Indian Journal of Science and Technology, *Vol 7(3S), 47–51, March 2014*
ISSN (Print): 0974-6846
ISSN (Online) : 0974-5645

Real Time Authentication System for RFID Applications

Swati Kumari*

Astt. Professor, Department of Electronics & Communication, Bharath University, Chennai, India; swati.ks1987@gmail.com

Abstract

Currently, the RFID (Radio\Frequency Identification) applications, such as banking (card payment), toll cards, access cards and package delivery do not use location information for authentication. These applications depend only on the information available in the RFID card to authenticate. This results in various security issues, such as unauthorized reading and relay attacks on RFID systems.

Using the location information, a new level of security layer can be introduced into the authentication mechanism. The location information can be used by a back end server, such as a bank server to analysee the current location and compare it with predefined authorized locations for that particular card. In case of positive match, authorization is granted to the payment gateway to proceed with the transaction. This approach protects the tag owners from unauthorized transactions or misusage of RFID card. The location information can also be used by payment gateway to authenticate the card payment machines to be legal and in the registered premises. In case the machine is not in the registered premises, then the machine can be blocked. This makes the machine steal proof, as the machine would be useless in any other location.

Keywords: Access Card, GPS, Location Based Authentication, RFID

1. Introduction

Low cost, small size and the ability of allowing computerized identification of objects make Radio\Frequency IDentification (RFID) systems increasingly ubiquitous in both public and private domains. Prominent RFID applications include supply chain management (inventory control), e-passports, credit cards, driver's licenses, vehicle systems (toll collection or car key), access cards (building, parking or public transport), and medical implants. In these applications, the secure information, such as card number, owner credentials, are stored in the card. Using a RFID reader, this information can be retrieved and analysed. Thus, breach in security can be used to generate a duplicate tag, and then unauthorized transactions can be carried on. Existing card authentication mechanism can also introduce different types of relay attacks, such as 'Ghost-and-Leech' attack.

Existing mechanisms are available, such as encrypting the tag data and decrypting the data in the reader. But this approach is costly and cannot be globally applied, as the same manufacturer might not produce the reader and tag. Location based authentication is a very new approach on RFID authentication, and various parameters are available for secure authentication. Di et al's work reports that[1], GPS system is used on both reader and tag side. This is a costly solution. Moreover, the payment gateway server does not do authentication of card payment machine.

*Author for correspondence

2. Security

We classify security threats to RFID protocols into weak and strong attacks.

2.1 Weak Attacks

These are attacks, which are feasible just by observing and manipulating communications between readers and tags.

- Tag Impersonation: An eavesdropper could impersonate a target tag without knowing the tag's internal

secrets. It could communicate with readers instead of the tag and be authenticated as the tag.

- Replay attack: In such an attack, an attacker reuses communications from previous sessions to perform a successful authentication between a tag and a server.
- Denial of Service attack: An adversary disturbs the interactions between readers and tags by intercepting or blocking messages transmitted. Such an attack could cause a server and a tag to lose synchronization. For example, the server might update the shared data, while the tag does not; in such a case they would no longer be able to authenticate each other.

2.2 Strong Attacks

These are threats possible for an attacker, which has compromised a target tag. The memory of a low-cost tag is not tamper-resistant, and hence the tag's internal data are liable to be exposed by physical attacks. Thus, addressing such attacks is essential for the security of RFID schemes.

- Backward Trace Ability: This occurs if, given all the internal state of a target tag at time t, the attacker is able to identify target tag interactions that occurred at a time $t' < t$ [2]. That is, knowledge of a tag's current internal state could help identify the tag's past interactions, and the past transcripts of a tag may allow tracking of the tag owner's past behaviour[2]. In some previous papers, backward untraceability is referred to as forward security[8]. Here, we use the terms backward trace ability and forward trace ability defined previously[2] to clearly distinguish between threats to past and future anonymity.
- Forward Trace Ability: This can similarly be defined as where knowledge of a tag's internal state at time t can help to identify tag interactions that occur at a time $t' > t$ [2]. The only way of maintaining future security, once the current tag secrets have been revealed is to detect key compromise as soon as possible, and to replace the exposed key to protect future transactions [15]. This issue is related to tag ownership transfer. This is because, if an RFID scheme does not provide forward untraceability, when the ownership of a tag is transferred, the previous owners might be able to read communications between the new owner and the tag.
- Server Impersonation: This means that an adversary with knowledge of the internal state of a tag is able to impersonate the valid server to the tag. This attack does not appear to have been discussed previously, despite its potential importance.

