An Efficient and Secure Authentication Protocol for Bus Rapid Transit Using the AES Algorithm

Shun Zhang
School of Electronics and Information
Nantong University
Nantong, China

Haijin Chen
Jiangsu Key Lab of ASIC Design
Nantong University
Nantong, China
E-mail：nt_chj@yahoo.com.cn

***Abstract*—Bus Rapid Transit (BRT) system as a new type public passenger transport system has been widely used, but it is lack of security mechanism and there is potential security hazard for the data transported between On Board Equipment (OBE) and Roadside Equipment (RSE). Radio Frequency Identification (RFID) technology brings user privacy and security concern because of wireless communication mode and no demand for line-of-sight. An efficient and secure authentication protocol is proposed based on the analysis of the security and privacy of RFID application in BRT system, which uses the Advanced Encryption Standard (AES) as cryptographic primitive. Compared with current typical protocols, this protocol efficiently prevents location tracking, spoofing, tampering, traffic analysis and replay attack, etc. Analysis result shows that this protocol is of high efficiency, low cost and good security.**

Keywords-Radio frequency identification (RFID),Security, Authentication, Bus Rapid Transit (BRT), Advanced Encryption Standard (AES)

I. INTRODUCTION

Along with the development of urban economy, the urban transportation problem is growing increasingly serious. The basic way of solving the urban transportation problem is to devote major efforts to develop public transit. The rail transit has the merits of big capacity and fast running speed, since it depends on high cost and long construction cycle, which has limited the widespread application in the big cities of our country. The conventional bus transit has suffered hindrance in the development because of low speed and inferior service. Bus Rapid Transit (BRT) system is a new type public passenger transport system, which combines the benefits of rail transit with the flexibility and efficiency of conventional bus transit. Its appearance brings the turning point for solving the transportation problem in the big cities of our country [1]. However, owing to lack of security mechanism, BRT system is unable to guarantee the secure wireless communication between On Board Equipment (OBE) and Roadside Equipment (RSE) by using Radio Frequency Identification (RFID) technology.

RFID is an emerging contactless technology using radio frequency to identify objects automatically, which is increasingly being deployed in diverse applications ranging from inventory management to anti-counterfeiting protection. RFID systems consist of Radio Frequency (RF) tags, or transponders, and RF tag readers, or transceivers. The object is equipped with a small circuit, called RF tag, and the information stored on the medium can be automatically retrieved by a reader device. This property can be used for wireless communication between vehicle and road in BRT systems. OBE and RSE communicate by RF signals, which makes a BRT system vulnerable to various attacks such as eavesdropping, spoofing, tampering, traffic analysis, and so on. These attacks may disclose sensitive information of OBE and hence infringe on privacy of vehicle. Therefore, it is of utmost importance to construct an efficient and secure authentication scheme in consideration of these potential attacks in BRT systems.

The security measures range from simple password protection and destroying the RF tag at the point of sales to extensive use of cryptographic algorithms. Most researcher propose the use of one-way hash functions as cryptographic primitives for security protocols [2], [3]. Only a few proposals have been published which employ block ciphers like the Advanced Encryption Standard (AES) [4]. In this paper, we introduce an efficient and secure mutual authentication protocol for BRT systems using srong cryptography. The AES is used as cryptographic primitive, because it is standardized and considered to be secure. Implementing a cryptographic unit for OBE is challenging due to the stringent requirements concerning the three parameters of die size, clock cycles and power consumption. M. Feldhofer and J. Wolkerstorfer[5] analyze and conclude that the AES-128 is the best choice in comparison to the standardized cryptographic algorithms SHA-256, SHA-1, MD5, and ECC-192 regarding the introduced metric.

The remainder of this paper is organized as follows. Section 2 reviews related works on RFID security and analyzes the protential privacy risks of current typical authentication protocols. Section 3 describes our proposed protocol followed by security analysis in Section 4. Finally, Section 5 provides a summary of our results.

