Received September 20, 2024, accepted October 6, 2024, date of publication October 15, 2024, date of current version November 9, 2024.

Digital Object Identifier 10.1109/ACCESS.2018.2875973

A New Mutual Authentication Protocol in Mobile RFID for Smart Campus

LIJUAN ZHENG[1], CHUNLEI SONG[1], NING CAO[2], ZHAOXUAN LI[1], WENFENG ZHOU[1], JIANYOU CHEN[3], and LILI MENG[4,5]

[1]School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang 050043, China
[2]College of Information Engineering, Qingdao Binhai University, Qingdao 266555, China
[3]Hebei Coal Safety (Security) Training Center, Qinhuangdao 066100, China
[4]Department of Information Science and Engineering, Shandong Normal University, Jinan 250358, China
[5]School of Engineering Science, Simon Fraser University, Burnaby, BC V5A 1S6, Canada

Corresponding author: Ning Cao (ning.cao2008@hotmail.com)

This work was supported in part by the Hebei Education Department under Grant QN2015231, in part by the Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, in part by the Research and Practice of Higher Education Teaching Reform of the Hebei Education Department under Grant 2016GJJG112, in part by the Doctoral Scientific Research Foundation of Shijiazhuang Tiedao University under Grant Z991015137, in part by the Natural Science Foundation of Hebei Province under Grant F2017210161 and Grant F2018210109.

ABSTRACT At present, with the increasingly growing application of Internet of Things, virtualization and intelligent technologies, and the maturity of smart campus systems, campus card technology based on radio frequency identification (RFID) has developed rapidly. Due to the convenience of use, it is widely used in dormitory access control system, book borrowing system, attendance system, and payment system. Because the data carried by the RFID card is more and more complex, the requirements for its security are getting higher and higher. In order to solve the problem of identity authentication and privacy protection of the RFID application existed in the digital campus in recent years, an improved mutual authentication protocol in mobile RFID for smart campus is put forward by analyzing and studying existing smart campus authentication protocols based on hash algorithm, which uses the technology of random number S and time stamp T. This protocol implements mutual authentication among the tag, reader, and backend database without the premise that the signal path between the database and reader communication is a safe signal path and can effectively resist counterfeit attack, replay attack, position tracking attack, de-synchronization attack, eavesdropping attack, denial of service attack, and man-in-the-middle attack, and it can also guarantee forward security. Due to the large data operations and storage have been transferred to readers and backend data, the protocol is formally proved to have a strong reliability and a good security. In addition, through the comparison with other existing authentication protocols on the resident variable storage overhead, the cost of computing complexity and the security performance, the authentication protocol proposed in this paper has a better storage and calculation performance, and it can better satisfy the security requirements in mobile RFID applications for smart campus in the future and has a good application prospect.

INDEX TERMS Smart campus, mutual authentication, mobile RFID, hash function.

I. INTRODUCTION

In the last few years, more and more applications of RFID (Radio Frequency Identification) technology can be seen. It has been used in multiple environments, for example access control system, electronic traceability, food traceability and product anti-counterfeiting [1]. Especially in the context that current campus security cannot guarantee the stable development of colleges and universities, in order to improve campus security issues, RFID technology has been applied more and more widely. Many colleges and universities have set up digital campuses, provided basic security alarms and other information technologies. Combined with the construction or renovation of campus facilities, campus cards including access control systems, firefighting systems, monitoring systems and electronic patrol systems, etc. have been established [2]. Based on the school's Internet environment, a number of payment and management related systems are integrated. Through the use of campus cards, the campus

digital application platform is seamlessly integrated. Through the unified authentication and data sharing center on the school's digital platform, all kinds of application systems in the school that need to be applied through the campus card are integrated [3], so that the campus cards can truly replace all kinds of campus credentials, which not only provide convenience for teachers and students, but also improve the campus security index. These facilities and the application of technology have eased the pressure on campus security to a certain extent [4]. But along with the extensive application of the RFID system and rapid evolvement of Internet of Things technology [5], the security problem becomes more and more severe, which has still not solved the campus security problem fundamentally. With the continuous promotion and construction of campus card system applications, security threats and hidden dangers have emerged in the development of campus card systems [6]. The existing campus card systems cannot meet the security requirements. RFID technology is the basis and core of the campus card [7]. It carries a variety of information and privacy. Therefore, in mobile RFID systems, how to realize identity authentication and ensure privacy protection are particularly important. So as to guarantee the security and stability of the campus card systems, and better serve teachers and students of university simultaneously, the related technologies of the RFID system should receive extensive attention. Based on the digital campus network, the RFID authentication protocol should be improved to provide a more secure, efficient and more business smart campus card information management system.

RFID technology is a wireless communication technology, it can distinguish specific goals and read related data through the radio signal, and it reads and writes the relevant data without physical contact. A typical RFID system is made up of three sections: reader, tags and backend database system [8]. The tag consists of the product details and confidential data for secure communication. The reader provides a link between the tag and the backend database system, allowing data to be read from the tag and transmitted to the backend database system, which is responsible for storing and processing the data [9]. In traditional RFID systems, fixed readers and backend databases communicate securely through wired communication line. But in mobile RFID systems, mobile readers, backend databases and tags use wireless communication line to realize communication [10], which makes the mobile RFID system have a better mobility. It is more convenient to use and easier to meet user needs compared with traditional RFID. Therefore, it has more extensive application prospects than the traditional RFID system. But because of its wireless communication, mobile RFID systems are more vulnerable to malicious attacks from outside, such as tracking, fake, replay, MTM, and so on. Most scholars at home and abroad usually assume that the signal path between the backend database and reader is safe, which makes their authentication protocols unsuitable for mobile RFID system applications.

Although many authentication protocols applied to mobile RFID systems have been proposed by some scholars, most of them cannot satisfy the security demands of the mobile RFID system such as privacy requirement.

A new mutual authentication protocol for smart campus is put forward, which aims to enhance the system safety and privacy while reducing label cost and improving system authentication performance. It can also solve a number of problems and its key technologies in the current campus security, and has great significance in enhancing the functions and effectiveness of digital campus, promoting the construction of security campus and ensuring the stable development of colleges and universities.