One reason that this is a genuine threat is because of the following attack. If it is possible to impersonate a server to a tag, an adversary could request a target tag to update its shared secrets. The tag and the real server would then be desynchronized, and incapable of successful communications.

3. Related Work

Hash-based Access Control (HAC), as defined by Weis et al.,[8] is a scheme, which involves locking a tag using a one-way hash function. A locked tag uses the hash of a random key as its metaID. When locked, a tag responds to all queries with its metaID. However, the scheme allows a tag to be tracked because the same metaID is used repeatedly[5]. Weis et al. also suggest another scheme, Randomized Access Control (RAC), which employs a random number generator to prevent the above tracking attack. In each session, a tag generates a new response as a hash function of the tag ID and a random number. However, tag impersonation remains possible because an intercepted response can be replayed. Moreover, it does not provide backward untraceability because the tag ID is fixed.

Ohkubo, Suzki, and Kinoshita (OSK)[9] propose an RFID privacy protection scheme providing indistinguishability (i.e. a tag output is indistinguishable from a truly random value and unlink able to the ID of the tag) and backward untraceability. This scheme uses a low-cost hash chain mechanism to update tag secret information to provide these two security properties. However, it is subject to replay attacks[5], and hence it permits an adversary to impersonate a tag without knowing the tag secrets.

Henrici and Müller[10] suggest a scheme relying on one-way hash functions to enhance location privacy. A tag sends two hashed values as its response to a query, and updates its stored values, including its ID, after a successful authentication. Despite this, the scheme still allows a degree of tag tracking, because a tag always replies with the same-hashed ID before the next successful authentication[5]. Also, a strong attacker could easily compute the identifiers used in previous sessions by combining the server's random number and the current identifier; that is, it does not provide backward untraceability.

Molnar and Wagner[9] propose a private authentication protocol for library RFID that uses a shared secret and a

pseudorandom number function to protect the messages communicated between tag and reader. This scheme cannot provide backward untraceability. Once a tag is compromised, the attacker can trace past communications from this tag[5], because a tag's identifier and secret key are static. They also build a new tree-based protocol to provide scalable private authentication, with reader work O (log N), O (log N) rounds of interaction, and O (log N) tag storage, where N denotes the number of tags, and the N tags are considered as leaves in a balanced binary tree[7]. However, this approach requires that each tag stores the Flog N secrets' corresponding to the path from the root to the tag, and privacy is weakened when an adversary is able to tamper with at least one tag[9]. Also, the more tags an adversary tampers with, the more privacy is exposed[9].

Dimitriou's Scheme (D)[6] is an RFID authentication protocol that enforces user privacy and protects against tag cloning. This scheme uses a challenge-response approach, where a tag uses a hash of its identifier as a response to a reader query to maintain scalability at the server, and the back-end server sends a message using the updated identifier to the tag after receiving the tag response, to authenticate the server to the tag. However, between valid sessions, the tag identifier remains the same, thereby making the scheme vulnerable to tracking and tag impersonation through reuse of the hashed tag identifier. Additionally, the scheme is prone to DoS attacks.

The identification scheme of Karthikeyan and Nesterenko[10] uses simple matrix multiplication, and does not require computationally expensive cryptographic mechanisms. Security is based on the difficulty of recovering the multiplicand or multiplier from the product of two matrices. An intruder could launch a DoS attack and could also attempt to mount a brute-force matrix or key guessing attack as discussed[3]. In addition, the scheme cannot resist replay and tracking attacks[5].

Duc et al. (DPLK) present a synchronisation-based communication protocol for the EPCGlobal Class 1 Gen-2 RFID tag. It uses a pseudo-random number Generator and a cyclic redundancy code. It cannot prevent replay attacks before the next successful authentication. Most seriously, a DoS attack could permanently desynchronise a server and a tag. It also does not provide backward untraceability if the fixed EPC code and the access key PIN are compromised[5].

