induced leakage of password.

Furthermore, due to the limitation of positioning technology, plaintext and ciphertext may be obtained by the attackers. This increases the risk of falsifying the information of the route. By disrupting the corresponding relationship of plaintext and ciphertext, our method improves the security of vehicle access control system and increases the difficulties of attacking. Even if the attackers can know the encryption algorithm and the key used to encrypt t_1 is the same, the attacker cannot predict the ciphertext as the sequence is disordered.

Our key cloaking method can resist a series of attacks or threats. For example,

1. The key may be captured by attackers during the time of communication. As we all known, everyone can capture the packets from the air. In order to avoid this problem, in our design, the vehicle only transmits and receives message when departing from the start center or arriving at the destination center. In other words, there is no communication during the journey. As a result, there is no risk of packet leakage.
2. An insincere driver may leak the key. The user only gets a character, which is chosen by the starting center randomly, such as a_2. The *Scode* is constructed based on the random character and the interfered code $(d_1d_2d_3d_4d_5d_6d_7)$, which is also randomly generated. The key table $Table_A$ is constructed based on the faked keys and k_A. Since $Table_A$ is stored in the RFID reader, the user cannot easily get it. Even when the user get the key table from the RFID reader, as the correct key k_A is hidden in the key table and the user cannot know the relationship between index value and random character, the user cannot find the correct key. Thus, the insincere driver cannot leak the key.
3. The vehicle may be occupied by attackers. If the vehicle is occupied by attackers, the only thing that attackers can get is the vehicle's identity and the key table, which is stored in the RFID reader, they cannot get the random character that the user knows. Suppose that attackers occupy an authorized vehicle and arrive at the destination center, the destination center will send the corresponding *Scode* to the vehicle according to its identity. Without the random character, which was issued to users by the starting center, attackers cannot find the relationship between index value and random character. Therefore, attackers cannot choose the correct key and pass the validation. If the key table includes n keys, the attackers only has $1/n$ chances to get the correct key.
4. The attackers can masquerade as an authorized vehicle. Attackers can masquerade an authorized vehicle easily as the vehicle's identity is exposed. We assume that the vehicles are authorized before departing the starting center. In other words, the starting center initializes the vehicles and sends the random character and key table to the users and the RFID reader installed on the vehicle, respectively. Thus, if attackers want to masquerade an authorized vehicle, the masquerading has to occur during the journey or at the destination center. The unauthorized vehicle intercepts the authorized vehicle's identity and reports it to obtain the certification when arriving at the destination center. The destination center verifies the identity and transmits the corresponding *Scode* to the vehicle. As the unauthorized vehicle neither has key table in the RFID reader nor the random character that the authorized users know, the attackers cannot successfully have the access to enter the protected area by pretending an authorized vehicle.

6 Conclusion

In this paper, we proposed an access control system that could verify not only the vehicle's identity for accessing a restrict area, but also its route before reaching the area. In our system, we have successfully hidden the key for route encryption from the drivers and the attackers who may take over an authorized vehicle. Moreover, our proposed system can also prevent the attackers from tampering the reported route. In our future work, we plan to design a system that can track the vehicle in real time based on the RFID system on roads so that the center can receive a warning signal and lock the position if the vehicle has taken a detour.

References

1. Cheng W, Cheng X, Song M, Chen B, Zhao W (2012) On the design and deployment of rfid assisted navigation systems for vanets. Parallel Distrib Syst IEEE Trans 23(7):1267–1274
2. Zhou R, Zhao C, Fu L, Chen A, Ye M (2010) Zigbee-based vehicle access control system. In: Intelligent information technology and security informatics (IITSI), Third International Symposium on. pp. 232–235
3. Roesner F, Kohno T, Moshchuk A, Parno B, Wang H, Cowan C (2012) User-driven access control: rethinking permission granting in modern operating systems. In: Security and privacy (SP), 2012 IEEE Symposium on. pp. 224–238
4. Almanza-Ojeda DL, Hernandez-Gutierrez A, Ibarra-Manzano MA (2006) Design and implementation of a vehicular access control using rfid. In: Electronics and photonics. MEP 2006. Multiconference on. pp. 223–225
5. Deriche M, Mohandes M (2012) A hybrid rfid-lpr system for vehicle access control during pilgrimage season in Saudi Arabia. In: Systems, signals and devices (SSD), 9th International Multi-Conference on. pp. 1–6
6. Shu Y, Gu Y, Chen J (2012) Sensory-data-enhanced authentication for rfid-based access control systems. In: Mobile ad hoc and sensor systems (MASS), IEEE 9th International Conference on. pp. 236–244
7. Choi K-H, Lee D (2013) A study about security awareness program based on rfid access control system. In: IT convergence and security 2012. Springer. pp. 87–92
8. Fan X, Zhang Y (2009) A design of bi-verification vehicle access intelligent control system based on rfid. In: Electronic measurement instruments. ICEMI. 9th International Conference on. pp. 1–569-1-573
9. Noman Mohammed MD, Fung Benjamin CM (2009) Walking in the crowd: anonymizing trajectory data for pattern analysis. In: Proceedings of the 18th ACM conference on Information and knowledge management
10. Xu T, Cai Y (2008) Exploring historical location data for anonymity preservation in location-based services. In: INFOCOM. The 27th Conference on Computer Communications. IEEE
11. Nergiz ME, Saygin Y, Atzori M (2008) Towards trajectory anonymization: a generalization-based approach. In: SPRINGL ’08 Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS
12. Abul O, Bonchi F, Nanni M (2008) Never walk alone: uncertainty for anonymity in moving objects databases. In Data engineering, 2008. ICDE 2008. IEEE 24th International Conference on. pp. 376–385
13. Yarovoy R, Lakshmanan LV, Wang WH, Francesco B (2009) Anonymizing moving objects: how to hide a mob in a crowd?. In: Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology
14. Gidofalvi G, Huang X, Pedersen T (2007) Privacy-preserving data mining on moving object trajectories. In: Mobile data management, 2007 International Conference on, pp. 60–68
15. Sweeney L (2002) K-anonymity: a model for protecting privacy. 10(557)
16. Terrovitis M, Mamoulis N (2008) Privacy preservation in the publication of trajectories. In: Mobile data management, 2008. MDM ’08. 9th International Conference on, pp. 65–72
17. Gruteser M, Liu X (2004) Protecting privacy, in continuous location-tracking applications. Secur Priv IEEE 2(2):28–34
18. Marc Joye J-JQ (2001) Hessian elliptic curves and side-channel attacks. Third international workshop paris. Springer, Berlin, pp 402–410