II. RELATED WORK

After decades of development, RFID technology has gradually become the mainstream technology for various identification applications [11]. In various applications of the campus card, due to its increasingly wide range of applications and increasingly complex applications, the security issues that RFID faced are becoming more and more severe [12]. It can mainly be divided into three aspects:

(1) Data security issues. The data security issue is mainly directed at the campus card service providers. It involves the isolation of data from different applications [13]. Since the application scope of the campus card is very wide and constantly expanding, various types of data are concentrated on a single card. It is obviously impossible to allow the reader to acquire various data on the card arbitrarily [14]. The scope of use and access permission of data must be carefully managed, which can neither affect its use of other functions, nor threaten data security.

(2) Personal privacy issues. The issue of personal privacy is mainly aimed at holding users of campus cards. In the modern society, privacy issues are getting more and more attention, and the resulting social problems are also increasing. Because of the wide application of campus cards, the amount of information it carried is also increasing. If there is no effective security and management specification, it will bring great threat to personal information.

(3) Illegal use. The scope of use of campus cards determines that the cost of the card cannot be too high. Therefore, it also limits the security measures that can be used, such as encryption, which may bring about problems that the card may be illegally copied and attacked [15].

At present, researchers have put forward a variety of solutions for the potential security problems in RFID systems, which are mainly classified as two types: one is based on the physical mechanism, and the other is based on the cryptographic mechanism [16]. The methods based on the physical mechanism are mainly divided into kill command method, active interference method and blocking label method, etc. In [17], the protocol used hash function to encrypt the message. Because of the unidirectional characteristic of hash algorithm, the strength of encryption is not weak. It can fully

meet the security requirements of information transmission in the RFID system. In addition, its requirements for hardware devices are not high. It can meet the low-cost requirements for labels [18]. Therefore, RFID authentication protocol based on hash function has attracted more and more attention from scholars both at home and abroad.

In [19], authentication protocol for RFID system based on hash algorithm was divided into three categories, one is randomized hash-lock protocol, the second is hash-lock protocol, and the third is hash-chain protocol. However, due to the continuous update of the security vulnerabilities, the existing protocols are found to no longer satisfy the need for security. In [20], a protocol for lightweight encryption function structure is proposed. It can better satisfy the security demands in the communication process. At the same time, the workload of the server makes the computing load of the server decreased. But during the authentication procedure, the unique identifier and the index value of the tag are all encrypted by a XOR operation. Because of the openness of the hash algorithm, the attacker can easily obtain this information. Therefore, it cannot satisfy the confidentiality and security of the information, and cannot effectively resist various attacks. On the basis of this protocol, ILAP is proposed in [21], which can meet the low-cost requirements of the label while resisting attacks. But it only uses lightweight Encryption functions to perform authentication, the computing load of the server is increased and the authentication efficiency is decreased.

In [22], a bi-directional protocol for RFID has been proposed, the protocol enhances the security of the RFID system on a certain degree, but it only regards the reader as a transfer station between label and back-end database, and the researcher assumes the signal path between backend database and reader is safe, which makes the protocol cannot be applied to mobile RFID systems. In addition, there exists a serious update vulnerability in the protocol, it is vulnerable to de-synchronization attack, if the messages were interrupted by the attacker during the authentication procedure, the back-end database cannot update the T value. But the T value has been updated by the tag. Therefore, it will appear data asynchronous problem at the next authentication.

In [23], a mobile RFID protocol is put forward. The protocol gets rid of the premise that the signal path between the back-end database and reader is safe, which satisfies the security requirement of the mobile RFID system to a certain extent. However, it cannot satisfy the privacy requirements of the user's location, if the attacker constantly replays the same random number R through the illegal reader while sending the certification query, the reader will get the same answer from the tag, so that the user's identity and location may be tracked and derived by attacker according to these same answers.

In [24], an improved ultra-lightweight RFID authentication protocol is proposed, which can resist common attacks such as algebraic attacks, and has higher security under the same network conditions. However, [25] points out that the protocol in [24] cannot effectively resist de-synchronization attack, and the attacker can replay the message to make the key shared by the tag and reader inconsistent. Therefore, subsequent authentication between the reader and the tag will be broken.

In [26], a bidirectional authentication protocol using NFSR is put forward. It can protect the privacy of tags and readers in a mobile environment. However, in the authentication process, tags must generate four random numbers, which increases the cost of tags, thus reducing the efficiency of the certification.

The authentication protocol proposed in [27] lacks identity authentication of the back-end server to readers, it can't resist replay and counterfeit attacks. Therefore, in view of this protocol, a two-way authentication protocol for ultra-lightweight mobile radio frequency identification is proposed in [25]. Although the cyclic check function used in this protocol can reduce the hardware cost of labels and reduce the calculation amount of label, the cyclic redundancy check has a poor security in the hash function. The method can only detect whether the communication information has been tampered with, but cannot protect the communication information from interference.

In [28], a two-way authentication protocol with ownership transfer is proposed. The protocol also uses a less secure cyclic redundancy check during the authentication procedure. Additionally, this protocol is not applicable to mobile RFID applications because of the lack of authentication of backend database to reader. On the basis of this protocol, a mobile two-way authentication protocol is put forward in [29], which is an improved protocol combining with the security demands of mobile RFID applications. The protocol adds the identity of the reader, so it can better resist counterfeiting and replay attacks. However, [30] points out that the two-way authentication protocol in [29] not only increases the computing and storage costs of backend database but also does not provide effective means to resist DoS attacks. If the attacker continuously sends false authentication information to the backend database using a forged reader, the background database will always be in a heavy load. It is easy to cause congestion, resulting in legitimate labels cannot be authenticated. Furthermore, when the protocol has asynchronous data, although it passes the authentication using the stored latest tag identifier, that is, the ID value of the tag, it does not account for whether or not to update the backend database. If the backend database is not updated, the ID value of the tag changed after the label has been authenticated to the database is not consistent with the shared ID of the database, so the legitimate label will not be authenticated again. On the contrary, if the backend database is updated using the previous update method, the label will also not pass authentication if it suffers desynchronization attack again in this authentication. In addition, the protocol ignores the situation where the attacker is located between the backend database and reader in resisting MTM attacks. Once the attacker forges legitimate reader using the intercepted legitimate reader value when located between the backend database and reader,

it can easily pass through the authentication and steal user information.

