Information Systems Frontiers
https://doi.org/10.1007/s10796-021-10177-x

On Group Ownership Delegate Protocol for RFID Systems

Yu-Ju Tu[1] · **Gaurav Kapoor**[2] · **Selwyn Piramuthu**[3]

Accepted: 17 July 2021

Abstract
As RFID tags identify objects at the item level, proper authentication of these tags is of paramount importance in RFID-based systems. While RFID tag authentication in systems where these tags are assigned to be read by a single reader is challenging enough due to resource constraints related to memory and processing power at the tag's side, it is not uncommon for RFID tags to be read by multiple readers. Even more, when an item moves between owners, ownership of the RFID tagged item needs to be updated to reflect reality. As authentication protocols play a critical role in RFID-based systems, it is necessary to ensure that any developed protocol is free from vulnerabilities that can be taken advantage by an adversary to mount attacks on the system. Lee et al. (*Information Systems Frontiers*, 21, 1153-1166, 2019) develop group ownership authentication protocols for a group of RFID-tagged items that simultaneously switch ownership. We evaluate the protocols in Lee et al. (*Information Systems Frontiers*, 21, 1153-1166, 2019) and identify several critical vulnerabilities. We then discuss the sources of these vulnerabilities and common precautions that should be taken to avoid such vulnerabilities.

Keywords RFID · group ownership transfer · authentication · vulnerabilities

1 Introduction

While RFID (Radio-Frequency IDentification) (Bose et al., 2011) tags have existed for more than eight decades, their widespread use began in the early 2000s with the introduction of mandates from the US Department of Defense, Wal-Mart, among others. Since then, the world has witnessed extensive adoption of RFID in a variety of disparate application areas. For example, RFID as an IoT (Internet of Things) device may create considerable innovative context for tracking and managing organizational or industrial assets. Reportedly, the US overall spending on logistics were around 8% of the country's GDP in 2018. Along with Industry 4.0, the US logistics market is expected to generate a value of 1.8 trillion USD over the next decade. Consequently, RFID-related solutions for tracking and managing assets are on a sharp rise and widespread across various industrial sectors that include automotive and electronics (https://www.globenewswire.com/news-release/2020/12/03/2138928/0/en/Worldwide-Asset-Tracking-Industry-to-2025-North-America-is-Expected-to-Hold-a-Strong-Market.html).

In contrast to another auto-ID technology, barcode, RFID tags identify objects at the item level, which has related security and privacy implications. This is clearly visible in issues related to authentication. RFID authentication is therefore a very active research area that helps foster the development of secure authentication protocols.

Among RFID authentication protocols, there are variations in terms of the number of tags and/or readers that are authenticated at any given point in time. For example, there are protocols that are used to authenticate multiple tags that simultaneously belong to a single reader as well as an RFID tag that is authenticated to communicate with a group of readers (e.g., Lee et al. 2019). There are also protocols to authenticate a group of RFID tags as they enter or leave their groups. A common denominator among these authentication protocols is that all these tags and readers belong to a given entity (e.g., a supplier, a retailer, a person).

In addition to authentication protocols for RFID tags that belong to the same entity, there are situations that necessitate movement of RFID tags across different ownership scenarios. For example, in the context of a

✉ Selwyn Piramuthu
selwyn@ufl.edu

[1] Management Information Systems, National Chengchi University, Taipei, Taiwan

[2] Infocomm Technology, Singapore Institute of Technology, Singapore, Singapore

[3] Information Systems and Operations Management, University of Florida, Gainesville, FL, USA

Published online: 24 July 2021

vehicle supply chain, each vehicle can be embedded with an RFID tag that stores its VIN (vehicle identification number), parking location, carrier status, and so forth. The associated RFID readers can then remotely retrieve or update the information. However, this does not signify that such RFID readers share the right to access (communicate with) the tag information at all times. Rather, during vehicle movement from one supply chain node (e.g., distribution hub) to another node (e.g., dealership), the ownership of the tags transfer between the nodes. Thus, only the readers at the latter node (i.e., dealership) own the right to access the tag information, while the readers at the former node (i.e., distribution hub) no longer possess that right (https://www.information-age.com/vehicle-distribution-supply-chain-123477690/).

