Scholars Journal of Engineering and Technology

OPEN ACCESS

Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com

Research on RFID authentication Protocol in Internet of Vehicles

Pengcheng Sun*, Fei Li

Cyberspace Security College, Chengdu University of Information Technology, Chengdu 610225

DOI: 10.36347/sjet.2021.v09i05.001 | **Received:** 02.05.2021 | **Accepted:** 08.06.2021 | **Published:** 11.06.2021

***Corresponding author:** Pengcheng Sun

Abstract

Review Article

With the development of Internet of Vehicles, radio frequency identification technology (RFID) has been widely used in vehicle networks. The classic RFID authentication scheme cannot meet the special security and confidentiality requirements of RFID in Internet of Vehicles. This paper proposes an RFID authentication protocol in the Internet of Vehicles based on the certification center (CA). Through the certification center, you can avoid the Dos attack problem faced by the back-end server and reduce the server's computing burden. At the same time, through the authentication center, the identity authentication of the back-end server, reader and vehicle tag is indirectly achieved, which solves the problems of replay and malicious tracking that are often faced in RFID. The theory of formal logic language GNY proves that the protocol has high security in the Internet of Vehicles.

Keywords: Internet of Vehicles; RFID; identity authentication.

PREFACE

As a key technology in the Internet of Vehicles, RFID [1] is a non-contact automatic Identification technology. It uses Radio Frequency signals to automatically identify communication objects and obtain relevant information. Widely used in electronic parking charging system (ETC), access control, RFID intelligent parking lot management and other vehicle network application scenarios. The identification and communication of vehicles and readers equipped with RFID electronic tags can be realized by using radio frequency signals.In the Internet of Vehicles, data communication using RFID technology is basically wireless transmission. If there are no effective protection measures for signals exposed in public places, it is easy to be illegally monitored, maliciously stolen and interfered with for replay. To effectively protect the data information in the entire RFID system in the vehicle network, a reliable information security mechanism is required [2]. Therefore, it is very important to study the RFID protocol with high security in the Internet of Vehicles.

1. THE PREPARATORY WORK

At present, researchers have proposed two kinds of solutions for solving RFID security problems [3].One is to prevent privacy leakage by setting the access control list in the RFID tag, so that the information in the RFID tag can not be read at will. Relevant measures mainly include tag failure (KILL command), Faraday cage, blocking tag, antenna energy analysis and so on. The other is to use the knowledge of cryptography to design the RFID authentication protocol to meet the security requirements. In view of the first kind of solution need additional auxiliary equipment, operation cost is higher, and not conducive to label use for a long time, it is hard to get in the car networking actual use such as faults, this paper mainly studies in electronic parking charge system (ETC) and RFID intelligent parking lot management car networking application scenarios of the second type of networking RFID authentication protocol.

The research of RFID protocol mainly focuses on how to correctly and reliably realize the identity authentication among back-end server, vehicle tag and reader. A complete RFID protocol should solve the problems of eavesdropping attack, replay attack, privacy protection and malicious tracking tag.