In [31], an efficient RFID security authentication protocol that can resist DoS attacks is proposed. This protocol solves the DoS attacks effectively by setting a simple XOR operation in the reader. But the protocol ignores the situation in which attackers directly send large amounts of false information using fake readers. The protocol needs to store a unique identifier RID of the reader in advance, that is, the label can only be read by this single reader while other readers can't pass the authentication, which greatly increases the limitations of protocol applications. In addition, there exists a serious security flaw in the protocol, when it sends the reader identifier RID to the backend database, it just performs a simple series operation with the result N of two random number XOR operations, which makes it easy for attackers to get the reader's unique identifier RID, so it can't guarantee the security of the reader. Furthermore, the protocol only includes authentication of backend database to the reader's, lacks of authentication of reader to the backend database. Therefore, it can't meet the security needs of mobile RFID system.

Combined with the security characteristics of mobile RFID and the security requirements of current users, a new improved mutual authentication protocol in mobile RFID for smart campus is put forward. The reader, timestamp of backend database system and the random number of the label are used to increase the system's non-traceability. It is able to effectively handle the location privacy security problem of system reader and tag. Confidentiality of communication is ensured using the Hash function to deal with communication data of each stage, and DoS attack is prevented by setting the filter mechanism in the reader. So that it can use a more simple operation to reduce system computing overhead and label costs in the premise of ensuring security.

III. DESIGN AND FORMAL PROOF OF HASH-BASED MOBILE RFID AUTHENTICATION PROTOCOL

A. PROTOCOL DESIGN

The evaluation parameters and the implications of the improved authentication protocol in this paper are represented as follows.

TABLE 1. The evaluation parameters and the implications.

Signal	Meaning
DB	Database
TID	Tag ID
RID	Reader ID
TID'	Database storage tag ID
RID'	Database storage reader ID
$Query$	Request message
T	The timestamp generated during the reader's authentication process
$T2$	The timestamp generated during the database's authentication process
ΔT	Time interval
$\Delta T'$	Time required by the longest distance authentication recorded in database
S	a random number generated by tag
$\oplus$	XOR operation
$\|\|$	Series operation

The procedure of the new protocol is shown as follows:

(1) The Reader reads the local system time T and sends T and the message Query to the Tag.

(2) When the tag receives the message of authentication request from the Reader, it generates a random number S, it performs series operation with the self-identifier TID and the timestamp T, and uses hash function to generate N1 $=$H (TID||T||S); The time stamp T and the random number S perform XOR operation to generate N2 $=$ T$\oplus$ S, finally it sends (N1, N2, S) to the Reader.

(3) When the Reader receives the response message from the Tag, it calculates S $=$ N2 $\oplus$T, judging whether S' is equal to S. If S' is not equal to S, it shows that the tag is forged, and the communication is terminated. If they are equal, using its own identifier RID, the time stamp T and the random number S to generate N3 $=$H (RID||T||S), finally it sends (N1, N3, T, S) to the DB.

(4) When the database receives the authentication information from the Reader, it extracts local time T2 and calculates T $=$T2-T. Compared with the time ΔT', if ΔT is much larger than T', It is possible to draw a conclusion that there exists attack during authentication process, so that the communication is terminated. If there is no abnormal condition, using T and random number S to traversal the database to see if there exists RID' that satisfies H (RID'||T||S)$=$ N3.If there exists such RID', it shows that the Reader is legal. Otherwise the communication is terminated.

After the Reader is verified successfully, according to the obtained T, S, traversing the database to see if there exists a corresponding tag identifier TID' that satisfies H (TID'||T||S) $=$ N1, If there exists such TID', it shows that the Tag is legal, in the following, N4 $=$ H (TID'||T2), N5 $=$ H (RID'||T2) are calculated, the (N4, N5, T2) is sent to the reader; Otherwise authentication fails and the communication is terminated.

(5) According to T2, the reader calculates the H (RID||T2) to determine whether it is equal to N4, if it is equal to N4, the authentication of reader to back-end database is successful, and then sends (N5, T2) to Tag, otherwise the authentication is failed and the communication is terminated.

The tag calculates H (TID||T2) and compares it with N5. If it is equal to N5, the authentication is successful and then starts to communicate; otherwise, the authentication fails and the communication is terminated.

B. SECURITY PROOF OF THIS PROTOCOL

Formal analysis of security protocols can discover many security vulnerabilities and results in a better understanding of how to design robust protocols [32]. Burrows, Abadi and Needham (BAN) coined a logic for proving the correctness of authentication and key establishment protocols formally.

The BAN logic is one of the formal methods which is used for the analysis of security protocols [33]. After GNY logic was put forward in 1990, it has been classified as BAN logic type. It becomes the most influential BAN logic because of its own good characteristics to make up for the shortage of BAN logic. In the following, GNY logic is used to formally analyze and prove mobile RFID authentication protocol put forward in this paper.

1) FORMALIZATION OF THE PROTOCOL

The message ''not starting from this'' is marked as $*$, and the message is formally explained as follows:

Protocol Generic Type :

$Msg.1\ Reader -> Tag : T$

$Msg.2\ Tag -> Reader : H(TID \| T \| S), S \oplus T, S$

$Msg.3\ Reader -> DB : H(TID \| T \| S), H(RID \| T \| S), T, S$

$Msg.4\ DB -> Reader : H(TID^r \| T2), H(RID^r \| T2), T2$

$Msg.5\ Reader -> Tag : H(TID^r \| T2), T2$

Formalized Protocol :

$Msg.1\ Tag \ni *T$

$Msg.2\ Reader \ni *H(TID \| T \| S), *S \oplus T, *S$

$Msg.3\ DB \ni *H(TID \| T \| S), *H(RID \| T \| S), *T, *S$

$Msg.4\ Reader \ni *H(TID^r \| T2), *H(RID^r \| T2), *T2$

$Msg.5\ Tag \ni H(TID^r \| T2), T2$

2) PROTOCOL INITIALIZATION AND PROOF

The protocol initialization conditions are as follows: (1) $\sim$ (4) are assumed as the possession among the Reader, Tag and backend database DB; (5)$\sim$ (11) are assumed as the trust of the fresh owned by Reader, Tag and backend database DB.