In an ownership transfer scenario, an additional constraint is that while the new owner must be able to authenticate and communicate over-the-air with the RFID tag, the previous owner should not have such access as that constitutes ownership *sharing* and not ownership *transfer*. The difference between ownership transfer and ownership sharing is that in the former the previous owner loses the access privilege for that tag whereas in the latter the previous owner continues to have access privilege for that tag. There are authentication protocols that are specifically designed for ownership transfer scenarios (e.g., Kapoor & Piramuthu 2012). Recently, Lee et al. (2019) proposed a suite of authentication protocols for a group of RFID tags that simultaneously transfer ownership between two entities. Any authentication protocol that is proposed must be critically evaluated to ensure the absence of at least the readily identifiable vulnerabilities. To this end, we consider the protocols presented in Lee et al. (2019) and identify several significant vulnerabilities (Mitrokotsa et al., 2010). In the remainder of this paper, we first present the authentication protocols and then list the identified vulnerabilities. We then conclude the paper with a brief discussion on the characteristics of these vulnerabilities and what can be done to avoid such vulnerabilities in authentication protocols.

2 Vulnerabilities in Lee et al. (2019) Protocols

The protocol suite presented in Lee et al. (2019) consists of four main stages that include the following. (1) registration phase during which RFID tags, current mobile reader, and delegated mobile reader register with the cloud server, (2) mutual authentication and ownership delegation phase when a user wants to acquire delegated ownership of a group of RFID tags, (3) e-th time verification phase to restrict the number (u) of verification rounds, and (4) earlier delegation revocation phase to revoke delegation before u verification rounds are complete.

We first present the notation used in the rest of this paper.

$n_r, n_{r_1}, n_{r_2}, n_{r_3}, n'_r, gk$	nonce
TID_i	identity of tag i
$r_{i,j}$	secret key shared by tag i and reader j
n_j	product of two large primes p_j and q_j
$K^{del}_{TID_{i,j}}$	delegate key shared by tag i and reader j
t_c, t_d	current and delegated mobile reader timestamps
u	maximum allowed number of verification rounds
$M(.)$	homomorphic MAC function
$H(.)$	one-way hash function
ΔT	valid delegation time gap
$PRNG$	pseudo-random number generator
$\oplus$	exclusive-OR operator
$\|\|$	concatenation operation

In the following subsections, we provide only a sketch of the protocols before we identify some of the vulnerabilities in these protocols. The interested reader is referred to the original publication (Lee et al., 2019) for further details on these protocols. We do not discuss the first (registration) and the last (earlier delegation revocation) phases as these likely are operationalized in a secure environment with cloud server involvement although Lee et al. do not specifically mention this aspect. There are few other minor issues in the paper (Lee et al., 2019). For example, the tag begins communication with the cloud server in the tag registration phase (Section 3.1.1). This is possible only when it is an active tag, which is not discussed in the paper. Moreover, some notation elements are unclear. For example, the subscripts (j) for both RFID tag and mobile reader (R_j and Tag_j) range from 0 through n, signifying the same number of tags and readers, which is unrealistic in most RFID-based systems. The hash value of TID_i is represented by $H(TIDi)$, whereas the same is represented by $h(TID_i)$ (i.e., small h) in Step2 in Section 3.1.1 (Lee et al., 2019).

The vulnerabilities we identify include tracking and tracing, key disclosure, full disclosure, impersonation, relay attack, and desynchronization. We now briefly explain each of these terms in the context of authentication in RFID-based systems. Tracking refers to the entity's current location and tracing refers to its previous location history. Tracking and/or tracing ability allows the identification of an RFID-tagged entity across time so as to roughly map its traversed path or locations at which the entity was present. An adversary with the ability to track and/or trace an entity

has the potential to violate privacy and/or security of the entity (i.e., privacy violation).