1.1. Current status of foreign research

In foreign countries, Xie [4] and others introduced a cloud-based RFID authentication scheme. The cloud server in the agreement has strong computing power and large storage space. The reader and the cloud server are connected through a virtual private network (VPN) for communication to ensure security; the protocol uses hash functions for tag information to ensure the confidentiality of the tag to a certain extent, but the information sent by the tag to the reader in the second step of the protocol will not be updated in the next authentication update. Therefore, there is a hidden danger of tags being tracked maliciously. At the same time, the use of VPN in the back-end channel increases the cost of the system. On the basis of the Xie protocol, Sarah [5] and others also proposed an RFID authentication protocol based on the cloud server. Although this protocol solves many deficiencies of the Xie protocol, new security problems have also appeared. Due to the tag ID in the protocol The hash value of is sent out in plain text, so that the attacker can intercept and predict part of the next authentication information, and then track the tag; at the same time, the confirmation information sent by the cloud service to the reader at the end of the agreement is not explained, resulting in The system may have certain security risks. Pakina [6] introduced an RFID authentication protocol that can be used in the non-stop toll collection system in the Internet of Vehicles. This protocol realizes the mutual identity authentication of the tag and the server, and solves the problems of replay attacks and malicious tracking, but it still faces the danger of Dos attacks. Kumar [7] proposed an elliptic curve-based RFID in-vehicle cloud computing (RSEAP) secure and efficient authentication protocol. This protocol introduces a timestamp to prevent replay attacks, but lacks the authentication of the tag to the reader, which is very easy. Through malicious monitoring and then tracking tags. Alamr [8] and others also proposed an ECC-based RFID authentication protocol, which has high security, but in this protocol, in addition to the task of calculation, the reader must also save all the scopes of it. The tag information increases the storage burden of the reader and cannot be directly applied to the Internet of Vehicles. Sun [9] et al. proposed a new private label authentication protocol based on jump tables. This protocol not only guarantees good authentication performance, but also provides a high privacy protection mechanism. However, due to some limitations of the protocol itself, it cannot be directly extended to label authentication in the Internet of Vehicles.

1.2. Research state in China

Many domestic scholars have also done a lot of research on the RFID authentication protocol in the Internet of Vehicles. Jiang Wei [10] and others proposed a cloud-based RFID privacy protection protocol based on the Schnorr identity authentication mechanism. In this protocol, the tag information will be continuously updated with the establishment of each session, which is well protected. The true identity of the label. However, the agreement uses constant information for the identity authentication of the reader and the cloud, and there is a possibility that the identity of the reader may be compromised by an attacker; at the same time, the agreement does not specify the confirmation that the cloud server sends to the tag after successfully updating the tag information Information, there is a possibility of replay attack. Wang Jie [11] and others proposed an RFID mutual authentication protocol based on a lightweight hash function and a dynamic ID mechanism combined with a shared key. This protocol reduces the computational cost of tags, but through in-depth analysis, it is found that the protocol cannot provide tag pairs. For the identity authentication of the reader, the illegal person can intercept the session data between the back-end server and the reader to hinder the information interaction between the legal tag and the legal reader, and at the same time fake the reader to send the intercepted information, Deceptive legal labels. Wang Guichao [12] proposed a multi-level RFID authentication protocol based on cloud computing and RBAC policy (role access control). In the authentication process, through the reader ID and PBAC permission rules, different readers are given different permissions, so as to achieve the purpose of protecting the privacy information of the label. Luo Qi [13] proposed a lightweight RFID authentication protocol based on cloud computing. This protocol generates a different time stamp for each authentication and stores and updates it as part of the tag information, which can be used to a certain extent. Avoid replay attacks; the authentication between the reader and the cloud server in this protocol is achieved through shared keys and shared encryption algorithms. Due to the fixedness of the keys, there is a possibility of being cracked; at the same time, if the agreement is updated at the end If the confirmation information is disturbed, it may cause an error in the next communication between the tag and the reader. Guo Yanhui [14] proposed an RFID authentication protocol based on elliptic curve cryptography, which can effectively resist replay attacks by selecting elliptic curve security parameters and random numbers. However, in this protocol, because the electronic tag must save every reading the public key of the writer is not ideal for use in the Internet of Vehicles. Li Wenjiang [15] introduced an RFID authentication protocol based on the key distribution center, which can effectively solve the Dos attack problem faced by the back-end server in the Internet of Vehicles. However, the protocol assumes that the communication between the reader and the server is secure and cannot be eavesdropped. In practical applications, if the communication channel is compromised, the attacker can easily gain the trust of the tag and obtain the private information of the electronic tag through the fake reader. At the same time, the attacker can cause the server and the legitimate electronic tag to pass the fake electronic tag. Label key update is out of sync. Although the protocols proposed by the above scholars more or less have some problems to be solved, their design ideas and methods are worthy of our reference.