(1) $Tag \in T$
(2) $Tag \in H(X)$
(3) $Reader \in S$
(4) $DB \in H(X)$
(5) $Tag| \equiv \#T$
(6) $Reader| \equiv \#S$
(7) $DB| \equiv \#(S, T)$
(8) $Reader| \equiv \#T2$
(9) $Tag| \equiv \#T2$
(10) $Reader| \equiv Reader -> DB(T, S)$
(11) $DB| \equiv DB -> Reader(T2)$

The proof target of correctness is generally classified into three as follows: that is, the trust on the freshness of interactive information between the interaction entities:

(1) $DB| \equiv Tag| \equiv \#H(TID \| T \| S), H(RID \| T \| S)$
(2) $Reader| \equiv DB| \equiv \#H(RID^r \| T2)$
(3) $Tag| \equiv DB| \equiv \#H(TID^r \| T2)$

On the basis of above initialization conditions, the proof related to GNY logic can be generated, inference rules in [34] is followed.

*Msg*1
(1) $Tag \ni *T$;
(2) $Tag \ni T$;
(3) $Tag \in T$;
*Msg*2
(4) $Reader \ni *H(TID \| T \| S), *S \oplus T, *S$;
(5) $Reader \ni H(TID \| T \| S), S \oplus T, S$;
(6) $Reader \in H(TID \| T \| S), S \oplus T, S$;
*Msg*3
(7) $DB \ni *H(TID \| T \| S), *H(RID \| T \| S), *T, *S$;
(8) $DB \ni H(TID \| T \| S), H(RID \| T \| S), T, S$;
(9) $DB \in H(TID \| T \| S), H(RID \| T \| S), T, S$;
(10) $DB| \equiv \#T \| S$;
(11) $DB| \equiv \#H(TID \| T \| S), H(RID \| T \| S)$;
(12) $DB| \equiv Tag| \equiv \#H(TID \| T \| S), H(RID \| T \| S)$;
(13) $D| \equiv Tag| \equiv H(TID \| T \| S), \| H(RID \| T \| S)$;
(14) $Reader \ni *H(TID^r \| T2), *H(RID^r \| T2), *T2$;
(15) $Reader \ni H(TID^r \| T2), H(RID^r \| T2), T2$;
(16) $Reader \in H(TID^r \| T2), H(RID^r \| T2), T2$;
(17) $Reader| \equiv \#T2$;
(18) $Reader| \equiv \#H(RID^r \| T2)$;
(19) $Reader| \equiv DB| \equiv H(RID^r \| T2)$;
(20) $Reader| \equiv DB| \equiv \#H(RID^r \| T2)$;
*Msg*5
(21) $Tag \ni *H(TID^r \| T2), T2$;
(22) $Tag \ni H(TID^r \| T2), T2$;
(23) $Tag| \equiv \#T2$;
(24) $Tag| \equiv \#H(TID^r \| T2)$;
(25) $Tag| \equiv DB| \equiv H(TID^r \| T2)$;
(26) $Tag| \equiv DB| \equiv \#H(TID^r \| T2)$;

As in the above steps, the correctness of the object is done in step (13), step (20) and step (26). It can be shown that the new mutual protocol in mobile RFID for smart campus is able to meet the security requirements of mobile RFID systems.

IV. PERFORMANCE ANALYSIS OF THE IMPROVED PROTOCOL

A. SECURITY PERFORMANCE ANALYSIS OF IMPROVED PROTOCOL

From the perspective of the security of the protocol, the analysis and demonstration are divided into nine aspects in this paper, and the specific analysis is shown in the following sections:

1) MUTUAL AUTHENTICATION

Mutual authentication refers to the bidirectional verification among the backend server, Reader and tag in the RFID system. During the authentication process proposed in this paper, the back-end database realizes authentication between Reader and tag using the verification of N1 and N3. The Reader realizes authentication of backend database using the verification of N4. The tag realizes authentication of back-end database using the verification of N5.

2) FORWARD SECURITY

Because of the unidirectional property of hash algorithm, the random number generated is uncertain. The timestamp generated by the reader and the backend database in the authentication process is not the same. Even though the tag content is intercepted by attackers, they are not able to deduce the previous content of the tag. So this protocol can effectively ensure forward security.

3) ANTI-COUNTERFEIT ATTACK

In this paper, unique identifier is needed if the attackers want to forge Reader or tag. However, in the entire authentication protocol, the identifier of tag and Reader is encrypted by the hash algorithm during transmission. Because of the unidirectional property of HASH function, even if attackers intercept these hash values, they also cannot parse the correct Reader or tag identifier. Therefore, it is hard for the attackers to fake the legal identifier to be certified successfully.

4) ANTI-REPLAY ATTACK

Replay attack refers to the attacker uses the normal data intercepted in previous authentication communication as the communication data in this authentication and sends to the reader, attempting to pass the authentication. There exist two cases in mobile communication, one is replay tag authentication information, and the other is Reader authentication information. If the tag authentication information is replayed, since the timestamp T generated by the Reader is not the same during each authentication process, even though an attacker replays the authentication information of the legal tag intercepted before, it is not able to be authenticated and even can't pass verification set by the reader in step (3). If Reader authentication information is replayed, when the authentication information is received from the Reader in step (4), the backend database will use the timestamp T2 extracted by itself to carry out a time check with the timestamp sent from the Reader. It is easy to determine whether or not it has been attacked by comparing the time interval with the maximum transmission time interval of the Reader stored in the database.

5) ANTI-LOCATION TRACKING

Location tracking means that attackers send repeated queries to tags, locate tags or even deduce historical track of the tag movement using response information to identify tag identities. In the mobile RFID system, the location information of the tag holder and the Reader holder needs to be protected. This protocol first uses the random number generated by the tag and the timestamp generated by the Reader. Even if the tag receives a duplicate request from an attacker, it will have different answers each time. Therefore, it is hard for attackers to distinguish the specific identification of the tag and track the tag using the information. It is even impossible to deduce the previous activity track of the tag. As for the Reader's location privacy, the Reader will not send any detail related to its identity to tag in this protocol. Thus, the attacker can't acquire any useful information to position the reader. The location tracking is well resisted.

6) ANTI-EAVESDROPPING ATTACK

In the paper, total messages are converted into hash value using hash algorithm. Since the hash function has unidirectional property, the attackers cannot accurately eavesdrop and analyze real and effective messages. Therefore, it can better resist eavesdropping attack.