Key disclosure occurs when a key that is meant to be a secret is disclosed to unintended parties. Full disclosure, on the other hand, refers to the disclosure of all the terms that are used in an authentication protocol. In other words, key or full disclosure will result in confidentiality violation.

Impersonation signifies the successful ability of an entity (say, E_1) to impersonate another entity (say, E_2). A goal of impersonation is that other entities that interact with E_1 are tricked into believing that they are indeed interacting with E_2. As a result, the accountability of involved entities will be violated.

Relay attack occurs when an entity simply relays messages between (at least) two other entities. The main goal of a relay attack is to decrease the perceived distance between two entities to accomplish something (e.g., open a car door when the car key is with the owner who is several blocks away from the car). Generally, this also suggests that one entity will be fooled to believe the presence of the other entity that is actually absent. Similar to impersonation attack, relay attack can cause severe accountability violation.

Desynchronization between two entities occurs, for example, when the two entities have different values for important attribute(s) (e.g., different shared key values) that prevents them from communicating with each other. The two entities are thus not available for each other (i.e., availability violation).

2.1 Part 1 of Mutual Authentication and Group Ownership Delegation

The mutual authentication and ownership delegation phase is split into three parts. A sketch of the first part of this phase is provided in Fig. 1. We now discuss the identified vulnerabilities in this protocol.

2.1.1 Vulnerabilities

Tracking and Tracing Message M_3 from tag to reader consists of R'_t and A where $R'_t = R_t^4 \ mod \ n_j$ and $A = r_{i,j} \oplus n_r$. Message M_4 from reader to tag consists of ACK_s and B, where $ACK = h(TID_i) \oplus n_r$ and $B = h(TID_i) \oplus n_r \oplus (t_c || K^{del}_{TID_{i,j}} || gk)$. An adversary passively listening to this conversation between reader and tag can capture these messages and perform $A \oplus ACK_s$, which is the same as $h(TID_i) \oplus r_{i,j}$. As this is a constant, the tag is readily tracked.

Key Disclosure Both $K^{del}_{TID_{i,j}}$ and $r_{i,j}$, respectively the delegate key shared between the tag Tag_i and the reader R_j and the secret key shared between the tag Tag_i and the reader R_j, can be easily determined by an adversary as