A mutual authentication protocol for RFID, conforming to the EPC Class 1 Generation 2 standards was introduced by Chien and Chen[5]. A challenge-response protocol is used to prevent replay attacks. The server database maintains copies of both old and new tag keys to resist DoS attacks. Both the authentication key and the access key are updated after a successful session in order to give backward untraceability. However, the schemes still permits backward and forward trace ability, because a strong attacker that compromises a tag, can identify a tag's past interactions from the previous communications and the fixed EPC of the tag, and can also read the tag's future transactions. Moreover, an adversary can successfully masquerade as an authorised server to a tag, if it has the tag secrets.

Lim and Kwon (LK)[2] describe an RFID authentication scheme satisfying both forward and backward untraceability and enabling perfect ownership transfer. They define update as deterministic evolution (of stored secrets) and refresh as probabilistic evolution, where the refresh process is introduced to help provide forward untraceability. A tag and a server both refresh their secrets, using exchanged random numbers, if an authentication procedure completes successfully. If an authentication procedure fails, the tag updates its secrets (i.e. using a deterministic process). The protocol provides forward untraceability from the moment that an adversary misses just one successful authentication session after it has compromised the tag secret. It uses two hash key chains: a forward key chain for tag secret evolution, and a backward key chain, used in reverse order, for server validation. These techniques make the scheme partially secure against server impersonation. The database keeps old and new key chains for relevant secrets in order to solve the desynchronisation problem arising from DoS attacks. However, it does have potentially scalability issues, because the server needs to perform significant computations to update tag secrets, and a large database is required to manage two key chains for each tag.

In this paper, we propose a scheme that significantly reduces the necessary storage and computation in a tag by comparison with the DPLK, CC, and LK schemes, as well as preventing the attacks mentioned above.

4. Security and Efficiency Analysis

In this section, we provide the security analysis and the comparison of the efficiency between the proposed protocol and the previous protocols.

4.1 Security Analysis

1. Confidentiality: Every message in the authentication process is secure against the unauthorized eavesdropper. It does not contain the usable information because it is a result of the hash function. Therefore, our proposed protocol satisfies the confidentiality.
2. Anonymity: In the authentication process, it should not reveal any usable information about the tags. Our proposed protocol performed XOR operation with hashed tag's id. Thus, we satisfy the anonymity.
3. Location privacy: If the same reader requests to the same tags, the tag answers the same response. In that case, the tag will be able to track the movements or locations. We answer the different response, even if the same reader is querying the same tag. Therefore, we provide the location privacy.
4. Mutual authentication: We provide the tag-to-reader authentication using the message 2 and the reader-to-tag authentication using the message 3. Therefore, we provide the mutual authentication.
5. Availability: Whenever the authentication process should be able to authenticate,we can provide the authentication protocol for the RFID tags and the reader without back-end server. Therefore, we satisfy the availability.

We show the security against the available attacks in RFID system as following Table 2.

1. Eavesdropping: The adversary cannot get any useful information through the eavesdropping. Therefore, our proposed protocol is a secure against eavesdropping.
2. Replay attack: The tag generates the different response in every transaction, using the random number. If the same reader request to the same tag, it cannot use the previous message. Thus, the replay attack is impossible.
3. Cloning attack: The attacker cannot predict the random number generated by the reader. Moreover, he does not know the tag's secret that shares with CA. Therefore, the adversary cannot make the fake tag.
4. Type attack: The type attack is possible when the challenge-message and the response-message is similar and equal the length. Therefore, our proposed protocol is a secure against the type attack.
5. Tracking attack: Han et al.'s protocol did not provide the location privacy. Therefore, the attacker will be able to track the movement of the tag. In our protocol, we generate the different message for each query. Thus, tracking attack is impossible.