7) ANTI-MTM ATTACK

MTM attack refers to an attacker located between the two parties of the communication achieves the purpose of passing authentication by tampering with the data in the communication. In this protocol, it is assumed that an attacker carries out MTM attack between the Reader and the tag, then the attacker needs to intercept the timestamp T that the Reader sends to the tag, the random number S of the tag itself, and TID value the unique identifier of the tag to construct a new N1. The timestamp T and the random number S can be obtained by capturing the communication information. But the unique identifier TID does not appear in the communication, the attacker can't obtain a valid TID, so the attacker can't reconstruct a correct N1 value. Similarly, when an attacker carries out MTM attack between the backend database and reader, he also can't reconstruct the correct N3 value to pass authentication because they can't get a legal Reader identifier RID.

8) DE-SYNCHRONIZATION ATTACK

Synchronization attack means that attacker uses flaws existed in identifier update process of tags or readers to make the only shared identifiers among the Reader, tag and backend database inconsistent, resulting in asynchronous data problems, which exists extensively in the authentication protocol that uses dynamic ID [35]. This protocol adopts a static ID mechanism and does not have an update to the unique identifier of tag or reader. So the synchronization attack has no effect on this protocol.

9) ANTI-DOS ATTACK

DoS attack refers to an attacker uses a great amount of illegitimate tags to enter the database through a reader to perform authentication, or uses fake readers to sends a large amount of fake authentication information directly, making the database blocked and cannot handle legitimate tag authentication requests. This protocol filters the illegal label by setting the XOR test to the random number of tags in the Reader. It can solve the DoS attack problem simply and efficiently.

The security performance of the authentication protocol put forward in this article is compared with that in [22], [23], [29], and [31], which is shown in TABLE 2. Where X represents not implemented, √ represents implementation, and O represents partial implementation.

TABLE 2. Comparison of security performance.

Security characteristic	Ref [22]	Ref [23]	Ref [29]	Ref [31]	This protocol
Forward security	√	√	√	√	√
Anti-counterfeit	X	√	√	√	√
Anti-replay	X	√	√	√	√
Anti-tracking	√	X	√	X	√
Anti-eavesdropping	√	√	√	√	√
Anti-man-in-the-middle	X	X	O	√	√
De-synchronize	X	√	X	√	√
Anti-DoS	X	X	X	√	√

Based on the above results in TABLE 2, compared with the above four protocols, this protocol has higher security. It can fully satisfy the security demands of mobile RFID system applications. It has the advantage of anti-counterfeit, anti-replay, anti-man-in-the-middle, anti-DoS and de-synchronize attack that the lightweight authentication protocol proposed in [22] does not have, the advantage of anti-tracking, anti-man-in-the-middle and anti-DoS attack that the mobile authentication protocol put forward in [23] does not have, the advantage of de-synchronize and anti-DoS attack that the mutual authentication protocol proposed in [29] does not have, and the advantage of anti-tracking attack that the anti-DoS authentication protocol proposed in [31] does not have. Based on the above analysis, it shows that the new improved mutual protocol in mobile RFID for smart campus can meet the security needs of mobile RFID system, and it can have a positive impact on protecting the user's privacy and security better.

B. PERFORMANCE COMPARATIVE ANALYSIS OF IMPROVED PROTOCOL

1) PROTOCOL STORAGE OVE RHEAD COMPARISON

In the RFID system, the computational complexity and storage cost of the tag are usually applied to describe the performance of the RFID protocol [36]. This authentication protocol is compared with protocol proposed in [22], [23], [29], and [31]. The evaluation parameters, their meanings and values of the improved authentication protocol in this paper are represented as shown in TABLE 3. The resident variable storage overhead is calculated according to the parameters in it. Resident variable storage cost of each authentication protocol is shown in TABLE 4. The resident variable storage overhead of Tag is shown in FIGURE 1. The resident variable storage overhead of Reader is shown in FIGURE 3. The resident variable storage overhead of Database is shown in FIGURE 4.

TABLE 3. Evaluation parameters.

Parameter	Meaning	Value
L	The storage length of each domain	100
n	The number of tags stored in the database	20
r	The number of the reader	4
S	The number of bits of the random number	2
T_{hash}(ms)	Time cost on one hash operation	1
T_y(ms)	Time cost on one modulo square operation	10
T_n(ms)	Random number generation time	1
T_s (ms)	Timestamp generation time	2

TABLE 4. Protocol resident variable storage overhead comparison.

Analysis factor	Ref [22]	Ref [23]	Ref [29]	Ref [31]	This protocol
Tag	2L	L	L	2L	L
Reader	L	L	L	L	L
Database	2nL	nL+rL	5nL+2rL+LS	3nL+rL	nL+rL

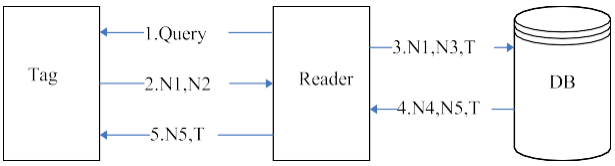

FIGURE 1. The new protocol implementation process.

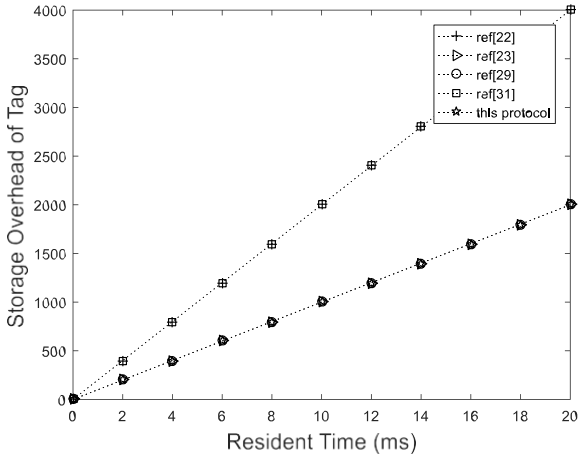

FIGURE 2. Resident variable storage overhead of tag.