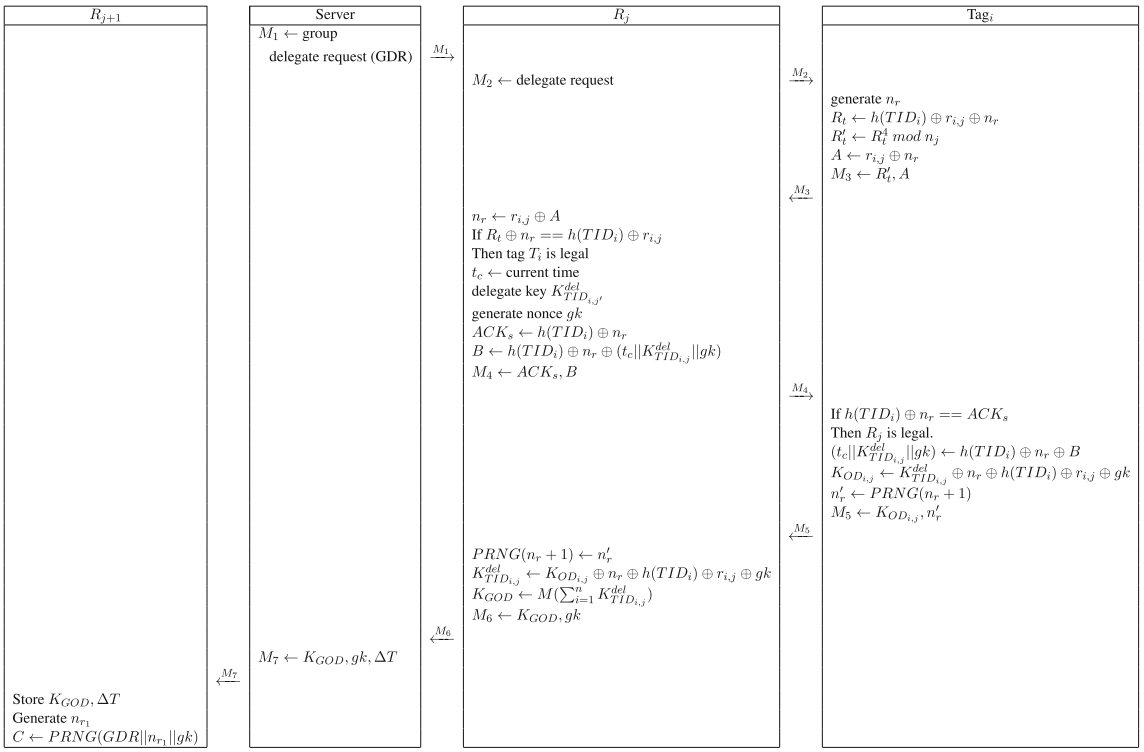

Fig. 1 Part 1 of the mutual authentication and group ownership delegation phase

follows. First the adversary does $ACK_s \oplus B$ to determine t_c, $K^{del}_{TID_{i,j}}$, and gk. The message M_5 from tag to reader contains n'_r and $K_{OD_{i,j}}$, which is $K^{del}_{TID_{i,j}} \oplus n_r \oplus h(TID_i) \oplus r_{i,j} \oplus gk$. Now, as $K_{OD_{i,j}}$, $K^{del}_{TID_{i,j}}$, gk, and ACK are known, the adversary can perform $K_{OD_{i,j}} \oplus K^{del}_{TID_{i,j}} \oplus gk \oplus ACK (= h(TID_i) \oplus n_r)$ to retrieve $r_{i,j}$.

Tag Impersonation to Reader To impersonate the tag to the reader, an adversary requires knowledge of M_3 and M_5. To this end, the individual components that make up M_3 and M_5 are required. This includes knowledge of $h(TID_i)$, $r_{i,j}$, n_r, n_j, $K^{del}_{TID_{i,j}}$, and gk. It is easy to determine n_r with $A \oplus r_{i,j}$. With knowledge of $n_r, r_{i,j}$, and $h(TID_i)$, it is easy to generate R_t. Next, n_j is not a secret for QR (Quadratic Residue) encryption as *security through obscurity* is generally not practiced. It is therefore easy to generate R'_t. This signifies that M_3 is easily generated by an adversary. Similarly M_5 can be generated with knowledge of $K^{del}_{TID_{i,j}}, n_r, h(TID_i), r_{i,j}$, and gk as these are all known to the adversary by now.

Reader Impersonation to Tag The reader sends two messages to the tag: M_2 (delegate request message) and M_4 $(h(TID_i) \oplus n_r, h(TID_i) \oplus n_r \oplus (t_c || K^{del}_{TID_{i,j}} || gk))$. Knowledge of $h(TID_i)$, n_r, t_c, $K^{del}_{TID_{i,j}}$, and gk is required to generate M_4 and just the delegate request message which can be replayed from a previous authentication round is required to generate M_2. As all these values are known to the adversary through passive observation of a previous authentication round between a tag and reader, an adversary can readily impersonate a reader to a tag.

Full Disclosure From the attacks mentioned above, it is clear that full disclosure of all terms that are meant to be secrets is possible. With no term remaining secret, an adversary has free rein over the generation of appropriate messages between readers and tags of interest.

Relay Attack As this protocol is not specifically designed to prevent relay attacks, such an attack is easily possible since these attacks rely on just relaying messages between the communicating parties with no need for any message decryption (Tu & Piramuthu, 2020).

2.2 Part 2 of Mutual Authentication and Group Ownership Delegation

A sketch of the second part of the mutual authentication and ownership delegation phase is provided in Fig. 2. We now discuss the identified vulnerabilities in this protocol.