II. RELATED WORKS

Several papers have examined the protection of user privacy. We describe some of the related studies below.

Hash lock scheme (HLK), by MIT [2]. This scheme prevents an exposure of tag ID by using cryptographic hash functions. Upon receiving a query from a reader, a tag first sends the hashed value of its key as a challenge to authenticate the reader. The tag reveals its ID only when the

reader sends a pre-image (key) of the hashed value as a response. However, since metaID is fixed, the adversary can track the tag via metaID. Moreover, the random key and ID of the protocol are transported in plaintext, the system is vulnerable to spoofing and replay attack.

Randomized hash lock scheme (RHLK), by MIT [2]. This is an extension of the hash lock type scheme. Each tag randomizes responses to a reader instead of a fixed tag response in order to protect location privacy. However, once IDk is eavesdropped, the attacker can impersonate the tag to a legitimate reader. Furthermore, this scheme is not scalable since the reader's computational workload is linear in the number of possible tags stored at the back-end database, which make the system susceptible to denial of service attack.

Hash lock chain scheme (HLKC), by NTT lab [3]. Initially tag has initial information s1. In the i-th transaction with the reader, the RF tag sends ai = G(si) to the reader, renews secret si+1 = H(si) as determined from previous si, where H and G are one-way hash functions. With tag-to-reader unilateral authentication, the protocol can not prevent the system from spoofing and replay attack.

Strong authentication for RFID systems using the AES algorithm, by project ART [4]. The ART project team selected AES-128 as a cryptographic primitive for symmetric authentication. The paper uses unilateral authentication, which works as follows: there are two partners A and B. Both possess the same private key K. B sends a random number rB to A. A encrypts the random number with the shared key K and sends it back to B. B proofs the result and can verify the identity (in other words the possession of K) of A. In this case, tracking and traffic analysis attacks are possible. The attacker sends the same number r to a tag. Then the tag replies with the fixed encrypted value of r to the attacker. Location privacy of the tag may be exposured. In addition, it is likely for the attacker to obtain the shared k value by analyzing many combinations of r and Ek(r). Therefore, the attacker can impersonate a legitimate reader to the tag or a legitimate tag to the reader.

Mutual three-pass authentication protocol (MTAP), by ISO/IEC 9798-2 standard [6]. Mutual authentication between reader and RF tags is based upon the principle of three-pass mutual authentication in accordance with ISO 9798-2, in which both participants in the communication check the other party's secret cryptological key. Each tag has a unique cryptological key via the key diversification scheme that is based on the tag's serial number and a master key, which is stored on the security access module (SAM) in the reader. This way of authentication enhances the security mechanism between reader and tags with the use of a master key but do not deter adversary from tampering attack.

Electronic toll collection (ETC) equipment application security, by Ministry of transport [7]. The payment transaction is secured by a two way authentication process, which consists of access credentials and message authentication. In order to Get/Set any application date from/to the OBE, the RSE must present a valid accessCredentials to the OBE. Before the application data are accepted by the RSE, the OBE has to present a valid authenticator to the RSE. the calculation of those signatures (accessCredentials and authenticator) is based on Triple Data Encryption Standard (TDES) algorithm. Keys are derived using TDES algorithm in order to increase the protection of the master key. However, AES outperforms DES and TDES in fulfilling the stricter data security requirement because of its enhanced security levels. In addition, known plaintext attack may exposure the AccessKey even the MasterAccessKey,then the attacker can duplicate a fake tag to spoof a legitimate reader.

III. PROPOSED MUTUAL AUTHENTICATION PROTOCOL

A. Notations

Tab.1 provides the notations used in the description of our proposed protocol.

B. Initialization Setup

The data fields of a RSE are initialized to M and KM. An OBE stores IDi, Mi and Ki. In addition, RSE and OBE equipped with a PRNG can perform eXclusive-OR (XOR) and the AES-128 encryption/decryption operation.

C. Authentication Process

When an OBE enters the operating range of a RSE, the RSE starts a protocol for mutual authentication. The detailed procedures are shown in Fig.1.

