A safe radio frequency identification system (RFID) authentication protocol for Internet of Things

Zhiguo Du*, Bin Wen1, Zhihui Wu1, Ruijia Su1, Wenzi Liu2

1College of Informatics, South China Agricultural University, Guangzhou 510642, China
2College of Veterinary Medicine, South China Agricultural University, Guangzhou 510642, China

*Corresponding author: zhiguod@163.com

Abstract. Internet of Things (IoT) is the evolution of related technologies and applications such as Internet and mobile networks. Agriculture, as the source of food, is one of the key areas for the application of the IoT technology, and it is also the field with the most urgent, difficult and integrated characteristics of the IoT application. Future research into IoT will focus on generic technology, information security, and critical applications. Based on IoT, the existing Radio frequency identification system (RFID) security mechanisms are analyzed, with a focus on cryptographic protocols. Investigate the weaknesses or flaws in these protocols, and then a theoretical model and method to design and analyze RFID protocols within the provable security framework is discussed. A mutual authentication protocol of RFID system using synchronized secret information is put forward.

1. Introduction

The Internet of Things (IoT), an emerging global Internet-based technical architecture, has broad application prospects in agricultural refinement management, agricultural resource and environmental monitoring, agricultural product traceability, food supply chain and many other aspects. It can facilitate the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture’s resilience to attacks, data authentication, access control and client privacy need to be established. This aims to provide an interconnected infrastructure supporting new and innovative services based on widespread access to contextual information about objects in the physical world. One of the main requirements for the ‘Internet of Things’ is that objects must have a unique identity, which would make them practically addressable when exchanging information. Radio frequency identification system (RFID) tokens, such as Electronic Product Codes (EPC) tokens, have sufficiently long identifiers to allow for unique identities to be assigned to individual items, rather than to groups of items as is currently done with barcodes. RFID tokens are also easy to integrate into many objects as they do not need to be visible or adhere to a specific form factor.

The IoT has the purpose of providing an IT-infrastructure facilitating the exchanges of “things” in a secure and reliable manner. RFID tags may either be disabled by putting them in a protective mesh of foil known as a “Faraday Cage” which is impenetrable by radio signals of certain frequencies or by “killing” them, removing and destroying them. However, both options have certain disadvantages.
While putting tags in a special cage is relatively safe, it requires that every tag from every single product is put in that cage if a customer desires so. Chances are that certain tags will be overlooked and left with the client and that he/she could still be traced. Sending a ‘kill’ command to a tag leaves room to the possibility of reactivation or that some identifying information could be left on the tag. Furthermore, businesses may be inclined to offer clients incentives for not destroying tags or secretly give them tags. Instead of killing tags, the dissolution of the connection between the tag and the identifiable object could be envisaged. The information on ONS is deleted to protect the privacy of the owner of the tagged object. While the tag can still be read, further information with potential information concerning the respective person, however, are not retrievable.

In this paper based on IoT, the existing RFID system security mechanisms are analyzed, with a focus on cryptographic protocols. Investigate the weaknesses or flaws in these protocols, and then a theoretical model and method to design and analyze RFID protocols within the provable security framework is discussed.

2. RFID protocol overview

RFID system and RFID authentication protocol are based on certain assumptions, one of the most critical is to assume that the background server B (Back-end server) R (Reader) and reader communication between always safe. Because the B and communication between the R, RS422, often through RS232 RS485, or USB mode, so the communication security is relatively easy to achieve, such as using AES encryption algorithm and MD5 algorithm is used to compress [1], on B and R communication safety between concrete realization in [2] is described in detail.

Today's popular RFID technology, there are some hardware based user privacy protection methods, such as "Kill" command, feature[3] blocker-tag[4] and Faraday case [5]. Kill command feature by Auto-ID center is presented, in this method, each transponder T (Tag) have a password. If the R sending "Kill" command to the T, the T will permanently cannot be used in the system. Kill command feature perfect solution to all security problems, but T cannot be reused. In one system, if the T entered the unsafe zone, then T must be destroyed by kill command; but when T back to a safe area when, T also become available. When the system is performing the operation of the [6] tree-walking simulation, Blocker-tag blocking all T, but also prevents the illegal user from T to collect information. Faraday case method through "close T" operation to prevent T to accept the new query, this method applies only to a few to be able to use Faraday case method to close the application system [7].