2.2.1 Vulnerabilities

As with the first part of the mutual authentication and group ownership delegation phase protocol, the second part has similar vulnerabilities that an adversary can readily take advantage to mount attacks.

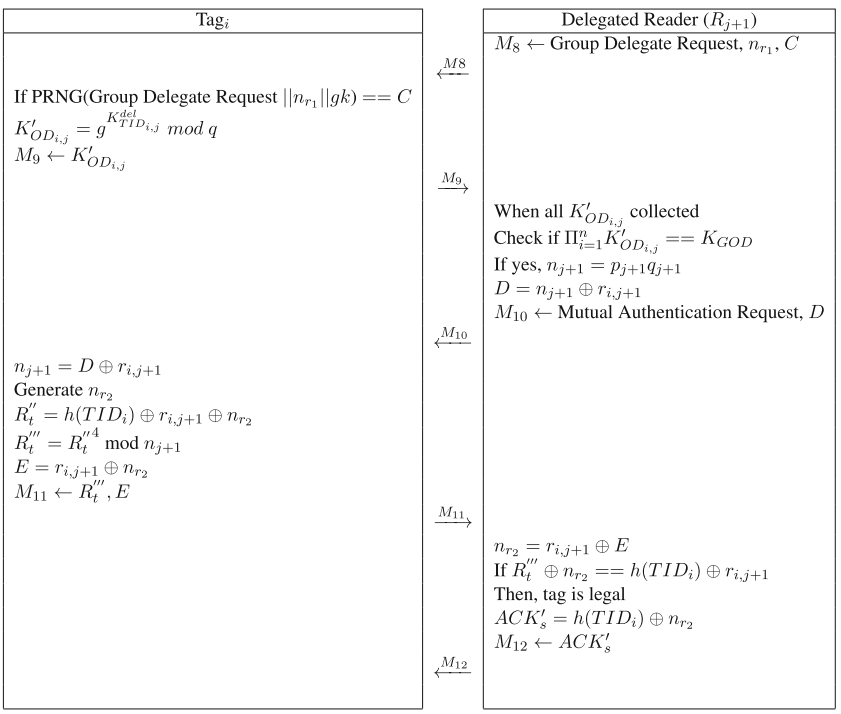

Fig. 2 Part 2 of the mutual authentication and group ownership delegation phase

Tracking and Tracing Message M_9 from tag to reader consists of $K'_{OD_{i,j}} = g^{K^{del}_{TID_{i,j}}} \ mod \ q$, which is a constant for the tag. The adversary can therefore repeatedly send M_8 to the tag to receive this consistent response from the tag which allows the adversary to track the tag.

Key and Full Disclosure An adversary can passively observe all the messages between tag and delegated reader to easily decipher the entire set of messages. One of the ways of accomplishing this is as follows. From the last message from delegated reader to tag (M_{12}), n_{r_2} can be determined as $h(TID_i)$ is known to the adversary from Part 1 of the mutual authentication and group ownership delegation phase protocol. With this knowledge, an adversary can use E from M_{11} to determine $r_{i,j+1}$ through $E \oplus n_{r_2}$. And, $R''_t = h(TID_i) \oplus r_{i,j+1} \oplus n_{r_2}$ is easy to determine as all the elements on the right hand side of this expression are known to the adversary. Next, $R'''_t = R''^4_t \bmod n_{j+1}$ can be determined as the right hand side of this expression too is now known to the adversary. From M_{10}, n_{j+1} can be determined from $D = n_{j+1} \oplus r_{i,j+1}$ as D and $r_{i,j+1}$ are known to the adversary. The adversary therefore knows the entire set of elements that are used in all messages between tag and delegated reader in this protocol.

Tag Impersonation to Reader Message M_9 from tag to delegated reader is easily generated by an adversary as all its elements are known to the adversary. Moreover, as seen in the *full disclosure* attack just discussed, it is clear that the adversary can readily impersonate the tag to the delegated reader.

Delegated Reader Impersonation to Tag Again, as seen in the *key disclosure* attack just discussed, it is clear that the adversary can readily impersonate the delegated reader to the tag.