Based on the above results in FIGURE 1, FIGURE 3 and FIGURE 4, compared with the lightweight protocol put forward in [22] and the anti-DoS authentication protocol proposed in [31], this protocol has higher performance in the tag resident variable storage overhead. Compared with the mobile authentication protocol proposed in [23], protocol put forward in this paper has similar performance. Compared with the mutual authentication protocol proposed in [29], protocol put forward in this paper has similar performance in the tag resident variable storage overhead, but has higher performance in database storage overhead. Therefore, it shows that this protocol not only can effectively reduce the storage consumption of the tag and the cost of the tag, but also can reduce the storage cost of the database and improve the system performance.

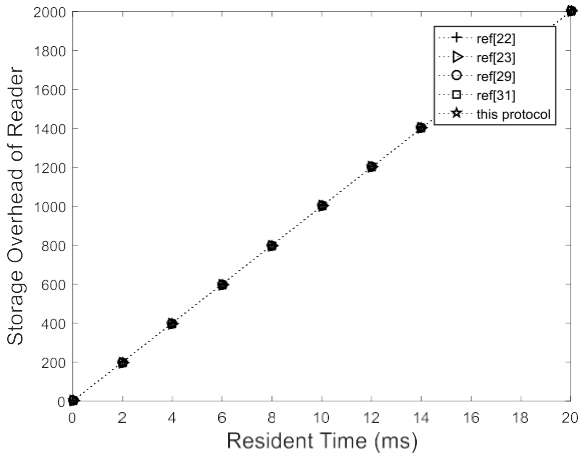

FIGURE 3. Resident variable storage overhead of reader.

2) PROTOCOL COMPUTATIONAL COMPLEXITY COMPARISON

The computational complexity of the authentication protocol put forward in this paper is compared with that in [22], [23], [29], and [31]. The computational complexity of the authentication protocol is shown in TABLE 5. The computational complexity of Tag is shown in FIGURE 5. The computational complexity of Reader is shown in FIGURE 6. The computational complexity of Database is shown in FIGURE 7.

TABLE 5. Computational complexity comparison.

Analysis factor	Ref[21]	Ref[22]	Ref[28]	Ref[30]	This protocol
Tag	$3T_{hash}+T_n$	$2T_{hash}$	$3T_{hash}+T_n+T_v$	$2T_{hash}+T_n$	$2T_{hash}+T_n$
Reader	T_{hash}	$2T_{hash}+T_n$	T_n+3T_{hash}	T_n	$2T_{hash}+T_s$
Database	$3T_{hash}+T_s+T_n$	$(n+r+2)T_{hash}$	$(n+4)T_{hash}+T_n+T_v$	$2T_{hash}$	$(n+r+2)T_{hash}+T_s$

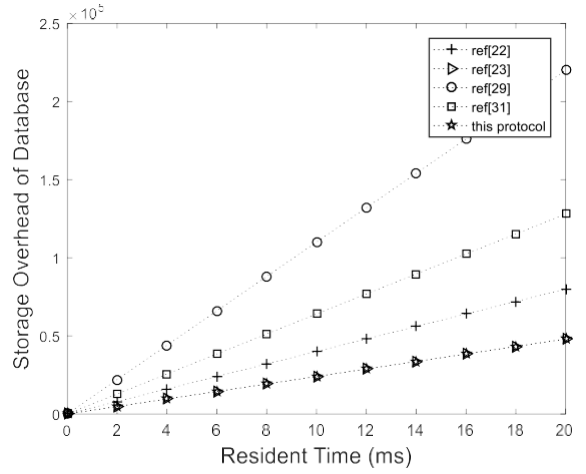

FIGURE 4. Resident variable storage overhead of database.

Based on the above results in FIGURE 5, FIGURE 6 and FIGURE 7, compared with the lightweight authentication protocol proposed in [22], the two-way protocol put forward in [29] and the anti-DoS protocol proposed in [31], protocol proposed in this paper has higher performance in the computational complexity of tag. Compared with the mobile protocol put forward in [23], it is slightly inferior to it. The protocol only adds a random number generation

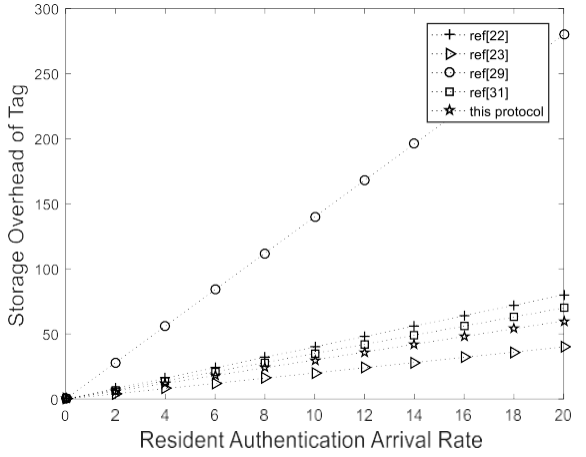

FIGURE 5. Computational complexity of tag.

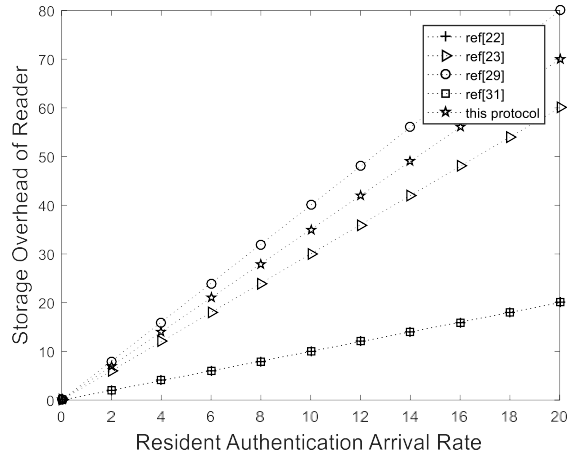

FIGURE 6. Computational complexity of reader.