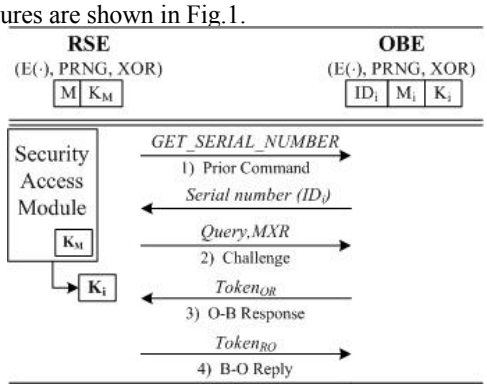

Figure 1. Proposed authentication scheme

1) Step 1(Prior Command): The mutual authentication begins by the RSE requesting the serial number IDi of the OBE. When the RSE receives the IDi, the SAM in the RSE computes the OBE's specific key Ki=E(IDi) using the master access key KM and AES-128 algorithm, then the derived mask bit Mi=E(M) is calculated using the master mask bit M and derived cryptological key Ki, so that these can be used to initiate the authentication procedure.

2) Step 2(Challenge): The RSE generates a random number R1, then the value of MXR is calculated using Mi and R1 through XOR operation, hence the RSE sends Query and MXR to an accessing OBE. When queried, the OBE generates the new symmetric key Ki' by XOR operation using R1, which is extracted from MXR, then another random number R2 is generated in the OBE and this is used to calculate TokenOR=E(R1||R2) with the secret key Ki'. TokenOR is sent to the RSE as a response frame.

3) Step 3(OBE authentication): When the received TokenOR is decrypted in the RSE, where a symmetric key Ki'=Ki ⊕ R1 is calculated, the random number R1' contained in the plain text is compared to the previously generated R1. If the two figures correspond, another new symmetric key Ki" is calculated using Ki' and R2 through XOR operation, then the RSE computes TokenRO=E(R1 ⊕ R2) using the secret key Ki" and forwards TokenRO to the OBE as a reply frame.

4) Step 4(RSE authentication): The OBE decrypts the received TokenRO and checks whether R2, which is generated previously, corresponds with R2'. If the two figures correspond, RSE and OBE have thus ascertained that they belong to the same system and futher communication between the two parties is legitimate.

IV. Security Analysis

In this section, we briefly give a security analysis of the proposed scheme. We claim that our scheme achieves the following security properties. We denote the adversary as μ, and a legitimate RSE and OBE as Ri and Oj respectively. A fake OBE j impersonating the real OBE j is depicted as Oj'.

Location tracking: Under this attack, by repeatedly querying with a value that yields a consistent reply, μ will be able to track the movements of Oj. Under our scheme, μ can reuse the same MXR for every query, but cannot predict the random R2 generated each time by Oj. In the protocol, we return the entire TokenOR with the dynamically changed symmetric key. Since R2 is a random number chosen by the OBE for each query, μ learns nothing from the repeated queries.

Replay attack: Replay attack is the attack that the adversary μ spoofs as legitimate OBE. First μ eavesdrops and obtains the responses from OBE, then μ can spoof the legitimate OBE by transmitting the obtained responses to the legitimate RSE. In our scheme, μ may replay the response TokenOR from an OBE. However, the RSE will find the invalidity of the replay value, because the random numbers R1 and R2 are different and independent in each session.

Spoofing attack: Under this attack, the adversary μ usually first queries Oj and obtains a response. When a legitimate RSE queries, μ attempts to pass off his counterfeits as legitimate. μ succeeds if Ri believes that Oj' is Oj. Under our protocol, μ transmits the obtained response to fool a RSE, but the RSE generates a new random number R1' and the symmetric key changes with R1', thus TokenOR ≠ Token'OR. Therefore, it is impossible for μ to make the correct response.