Relay Attack As this protocol is not specifically designed to prevent relay attacks, such an attack is easily possible since these attacks rely on just relaying messages between the communicating parties with no need for any message decryption.

2.3 Part 3 of Mutual Authentication and Group Ownership Delegation

A sketch of the third part of the mutual authentication and ownership delegation phase is provided in Fig. 3. We now discuss the identified vulnerabilities in this protocol.

2.3.1 Vulnerabilities

As with the first and second parts of the mutual authentication and group ownership delegation phase

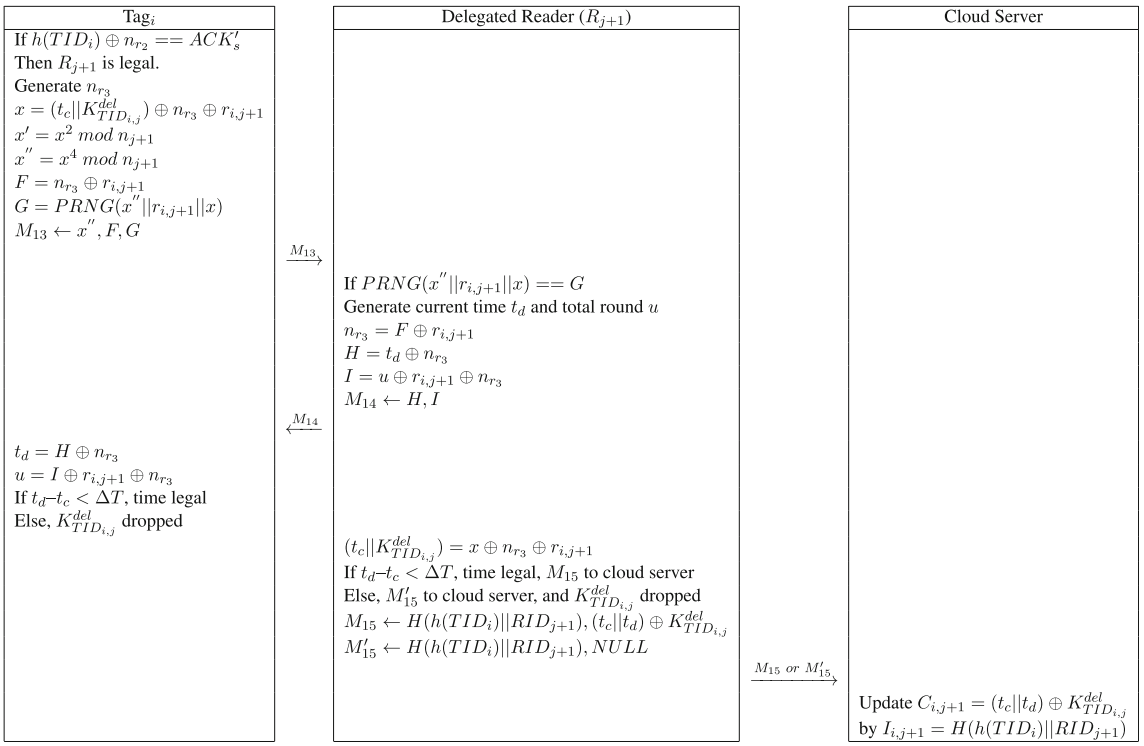

Fig. 3 Part 3 of the mutual authentication and group ownership delegation phase

protocol, the third part has vulnerabilities that an adversary can readily take advantage to mount attacks.

Full Disclosure An adversary can passively observe all the messages between tag and delegated reader to easily decipher the entire set of messages. One of the ways of accomplishing this is as follows. In M_{13}, $F = n_{r_3} \oplus r_{i,j+1}$. Here, as F is broadcast in the open and $r_{i,j+1}$ is known from the previous parts of this protocol, n_{r_3} can be readily determined. With knowledge of n_{r_3}, x can be determined from $x = (t_c || K^{del}_{TID_{i,j}}) \oplus n_{r_3} \oplus r_{i,j+1}$ as the rest of the terms on the right hand side of the expression are known. From this, x', x'', and then G can be determined. From H and I in M_{14}, both t_d and u can be readily determined as the other terms are known to the adversary.