2. The composition and security requirements of RFID systems in the Internet of Vehicles

A complete car networking RFID system generally consists of three physical parts and two communication channels: RFID tags, readers, back-end servers, wireless communication channels, and back-end network communication channels. The back-end server stores vehicle information and has powerful computing capabilities; tags store vehicle information and also have certain computing capabilities; readers are generally built in smart parking lots, intersections, toll stations, etc., and can sense within a certain distance, and establish communication with it. Generally speaking, the communication between the tag, the reader and the server is all wireless communication. For an attacker, all three entities and two communication channels in the RFID system can be the target of the attack. Therefore, the security requirements of the RFID system of the Internet of Vehicles mainly include:

1. Mutual authentication: It is necessary to ensure that each party in the RFID system correctly authenticates the other party.
2. Confidentiality: All secret information is exchanged securely in all communication processes, which requires encryption of information.
3. Anti-malicious tracking: The attacker cannot mark the user's identity for malicious tracking by intercepting the communication information.
4. Forward security: It is necessary to ensure that even if an attacker cracks the key of the current communication, he cannot crack the previous conversation information.
5. Anti-replay attack: Even if the attacker can eavesdrop and capture the conversation from one party to the other, he cannot replay the same information previously sent to pass system verification.
6. Anti-Dos attack: Sending service requests with a large number of illegal tags at the same time will not cause the backend server to crash.

In response to the above security requirements, this paper proposes an RFID authentication protocol based on an authentication center, which solves the problem of direct communication between back-end servers, tags and readers without authentication. Through the authentication center, the request load of the server is reduced, and the back-end server can also be prevented from Dos attacks. Usually, the communication channel between the authentication center and the server is safe by default and cannot be eavesdropped. When the tags and readers communicate with the back-end server, they must pass the key authentication of the certification center before they can get the service of the server.

3. SPECIFIC AGREEMENT

3.1. Symbol interpretation

The explanation of the symbols used in the agreement is shown in Table 1.

Table-1: Explanation of all symbols in the agreement

symbol	description
Q	Request information sent by the reader
TID	Unique identifier of the label
R_2	Random number generated by label
key_t	Shared key between label and server
key	Shared key between reader and certification authority
RID	The unique identifier of the reader
R_1、R_3	Random number generated by the reader
h()、g()	Hashing
R_4	Random number generated by the certification center
$\|\|$	Connect operation
$\oplus$	XOR operation

3.2. Initialization

Each tag saves its own unique g(TID) and key_t. The TID is assigned by the back-end server, and the key_t is updated synchronously every time the tag is successfully authenticated with the certification center. CA is the certification center, and it saves a list of reader information RL, which stores the RID and (a, p) of each reader. The server saves a tag information list TL, which stores the TID and key_t of each tag. The authentication between the reader and the certification center is achieved through a verification key, which is based on the idea of DH key exchange algorithm. Table 2 lists the main parameter symbol variables stored in each part of the system, where p is a large prime number that meets the requirements, a is the generator of the cyclic group Zp, a and p are not public, and each reader and certification center saves The only (a, p).

Table-2: RFID system save parameters

System part	Storage parameters
Server	{ TID，key_t }
CA	{RID，a，p }
Reader	{g(RID)，a，p }
Tag	{g(TID)，key_t}

3.3. Agreement process

(1）Reader→Tag：R_1、Q；Reader→CA：h (g(RID) $\oplus R_1$)，R_1。

Reader generates random number R1 and query command Q, and sends them to Tag as an authentication request.

(2）CA→Reader：S_c，R_3，D；Tag→Reader：A，B，R_T。

After CA receives the authentication request from Reader, it searches RL, calculates h(g(RID) ⊕R_1), finds the reader that communicates with it, generates random numbers R_2, R_3, and calculates Sc=a^{R2}(modp), calculate D=h(R_3||R_1||g(RID)||S_c), send S_c, D, R_3 to Reader. After Tag receives the query command from Reader, it generates random number RT, calculates A=h(g(TID) ⊕key_t⊕R_T), B=h(R_1||R_T||A), and then sends A, B, R_T to Reader.