Some people proposed the use of generic heavy encryption (Universal re-encryption) security model. Through the general heavy encryption technology encryption to encrypt information m, does not require public key cryptosystem related knowledge, because m is already encrypted the information [8]. Golle et al [4] protocol provides a general heavy encryption technology, and its application to RFID system. Saito et al. proposed an attack mode according to Golle’ protocol, and based on this puts forward two kinds of improved Golle protocol [9], and based on this puts forward two kinds of improved Golle protocol. The first protocol of Golle protocol is improved by modifying T operation; second protocol and Golle protocol is different from general heavy encryption techniques are applied to T instead of R. All based on general heavy encryption modes are vulnerable to eavesdropping; because of a heavy encrypted daa is the next authentication session output, so an eavesdropper can turn every session links, so as to achieve the purpose of tracking T. Some safe mode using the Hush approach to identifying T, such as in Weis et al in the agreement, when the R needs to query the T ID, T sends a random r and h (ID || r). This agreement is a safety issue, is when A successfully bribed a T, the ID, K information, and recorded the number of a R and some T certification process (there is more than one T), A can be in the tapping of the certification process to distinguish which is which T bribe the participation, and A realization of T prior to engagement with the certification of tracking [1]. Ohkubo proposed a can prevent T were tracked and completely independent of protocol [1]. In the Ohkubo protocol, the T response is sent, in which G and H are different Hash function, and was the first T initial values. In this protocol, in order to find a G (H^k(S^1)), must find every T hash chain, so this protocol efficiency is very low, it is not suitable to be applied to relatively small RFID system.
3. A RFID authentication protocol for IoT

3.1. Introduce
This paper explores the RFID system hypothesis responder $T$ (Tag) has a one-way hash function $h()$, a pseudo random number generator and an exclusive-OR gate XOR PRNG, and having in a interaction to maintain its state ability. The most widespread application of RF card is passive tag. (i.e., it does not have the battery, energy from the reader through radio wave transmission.)The proposed RFID system using passive tag, and it has little storage capacity and can copy function.

In the RFID system, $R$ had to do the calculation work is just a random number $s$, is the $s$ ensures that the $T$ is not affected by repeated attacks. Fig. 1 shows the RFID system architecture.

![RFID System Architecture](image)

**Figure 1.** The RFID system architecture of this paper

3.2. Safety needs
In order to solve the security problem and privacy protection of $T$, this paper defines the safety requirements, namely the RFID authentication protocol to achieve the safety index.

1. $T$ real information confidentiality: in order to protect the privacy of users, information about $T$ must be well protected. Even if the $T$ information is an unauthorized $R$ steal, then $A$ obtained should also be no true sense information.

2. $T$ response may not be $A$ identification properties: for each authentication, $T$ response information should be distinguished with other $T$, because $R$ and $B$ must identify all of the different $T$. But should $A$ cannot distinguish the $T$ collection of different $T$.If the $A$ in the $T$ collection to a $T$ every time response with other $T$ responses to distinguish, so this $T$ becomes can be tracked.

3. The forward security: the concept is defined, if $A$ had by some means (such as bribe) obtained the information on the $T$, but $A$ could pass this information to get the $T$ previously involved in certification activities information.

4. $T$ antisense clones: unless the $A$ successfully bribed $T$ users get the information of $T$, or $A$ cannot clone $T$, disguised as a $T$ to $R$ interaction.