Eavesdropping: Here μ is able to observe all interactions between Ri and Oj. In others words, μ learns MXR, TokenOR, TokenRO. In this case, random number R1 delivers to the OBE through the mask operation, then the data block R1||R2 and R1 ⊕ R2 are transmitted using AES-128 algorithm with the dynamical key, the value of the response changes all the time, which means that eavesdropping is completely worthless.

Tampering attack: Under this attack, the adversary μ partially or completely tampers the content of information transmitted between RSE and OBE. In our scheme, μ is unable to convert primitive information into another legitimate one without access key. Any modification on the values TokenOR and TokenRO will cause authentication failure but not authentication error.

Traffic analysis: Under this attack, the adversary μ repeatedly queries OBE and receives data. By intercepting and analysing the responses from OBE, μ can extract the sensitive information. In our protocol, it is impossible for μ to obtain the derived key Ki value through analyzing many combinations of TokenOR and TokenRO, because the symmetric key changes along with R1 and R2 updating.

Security comparisons with the previous schemes are summarized in Tab.2.

V. Summaries

In this paper, we proposed a mutual authentication protocol for Bus Rapid Transit using the symmetric AES-128 algorithm as cryptographic primitive. Our protocol achieves desirable security features of a RFID system and efficiently withstands all the possible attacks that break the security of the previous schemes. A major departure from the previous research is that our scheme does not require back-end database support and dynamically changes the symmetric key. These excellent features make it very attractive to BRT system.

Acknowledgment

This work was financially supported by the research project of Ministry of Transport (2009-353-332-290) and Nantong municipal research project of science and technology (K2010050).

References

[1] Cai Zhi-Li. Bus Rapid Transit System and It's Pivotal Technologies[J]. Journal of Shandong Jiaotong University, 2008, PP:39-43.

[2] Weis S A. Security and Privacy in Radio-Frequency Identification Devices[D]. The Department of Electrical Engineering and Computer Science of MIT, 2003.

[3] M. Ohkubo, K. Suzuki, and S. Kinoshita. Cryptographic Approach to "Privacy-Friendly" Tags[C]. RFID Privacy Workshop, USA MIT MA, 2003.

[4] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems Using the AES Algorithm[C]. Workshop on Cryptographic Hardware and Embedded Systems (CHES), Springer, August 2004, PP:357–370.

[5] M. Feldhofer and J. Wolkerstorfer. Strong Crypto for RFID Tags-A Comparison of Low-Power Hardware Implementations[C]. IEEE International Symposium on Circuits and Systems (ISCAS), May 2007, PP:1839–1842.

[6] K. Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification[M]. Second Edition. New York: John Wiley & Sons Ltd, 2003, PP:220-224.

[7] Ministry of Transport. GB/T20851.4-2007. Electronic Toll Collection Dedicated Short-Range Communication Part 4: Equipment Application[S]. Beijing, Standards Press of China, 2007.

TABLE I. NOTATIONS

Notation	Representation
E(·)	symmetric cryptography (AES-128)
PRNG	pseudo-random number generator
KM	master access key
Ki	derived cryptological key
M	master mask bit
Mi	derived mask bit
IDi	the serial number of the OBE
MXR	converted mask bit
Ki', Ki''	dynamical symmetric key
R1	a pseudo-random number generated in the RSE
R2	a pseudo-random number generated in the OBE
‖	concatenation
⊕	eXclusive-OR

TABLE II. COMPARISONS OF THE SECURITY (○: SECURE, ×: INSECURE)

Protocol	HLK	RHLK	HLKC	ART	MTAP	ETC	Proposed
Location tracking	×	○	○	×	○	×	○
Replay attack	×	×	×	○	○	○	○
Spoofing attack	×	×	×	○	○	○	○
Eavesdropping	×	×	○	○	○	○	○
Tampering attack	×	×	×	○	×	○	○
Traffic analysis	×	×	○	×	○	×	○
Dynamic key	No	No	No	No	No	No	Yes
Mutual authentication	No	No	No	No	Yes	Yes	Yes