(3）Reader→CA：A，B，R_T，S_r，T_r，key，F。

After the Reader receives the information from CA, it calculates D'=(R_3||R_1||g(RID)||S_c), and then compares whether D and D'are equal. If they are not equal, the authentication ends; otherwise, generate a random number R_4, calculate Sr= a^{R4}(modp), key= S_c^{R4}(modp), generate a timestamp Tr, calculate F=h(g(RID)⊕S_r⊕key⊕T_r ⊕R_3), then send A, B, R_T, S_r, T_r, key, F to CA.

(4）CA→Server：A，R_T；

After the CA receives the verification information sent by the Reader, it generates a time stamp Tc to verify the certification life cycle T. If the certification life cycle conditions are not met, the certification will end; if T_r<T_c and T_c－T_r≤T, calculate B'=h(R_1||R_T||A), F'= h(g(RID)⊕S_r ⊕key⊕T_r⊕R_3), if F and F'are not equal or B and B'are not equal, the authentication is ended, otherwise, key'= S_r^{R2}(modp) is calculated, and key and key' are compared whether they are equal, if not, If the reader is illegal, end the authentication; otherwise, the reader is legal, and send A, R_T to the server.

(5）Server→Reader：G、R_5；

After receiving the authentication information, Sever queries TL. If there is no A, the label is illegal and ends the authentication; otherwise, it generates a random number R_5, calculates G=h(g(key_t) ⊕R_T⊕R_5), and sends G and R_5 to Reader. Then, calculate key_t=h(g(key_t)⊕R_T), and update the corresponding tag information in the list TL.

(6）Reader→Tag：G、R_5；

After Reader receives the information from S, it forwards G and R_5 to Tag.

(7）After the Tag receives the authentication information from the Reader, it calculates whether G'= h(g(key_t) ⊕R_T⊕R_5) is equal to G. If it is equal, then the Reader is authenticated as legal, update key_t = h(g(key_t)⊕R_T); If the authentication fails, the authentication ends.

The authentication flow chart of the agreement is shown as in Fig. 1.

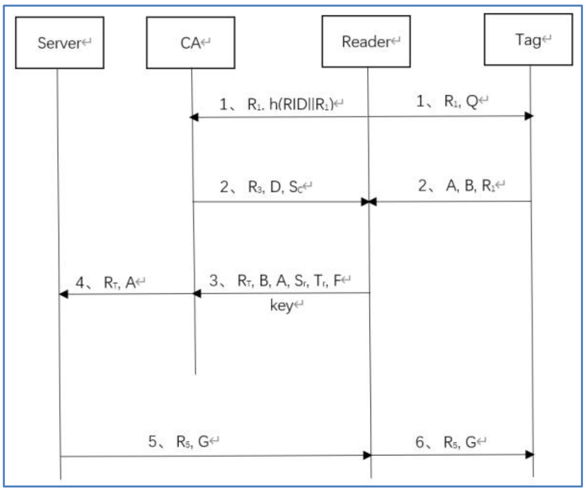

Fig-1: RFID authentication protocol

4. PROTOCOL SECURITY ANALYSIS AND PROOF

4.1 Protocol security analysis

This article analyzes the security of the proposed protocol from the following aspects:

(1) Malicious tracking: In the authentication process of the protocol, after the tag receives the request information from the reader, the response $A = \mathrm{h}(g(TID) \oplus key\_t \oplus R_T)$ contains a random number R_T, that is, the information in each response is different, and the tag cannot be located and tracked. Even if the attacker intercepts the message A, due to the one-way nature of the hash function, the value of the tag TID cannot be obtained.