5. $T$ availability: when a user needs, $T$ must always be available, even $T$ and $D$ occasionally not synchronization. Therefore, authentication protocol must provide a mechanism for handling repair.
certification occurs in the synchronization, especially when produce the occasional message send failure cause is not synchronous, such as server denial of service, message transfer fails, B or R power supply interruption. Especially when the A through the R and T is arranged between the metal barriers caused by R send updates to T failed, this time T and D is generated out of sync, then the next time the certification must repair the synchronization, or at least to ensure T available (can be accepted).

3.3. Protocol design
RFID system security problem mainly from communicating through a radio wave interaction between R and T. A may attempt to revise the T authentication information so that B and T authentication information between synchronization; A also may be on a certain T tracking; A even masquerading as a valid T or R. All of these are the authentication protocol which mainly solves the safety problem. After the introduction of authentication protocol, this paper assumes that the B and communication between the R is safe. As mentioned before, the security channel implementation please reference [2]. In each authentication process, first by R to generate a random number and sends the information to T. This random number will be integrated into the authentication message to avoid T by repeated attacks.

In this paper the authentication protocol, T will not have any real product, the user information (such as product model, user ID number), all authenticated communication messages are random and Hash two way. In order to prevent the synchronization problem caused the loss of data, this paper chooses with a similar to the database structure and similar synchronization mechanism [4]. In order to prevent from B send T message for some reason lost which generate a D and T information is synchronized, such as T has left the R identification range, or R and T between the metal barriers, caused by the B send T message loss, [4] has taken on each T in the D recorded in the two recording method, i.e. a is the current authentication information, the other is a first authentication information. When the D has updated the authentication information, and B send a message to T failure T authentication information is not updated, then in the next authentication, D will retrieve the last authentication information and T authentication information matching, then D does not update request send T updates to B, if the T receives the update request to update its authentication information, then the next time when authentication, D will update its authentication information; if T is missing the B sent to the update request, then the next time when authentication, D still will be retrieved to the first authentication information matching with T, and D still not be updated. So the principle of synchronization and the same, only in the database structure design is based on a T two copies of the record method; but take on a T keep a record, but two certification field method, wherein a field recording is the secondary authentication information, another field is used to record the latest certification information [10].

3.4. The communication protocol overview
B and T have XOR calculation ability, and have a Hash function, and the Hash function is not in the time from the output value to calculate the input value. R has a pseudo-random function PRNG and a bit length of the variable. Function is used to detect repeated attack. T also has a pseudo-random function PRNG, the PRNG can be associated with different R. In each authentication, T will have a temporary variable, is there to make the B and T certification testing information is wrong, only the authentication information correctly updated certification information. Because it is a temporary, so it will be removed in the certification.

4. A safe RFID authentication protocol for IoT
4.1. Introduce
The Internet of Things (IoT) will present new security challenges in cryptographic security, credentialing, and identity management. Currently available cryptographic techniques require further analysis to determine applicability in the Internet of Things. Credentialing presents significant challenges in the current Internet and these challenges will be exacerbated by the sheer number of devices and the expected limitations in user interfaces. Identity management is currently oriented
towards either user or device identity; in the Internet of Things making an implicit or explicit mapping between IoT device identities and Internet user identities may be required. Network security devices, such as firewalls and network guards, will be essential to meet security requirements. Security will be in tension with usability, privacy, and devices’ constrained resources.

4.2. The protocol details
The protocol details are listed as follows:

1. R used PRNG to generate a random number s temporary, R saves s and sends s to T.
2. T generates a random number r1, and obtained by h (r1 + k + s) calculating to received r2 (s is sent by R over), and then sent r1, r2 to the R, and T temporary s, r1, r2.
3. R sends s and r1, r2 to B. R can delete the temporary variable s.
4. In order to find the associated T’s real product or the user ID (fixed), the domain B in D lookup, which satisfies the following properties:

\[ h(r_1 \oplus k \oplus s) \oplus r_2 = \] (1)

Which sent over by R. Found only a k’ satisfies the equation (1) in D, then the IDF domain corresponding to that record that T is associated with a product or user’s ID; if it find k’ more than one, then the hash collision (despite the probability of occurrence of such a situation m/2^l only), then B should report the case of failure to find the ID of the T to R and R resend s to T, thus it has to start again certification process. (ie, go back to step one.)