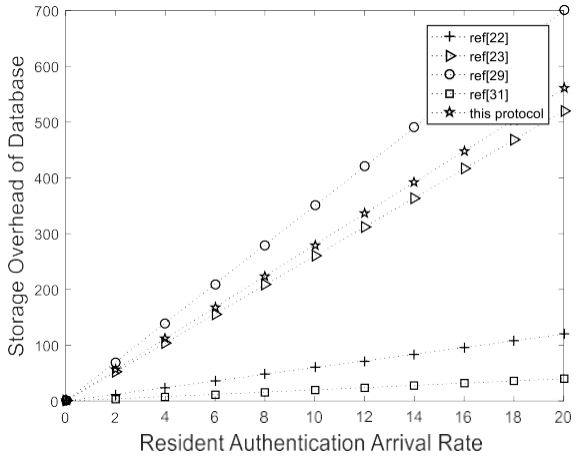

FIGURE 7. Computational complexity of database.

operation compared with the mobile authentication protocol, completely within acceptable level of low cost tag. Although the computational complexity of the reader and backend database in this protocol is slightly inferior to the lightweight authentication protocol proposed in [22], the mobile RFID protocol put forward in [23] and anti-DoS protocol proposed in [31], the protocol proposed in this paper has higher security in anti-Counterfeit, anti-replay, anti-man-in-the-middle, de-synchronize, anti-DoS compared with the lightweight authentication protocol proposed in [22], has higher security in anti-tracking, anti-man-in-the-middle, anti-DoS compared with the mobile protocol put forward in [23], and has higher security in Anti-tracking compared with the anti-DoS protocol proposed in [31]. In addition, with the increasingly growing application of intelligent terminals and information technology, readers and servers will be more powerful, these computing loads do not have a great effect on overall performance.

V. CONCLUSION

In order to solve the issue related to identity authentication and privacy protection of the RFID application existed in the digital campus in recent years and reduce security risks to provide a security, harmonious and comfortable campus learning and living environment, based on the RFID technology application in smart campus, a new mutual authentication protocol applicable to mobile RFID is proposed in this paper, which is not constrained by the premise that the signal path between the database and reader communication is safe. It implements mutual authentication among the backend database, the tag and the reader, so that it can better resist tracking, forgery, replaying attacks, MTM attacks, de-synchronization attacks and DoS attacks, etc. With good confidentiality, the protocol reduces computation and storage of the tag in condition of guaranteeing safety and transfers a great number of data computing and storage to the Reader and back-end database. With the increasingly growing application of information technology and intelligent terminal, these storage space requirements and computation costs will not have a serious effect on performance of the system. Therefore, the protocol fully satisfies the security and cost conditions for mobile RFID systems. It has a good application prospect and can make a positive contribution to the security construction of the smart campus.

REFERENCES

[1] B. Q. Yuan, ''Analysis and design of RFID security protocol in Internet of Things,'' M.S. thesis, Beijing Jiaotong Univ., Beijing, China, 2016.
[2] Z. J. Tang, ''Research on Key Technologies of campus security Internet of Things,'' *Modern Vocational Educ.*, no. 25, pp. 140–141, Sep. 2016.
[3] Z. J. Guo, ''Design and security analysis of intelligent campus card information management system,'' M.S. thesis, Huaqiao Univ., Quanzhou, China, 2017.
[4] Y. C. Xu and Y. Y. Ma, ''Exploration of intelligent campus construction in the age of Internet +,'' *Shandong Ind. Technol.*, no. 15, p. 126, Aug. 2016.
[5] J. Kaur and K. Kaur, ''A fuzzy approach for an IoT-based automated employee performance appraisal,'' *Comput. Mater. Continua*, vol. 53, no. 1, pp. 24–38, Jan. 2015.
[6] S. L. Ma and Z. D. Liu, ''Application of Internet of Things technology in intelligent campus,'' *Internet Things Technol.*, vol. 2, no. 6, pp. 68–69, Jun. 2012.
[7] Y. Xu, J. Zhou, and W. Y. Liu, ''Intelligent campus security inspection system based on RFID technology,'' *Practical Electron.*, no. 1, p. 39, Jan. 2017.
[8] S.-J. Zhou, W.-Q. Zhang, and J.-Q. Luo, ''Survey of privacy of radio frequency identification technology,'' *J. Softw.*, vol. 26, no. 4, pp. 960–976, Feb. 2015.
[9] S. Anandhi, R. Anitha, and V. Sureshkumar, ''An RFID cloud authentication protocol for object tracking system in supply chain management,'' in *Digital Connectivity—Social Impact*. Singapore: Springer, 2016, pp. 247–256.
[10] D. Robin, S. Saravanan, and W. Zhou, ''A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems,'' *Ad Hoc Netw.*, vol. 11, no. 1, pp. 383–396, Jan. 2013.
[11] Y. C. Wu and N. Li, ''Design and implementation of intelligent campus security system,'' *Internet Things Technol.*, vol. 3, no. 8, pp. 79–81, Aug. 2013.
[12] Y. H. Cao, A. Li, and L. Tang, ''Research and design of a smart cross-layer security solution for campus card,'' *J. Beijing Inst. Petro-Chem. Technol.*, vol. 20, no. 2, pp. 29–31, Jun. 2012.
[13] Z. H. Zhou, ''Intelligent campus network based on RFID and campus card,'' *Electron. World*, no. 15, p. 163, Aug. 2014.
[14] S. Q. Zhai, ''Discussion on the application of Internet of Things technology in intelligent campus construction,'' *Electron. Technol. Softw. Eng.*, no. 10, p. 37, Jun. 2016.
[15] D. C. Ranasinghe, D. W. Engels, and P. H. Cole, ''Security and privacy solutions for low-cost RFID systems,'' in *Proc. Intell. Sensors, Sensor Netw. Inf. Process. Conf.*, Melbourne, VIC, Australia, Dec. 2004, pp. 337–342.
[16] Z. Cao, ''Study on security related to RFID technology in Internet of Things,'' M.S. thesis, Xidian Univ., Xi'an, China, 2013.
[17] B. Zhang, ''RFID system security architecture and key technology research,'' M.S. thesis, Univ. Electron. Sci. Technol. China, Chengdu, China, 2014.
[18] P. Anju, S. Mridula, and P. Mohanan, ''High security identity tags using spiral resonators,'' *Comput. Mater. Continua*, vol. 52, no. 3, pp. 185–195, Jan. 2016.
[19] B. Andrey, K. Miroslav, L. Gregor, T. Deniz, V. Kerem, and V. Ingrid, ''SPONGENT: The design space of lightweight cryptographic hashing,'' *IEEE Trans. Comput.*, vol. 62, no. 10, pp. 2041–2053, Oct. 2013.
[20] M. Sandhya and T. R. Rangaswamy, ''A practical approach for enhancing security in mobile RFID environment,'' in *Proc. Future Inf. Technol.–Int. Comput. Sci. Inf. Technol. (ICFIT)*, Singapore, 2011.
[21] Y. Wang and Y. Z. Li, ''An improved two-way security authentication protocol in mobile RFI and D,'' *Inf. Secur. Commun. Secur.*, no. 9, pp. 116–120, Sep. 2014.
[22] B. Zhang, X. X. Ma, and Z. G. Qin, ''Design and analysis of two-way authentication protocol for lightweight RFID,'' *J. Univ. Electron. Sci. Technol. China*, vol. 42, no. 3, pp. 106–111, May 2013.
[23] P. Liu, C. H. Zhang, and Q. Y. Ou, ''Design of security protocol for mobile radio frequency identification based on Hash function,'' *J. Comput. Appl.*, vol. 33, no. 5, pp. 1350–1352, May 2013.
[24] J. W. Shen and J. Ling, ''An improved ultra-lightweight RFID authentication protocol,'' *Comput. Appl. Softw.*, vol. 32, no. 2, pp. 304–306, Feb. 2015.
[25] Q. Huang and J. Ling, ''A two-way authentication protocol for ultra-lightweight mobile radio frequency identification,'' *Comput. Sci.*, vol. 44, no. 7, pp. 111–115, Jul. 2017.
[26] T. Suresh and M. Ramakrishnan, ''Mutual authentication protocol for RFID security using NFSR,'' in *Proc. IEEE Int. Conf. Commun. Softw. Netw.*, Jun. 2015, pp. 255–259.
[27] B. Niu, X. Zhu, H. Chi, and H. Li, ''Privacy and authentication protocol for mobile RFID systems,'' *Wireless Pers. Commun.*, vol. 77, no. 3, pp. 1713–1731, Aug. 2014.
[28] X. Fu and Y. Guo, ''A lightweight RFID mutual authentication protocol with ownership transfer,'' in *Advances in Wireless Sensor Networks*. Berlin, Germany: Springer, 2012, pp. 68–74.
[29] Y. Tao, X. Zhou, Y. P. Ma, and F. Zhao, ''Mobile bidirectional authentication protocol based on Hash function,'' *J. Comput. Appl.*, vol. 36, no. 3, pp. 657–660, Mar. 2016.
[30] G.-W. Wang, Z.-P. Jia, and W.-P. Peng, ''A mutual authentication protocol of mobile RFID based on dynamic shared-key,'' *Acta Electronica Sinica*, vol. 45, no. 3, pp. 612–618, Mar. 2017.