(2) Replay attack: In the authentication process of the protocol, if the attacker captures the authentication information between the authentication center, the reader and the tag, the replay attack cannot be launched during the execution of the subsequent authentication protocol. Because these related authentication information have introduced a random number mechanism and timestamp to ensure the freshness of the data, at the same time, the shared key key_t of the tag and the certification center and the certification key key of the certification center and the reader change every time . Therefore, attackers cannot perform replay attacks on tags, readers and servers.

(3) Counterfeit attack: For reader counterfeit attacks, the attacker will pretend to be a legitimate reader to send query information to the tag. At the same time, the reader will send the random number generated by itself to the authentication center to request

authentication. When the attacker receives the response information from the tag and the authentication center, the fake reader will not be able to send the correct authentication information to the authentication center because the fake reader does not have a legal RID and the correct (a, p). Therefore, it is difficult for an attacker to launch a counterfeit reader attack. For tag counterfeiting attacks, when the reader sends query information, since the counterfeit tag does not have a legal TID and keyt, it will fail during server authentication.

(4) Initiate a Dos attack on the server: Since the authentication center is added to the protocol, only the authentication information sent by the legal reader will be recognized by the authentication center and forwarded to the server. If the tag does not have a legal reader to forward authentication information, even if a large number of illegal tags require communication with the server, they will be intercepted by the authentication center, thus avoiding the server from Dos attacks.

(5) Two-way authentication: In this protocol, the server's authentication of the reader is implemented through the certification center. The tag and the back-end server store the shared key key_t and the tag's TID that can be updated, so only legal tags are available. The authentication of the server can only be passed through the authentication information forwarded by the legal reader, thus realizing the authentication of the label by the server and the reader; the authentication of the reader and the server by the label is the last authentication forwarded by the authentication center and the reader The information is completed, the shared private information (RID, a, p) is stored between the certification center and the reader. Only a legitimate reader can send the certification information correctly, and can receive it after passing the certification of the certification center. The correct authentication information from the server is forwarded to the tag, and the tag is calculated to verify the legitimacy of the reader and the server.

(6) Forward security: In this protocol, all random numbers and timestamps Tr used are generated temporarily during the authentication process, and only act on the current authentication process. When the next authentication starts, these values have been regenerated there is no direct connection before and after. At the same time, the result of the logical operation involved in these data is temporary and fresh, which means that even if the attacker obtains the current authentication information, it is difficult to calculate the previous historical data. Therefore, this protocol satisfies the system's requirements for forward security.

4.2. Formal Proof of Agreement

GNY logic has made up for the shortcomings of BAN logic due to its own good characteristics, and is currently recognized as the most influential BAN logic. Therefore, the protocol proposed in this paper uses GNY logic to analyze and prove. Literature [16] introduces the specific grammar and related reasoning rules of GNY logic in detail. The formal analysis and security proof of GNY logic of the protocol are as follows.

(1) Use GNY logic language specification to describe the protocol process

$$\text{S1：R→T：}\ T \triangleleft *R_1\text{；}\ \ \text{R→C：}\ C \triangleleft *\mathrm{h}(\mathrm{g}(RID) \oplus R_1)\text{，}\ *R_1$$

$$\text{S2：C→R：}\ R \triangleleft *\mathrm{h}(R_3 \,\|\, R_1 \,\|\, \mathrm{g}(RID) \,\|\, S_{\mathrm{c}})\text{，}\ *R_3\text{；}$$

$$\text{T→R：}\ R \triangleleft *\mathrm{h}(R_1 \,\|\, R_T \,\|\, A)\text{，}\ *\mathrm{R}_{\mathrm{T}}\text{，}\ *A\text{；}$$

$$\text{S3：R→C：}\ C \triangleleft *h(\mathrm{g}(RID) \oplus S_r \oplus \mathrm{key} \oplus T_r \oplus R_3)\text{，}\ *T_{\mathrm{r}}\ \text{；}$$

$$\text{S4：C→S：}\ S \triangleleft *h(g\left(TID\right) \oplus key\_t \oplus R_T)\text{，}\ *R_T\text{；}$$

$$\text{S5：S→R：}\ R \triangleleft *h(g\left(\mathrm{key\_t}\right) \oplus R_T \oplus R_5), *R_5\text{；}$$

$$\text{S6：R→T：}\ T \triangleleft *h(g\left(\mathrm{key\_t}\right) \oplus R_T \oplus R_5), *R_5\text{；}$$