Table 1. Comparison of the requirements for the RFID system

Requirements	Tan et al.	Han et al.	Proposed protocol
Confidentiality	O	O	O
Anonymity	O	O	O
Location privacy	O	X	O
Mutual authentication	X	O	O
Availability	O	O	O

O: satisfied, X: not satisfied

Table 2. Security comparison between our proposed protocol and the previous schemes

Attacks	Tan et al.	Han et al.	Proposed protocol
Eavesdropping	O	O	O
Replay attack	O	O	O
Cloning attack	O	O	O
Type attack	O	O	O
Tracking attack	O	X	O
Man-in-the-middle attack	O	O	O

O: secure, X: insecure

6. Man-in-the-middle attack: Our proposed protocol is impossible to man-in-the-middle attack because the attacker does not know tag's secret. Therefore, he cannot generate the hash using the random number.

If the attacker obtains the authenticated reader, he cannot know each tag's secret because they only have the hashed value. Therefore, the attacker cannot impersonate the other tags.

4.2 Efficiency Analysis

Table 1 shows the efficiency of the proposed protocol comparing with the previous RFID authentication protocols.

We compared between our proposed protocol and the previous proposed protocols of the authentication protocols for the RFID tags and the reader without back-end server (Table 3). When the proposed protocol is compared with Han et al., it reduced the communication rounds and the computation. Moreover, we solved the problem of the location privacy. Also, when our protocol is compared with Tan et al., the proposed protocol provides mutual authentication that both tag-to-reader and reader-to-tag authentication. Therefore, our proposed protocol is a more secure and efficient.

5. Conclusion

In this paper, we have studied the previous RFID authentication protocols that do not require the back-end server.

Table 3. Efficiency comparison between our proposed protocol and the previous schemes

		Tan et al.	Han et al.	Proposed protocol
Reader	H	1	2	2
	X	1	1	–
	R	1	1	1
Tag	H	3	4	4
	X	1	1	–
	R	1	1	1
Rounds		4	6	3

H: the number of hash operation, X: the number of XOR operation; R: the number of random number generator

The previous protocols still have security problems, such as mutual authentication and location privacy. Therefore, we try to resolve it.

Our proposed protocol has reduced the computational complexity and communication rounds. Moreover, we solved the problem of the location privacy. Finally, we show that the proposed protocol is a more secure and efficient protocol than the previous ones.

6. References

1. Di M, Saxena N, Xiang T, Zhu Y. Location-aware and safer cards: enhancing rfid security and privacy via location sensing. IEEE Transactions on Dependable and Secure Computing. 2013 Mar–Apr; 10(2):57–59.
2. Juels A. RFID security and privacy: a research survey. IEEE J Selected Areas in Comm. 2006 Feb; 24(2):381–94.
3. Song B, Hwang JY, Shim K-A. Security improvement of an RFID security protocol of ISO/IEC WD 29167-6. IEEE Communications Letters; 2011 Dec; 15(2):1375–77.
4. Sun DZ, Zhong JD. A hash-based RFID security protocol for strong privacy protection. Consumer Electronics, IEEE Transactions on. 2012 Nov; 58(4): 1246–52.
5. Bashir AK, Chauhdary SH, Shah SC, Park MS. Mobile RFID and its design security issues. Potentials, IEEE. 2011 Jul–Aug; 30(4):34–38.
6. Rizomiliotis P, Rekleitis E, Gritzalis S. Security analysis of the song-mitchell authentication protocol for low-cost RFID tags. Communications Letters, IEEE. 2009 Apr; 13(4):274–76.
7. Sun HM, Ting WC. A Gen2-based RFID authentication protocol for security and privacy. IEEE Transactions on Mobile Computing. 2009 Aug; 8(8):1052–62.
8. Mirowski L, Hobart TAS, Hartnett J, Williams R. An RFID attacker behavior taxonomy. IEEE Pervasive Computing. 2009 Oct–Dec; 8(4):79–84.
9. Zuo Y. Survivability experiment and attack characterization for RFID. IEEE Transactions on Dependable and Secure Computing. 2012 Mar–Apr; 9(2):289–302.
10. Errington AFC, Saskatoon SK, Daku BLF, Prugger AF. Initial position estimation using RFID tags: a least-squares approach. Instrumentation and Measurement, IEEE Transactions on Instrumentation and Measurement. 2010 Nov; 59(11):2863–69.