[31] C. Q. Shi, D. Wu, and R. Q. Xiao, ''Efficient RFID security authentication protocol that resists denial of service attacks,'' *Comput. Eng. Appl.*, vol. 52, no. 2, pp. 105–111, May 2014.
[32] S. Anandhi, R. Anitha, and V. Sureshkumar, ''An automatic RFID reader-to-reader delegation protocol for SCM in cloud computing environment,'' *J. Supercomput.*, vol. 74, no. 7, pp. 3148–3167, Jul. 2018.
[33] V. Sureshkumar, R. Amin, and R. Anitha, ''A robust mutual authentication scheme for session initiation protocol with key establishment,'' *Peer-to-Peer Netw. Appl.*, vol. 11, no. 5, pp. 900–916, Sep. 2018.
[34] L. Gong, R. Needham, and R. Yahalom, ''Reasoning about belief in cryptographic protocols,'' in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, Oakland, CA, USA, May 1990, pp. 234–248.
[35] Y. Zheng, ''Application of wireless connection based on hash function of RFID security authentication protocol,'' M.S. thesis, Jilin Univ., Changchun, China, 2015.
[36] Y. M. Guo, S.-D. Li, and Z.-H. Chen, ''A lightweight privacy-preserving grouping proof protocol for RFID systems,'' *Acta Electronica Sinica*, vol. 43, no. 2, pp. 289–292, Feb. 2015.

LIJUAN ZHENG was born in Baoding, China, in 1978. She received the B.S. and M.S. degrees in computer application from North China Electronic Power University, Baoding, in 2000 and 2003, respectively, and the Ph.D. degree in information security from the Beijing Jiaotong University, China, in 2014.

She is currently an Associate Professor with the School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang, China. She has published over 20 technical papers in international journals and conference proceedings. Her research interests include security protocol analysis and design, trusted computing, and privacy protection.

Dr. Zheng is a member of the China Computer Federation (CCF), the Supervision Committee Chairman of the CCF Shijiazhuang branch, and a Committee Member of the CCF Shijiazhuang branch.

CHUNLEI SONG received the B.S. degree in network engineering from Shijiazhuang Tiedao University, Shijiazhuang, in 2017, where she is currently pursuing the M.S. degree in computer science and technology.

Her research interests include information security and privacy preserving.

NING CAO received the bachelor's degree in software engineering from the Harbin Institute of Technology in 2004, and the Ph.D. degree in Computer Science from the University College Dublin in 2015.

He is currently an Academic Leader of computer science with the School of Information Engineering, Qingdao Binhai University, Qingdao, China. He has published over 30 technical papers in international journals and conference proceedings.

His research interests include security, IoT, and future communication technologies.

ZHAOXUAN LI was born in Changzhi, China, in 1997. He is currently pursuing the B.S. degree in network engineering with Shijiazhuang Tiedao University.

His research interests include privacy preserving and information security.

WENFENG ZHOU received the M.S. degree in computer technology from Shijiazhuang Tiedao University in 2009.

Her research interests include information security and network technology.

JIANYOU CHEN received the degree in computer science and technology from the Shijiazhang Institute of Railway in 2006. He is currently pursuing the degree in computer science and technology.

His research interests include information security and interacting between human and mechanism.

Mr. Chen is a member of the China Computer Federation.

LILI MENG received the B.E. degree from Shandong University, Jinan, China, and the Ph.D. degree from Beijing Jiaotong University, Beijing, China, in 2005 and 2013, respectively. From 2010 to 2011, she was a Visiting Student with Simon Fraser University, Canada. She is currently with the School of Information Science and Engineering, Shandong Normal University, Jinan.

Her research interests include image/video coding and 3-D videos.