(2) Conditional assumptions

$$\text{Assumption 1：}\ R \ni (\mathrm{g}(RID), key), R_1, \mathsf{T}_{\mathrm{r}}\text{；}$$

$$\text{Assumption 2：}\ T \ni (\mathrm{g}(TID), key\_t), R_T\text{；}$$

$$\text{Assumption 3：}\ C \ni (g\left(RID\right)\text{，}\ \mathrm{key}\ ), R_3\text{；}$$

$$\text{Assumption 4：}\ S \ni (TID, key\_t), R_5\text{；}$$

$$\text{Assumption 5：}\ R \mid\equiv C \xleftrightarrow{\mathrm{g}(RID),\mathrm{key}} R\text{；}\ C \mid\equiv R \xleftrightarrow{\mathrm{g}(RID),\mathrm{key}} C\text{；}$$

$$S \mid\equiv T \xleftrightarrow{\mathrm{g}(TID),key\_t} S\text{；}\ T \mid\equiv S \xleftrightarrow{\mathrm{g}(TID),key\_t} T\text{；}$$

(3) Prove the goal

$$\text{G1：} C|\equiv R|\sim \#\{T_r, h(g(RID)\oplus S_r \oplus key \oplus Tr \oplus R_3)\text{；}$$

$$\text{G2：} S|\equiv T|\sim \#\{R_T, h(key\_t \oplus g(TID) \oplus R_T)\}\text{；}$$

$$\text{G3：} T|\equiv S|\sim \#\{R_5, h(g(key\_t) \oplus R_T \oplus R_5)\}\text{；}$$

(4) Proof of agreement

Prove Goal G1:
From the ownership rules and S3, it can be inferred:

$$C \ni \#T_r$$

According to the informed rule and S3:

$$C \triangleleft (g(RID) \oplus S_r \oplus key \oplus T_r \oplus R_3)$$

From Hypothesis 3 and the freshness rule:

$$C \ni (g(RID), key)$$

From Hypothesis 5 and the identifiable rule:

$$C |\equiv h(g(RID) \oplus S_r \oplus key \oplus T_r \oplus R_3)$$

From Hypothesis 5 and S3, we can see:

$$C |\equiv \#(g(RID) \oplus S_r \oplus key \oplus T_r \oplus R_3)$$

From the assumption 5, message interpretation rules and the above reasoning, we know:

$$C |\equiv R|\sim(g(RID) \oplus S_r \oplus key \oplus T_r \oplus R_3)$$

From S3 and the above inference:

$$C|\equiv R|\sim \#\{T_r, h(g(RID) \oplus S_r \oplus key \oplus Tr \oplus R_3)\}$$

Prove Goal G2:
From the ownership rules and S4, it can be inferred:

$$S \ni \#R_T$$

According to the informed rule and S4:

$$S \triangleleft (g(TID) \oplus key\_t \oplus R_T)$$

From Hypothesis 4 and the freshness rule:

$$S \ni (g(TID), key\_t)$$

From Hypothesis 5 and the identifiable rule:

$$S |\equiv h(g(TID) \oplus key\_t \oplus R_T)$$

From Hypothesis 5 and S4, we know:

$$S |\equiv \#(g(TID) \oplus key\_t \oplus R_T)$$

From the assumption 5, message interpretation rules and the above reasoning, we know:

$$S |\equiv T|\sim (g(TID) \oplus key\_t \oplus R_T)$$

From S4 and the above inference:

$$S |\equiv T|\sim \#h(g(TID) \oplus key\_t \oplus R_T)$$

In the same way, the above-mentioned similar method can be used to prove G3.