5. B updates the information of B. If k’ is found in the domain of K, then the value of k’ is copied to the K_{last’} domain of the rows, and the K of the rows field is updated to h (k’). If checked to find k’ in the K_{last’} domain, then do not need to update D, because of D is updated in the last certification, but T is the update fails.

6. B calculated Equation \( h(r_2 \oplus k \oplus s) \) to receive r3’, and sent r3’ to the R, and then R will be sent r3’ to T directly.

7. T received r3’, and used itself stored variable s, k, and r2 to calculated equation \( r_3 = h(r_2 \oplus k \oplus s) \). Then to determine:

\[ r_3 \oplus r_3' \] (2)

If (2) is true, then T updated k, h(k).

This article assumes that T does not have the ability to complete all the steps of a certification matter of principle, the interaction of the R and T and A can be interrupted at any moment in time certified. Based on this assumption, the agreement becomes unavailable. For example, the greement each time you send the data is necessary to update the content. A can send data at T in immediately cut off the energy provided by the R to T (T is passive tags, energy rely on the R radio transmission), such that T can not update their own content. A through T after each query interrupt source of energy, so the data sent each time T are the same, and thus become can be tracked. The proposed authentication protocol to send the first data is randomly generated, so this attack for the system impracticable (Fig. 2).

IoT protocols do not rely on pre-shared keys. Credentialing/registration of devices will also be a challenge, but pairing protocols are well-understood and provide one possible solution set. Privacy concerns may provide incentives for adoption for technologies designed to prevent information leakage in military/intelligence environments. Privacy issues are also expected to be significant. Our experiences with Smart Grid demonstrate the sensitivities of exposing electricity usage associated with a home or business. The IoT has the potential to expose the precise application of that energy demand, further violating the privacy expectations of the population. In combination with these privacy issues, compromises in the IoT protocol suites are likely to require establishing a security perimeter that monitors and restricts IoT devices.
5. Conclusion
Internet of Things (IoT) is the evolution of related technologies and applications such as Internet and mobile networks. Future research into IoT will focus on generic technology, information security, and critical applications. Based on IoT, the existing RFID system security mechanisms are analyzed, with a focus on cryptographic protocols. Investigate the weaknesses or flaws in these protocols, and then a theoretical model and method to design and analyze RFID protocols within the provable security framework is discussed. A mutual authentication protocol of RFID system using synchronized secret information is put forward. Currently available cryptographic techniques require further analysis to determine applicability in the Internet of Things.

Acknowledgements
This work is supported by the Science and Technology Major Project of Guangdong Province of China (Grant No.2014B02050004 and No.2016B010110005).

References
[1] Rieback M R, Crispo B and Tanenbaum A S 2006 IEEE Pervasive Computing 5 62
[2] Barreto P, Kim H, Lynn B and Scott M 2002 Advances in Cryptology — CRYPTO 2002 2442 354
[3] Tana Y and Sata M 2010, IEEE Communications Letters 14 101
[4] Juels A 2006 *IEEE Journal on Selected Areas in Communications* **24** 381
[5] Fabian B 2008 *Secure Name Services for the Internet of Things* (PhD Thesis, Humboldt-Universität zu Berlin).
[6] Yan L, Zhang Y, Yang L T and Ning H S 2008 *The Internet of Things: from RFID to the next-generation pervasive networked systems* (London: Auerbach Publications)
[7] Osaka K, Takagi T, Yamazaki K and Takahashi O 2006 *Conference on Computational Intelligence and Security* **4456** 1090
[8] Mulliner C 2009 *Proceedings of the 1st International Workshop on Sensor Security (IWSS) at ARES (Fukuoka)* pp. 695–700
[9] Rotter P 2008 *IEEE Pervasive Computing Magazine* **7** 70
[10] Mitrokotsa A, Rieback M R and Tanenbaum A S 2009 *Information Systems Frontiers* **12** 491