5. CONCLUDING REMARKS

The number of vehicle tags in the Internet of Vehicles is huge and mobile is very strong. The traditional RFID system cannot be directly used in the Internet of Vehicles. This article introduces an RFID security authentication protocol in the Internet of Vehicles, which can ensure the communication security of the RFID system in the Internet of Vehicles. Through the use of the authentication center, the identity authentication between the reader, tag, and server is indirectly realized, which solves the problems of Dos attacks, malicious tracking, counterfeiting attacks and replay attacks faced by back-end servers. Finally, this paper uses the formal analysis method of GNY logic to prove the security of the protocol. The introduction of the authentication center into the protocol can reduce the computing load of the server, improve service efficiency, and ensure the safety of the Internet of Vehicles system. RFID technology has broad application prospects in the Internet of Vehicles. The protocol proposed in this article is of great significance to the development of RFID security in the Internet of Vehicles.

REFERENCES

1. Shu, Y., Shao, J., Lu, T. (2019). Application of RFID technology in 5G Internet of Vehicles [J]. Communication World, 26(10): 21-23.
2. Wang, H. (2016). Smart city network security risk analysis and standardization research [J]. Information Technology and Standardization, 3; 46-49.
3. Tao, Y., Zhou, X., Ma, Y., & Zhao, F. (2016). Mobile mutual authentication protocol based on hash function. Journal of Computer Applications, 36(3), 657-660.
4. Xie, W., Xie, L., Zhang, C., Zhang, Q., & Tang, C. (2013, April). Cloud-based RFID authentication. In 2013 IEEE international conference on RFID (RFID) (pp. 168-175). IEEE.
5. Abughazalah, S., Markantonakis, K., & Mayes, K. (2014). Secure improved cloud-based RFID authentication protocol. In Data privacy management, autonomous spontaneous security, and security assurance (pp. 147-164). Springer, Cham.
6. Ghosh, P., & Mahesh, T. R. (2016, November). A privacy preserving mutual authentication protocol for RFID based automated toll collection system. In 2016 International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-5). IEEE.

7. Kumar, V., Ahmad, M., Mishra, D., Kumari, S., & Khan, M. K. (2020). RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing. Vehicular Communications, 22, 100213.
8. Alamr, A. A., Kausar, F., Kim, J., & Seo, C. (2018). A secure ECC-based RFID mutual authentication protocol for internet of things. The Journal of Supercomputing, 74(9), 4281-4294.
9. Sun, M. T., Sakai, K., Ku, W. S., Lai, T. H., & Vasilakos, A. V. (2015). Private and secure tag access for large-scale RFID systems. IEEE Transactions on Dependable and Secure Computing, 13(6), 657-671.
10. Zheng, L., Song, C., Cao, N., Li, Z., Zhou, W., Chen, J., & Meng, L. (2018). A new mutual authentication protocol in mobile RFID for smart campus. IEEE Access, 6, 60996-61005.
11. Yang, K., Xiao, M., Song, J., Chen, J., Zhong, X., & Wang, X. (2018). Proving Mutual Authentication Property of KerNeeS Protocol Based on Logic of Events. IEEE Access, 6, 51853-51863.
12. Wang, G. (2020). Research on multi-level RFID authentication protocol based on cloud computing and RBAC strategy [J]. Science and Technology and Innovation, 05; 85-86.
13. Luo, Q. (2019). Research on RFID-based secure car networking authentication protocol [D]. Xidian University.
14. Zhang, X., Guo, Y. (2018). Research on RFID system security authentication protocol based on elliptic curve cryptography [J]. Information Network Security, 10; 51-61.
15. Xiao, J., Li, W., Geng, H., Zhai, Y. (2019). RFID security authentication protocol that can resist DoS attacks in the Internet of Vehicles [J]. Journal of Beijing University of Posts and Telecommunications, 42(02); 114-119.
16. Zheng, Y. (2015). Hash function-based RFID security authentication protocol for wireless connection [D]. Jilin University.