Tag Impersonation to Delegated Reader There is only one message (M_{13}) from tag to delegated reader. As can be seen from the full disclosure attack described above, this message can be easily generated in the future to impersonate this tag to this delegated reader.

Delegated Reader Impersonation to Tag There is only one message (M_{14}) from delegated reader to tag. Again, as described in the full disclosure attack above, it is clear that the adversary can readily impersonate the delegated reader to the tag.

Relay Attack As this protocol is not specifically designed to prevent relay attacks, such an attack is easily possible since these attacks rely on just relaying messages between the communicating parties with no need for any message decryption.

2.4 e-th Time Verification Phase

We now discuss the identified vulnerabilities in the e-th time verification phase protocol. The purpose of this protocol is to restrict the number of verification rounds to a predetermined u. A sketch of the protocol is presented in Fig. 4.

2.4.1 Vulnerabilities

This protocol has only one message - that from the delegated reader to the tag. Therefore, there is no possibility or need for the adversary to impersonate the tag to the delegated reader.

Full Disclosure Here, all the elements (t_d, n_{r_2}, e) that go into the generation of the only message M_1 are known from the previous parts (1,2, and 3) of the protocol. Therefore, this message (M_1) can be readily generated by an adversary.

Delegated Reader impersonation to Tag There is only one Message (M_1) from delegated reader to tag. Again, as described in the full disclosure attack above, it is clear that the adversary can readily impersonate the delegated reader to the tag.

Desynchronization Between Tag and Delegated Reader Since e is essentially a counter, an adversary can repeatedly send M_1 to the tag by incrementing e by one each time. This would result in the tag reaching round u whereas the delegated reader has a lower value for u. Both the delegated reader (R_{j+1}) and the tag (Tag_i) keep track of the counter e. Both the delegated reader and the tag also expect the e value at their end to be in sync with that on the other end. When the e values are not the same, a side effect of this desynchronization is that these two entities may not be able to communicate with each other or accept messages from the other as valid. Here, both sides consider t_d, which might not match if the e values on both sides are different.

Time Difference Modification An adversary can easily modify t_d in M_1 that is sent to the tag. This would result in

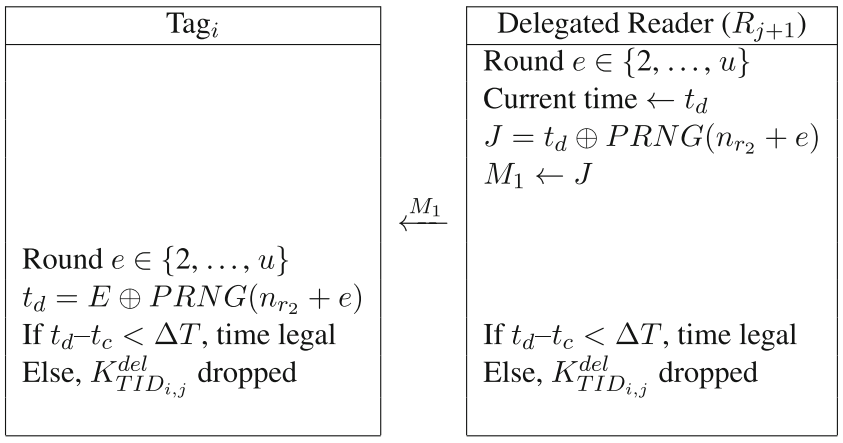

Fig. 4 e-th time verification phase

the tag dropping the delegated key and termination of e-th time verification at the tag's end.

Relay Attack As this protocol is not specifically designed to prevent relay attacks, such an attack is easily possible since these attacks rely on just relaying messages between the communicating parties with no need for any message decryption.

3 Discussion

With the increase in interest toward adoption of RFID technology in a wide variety of applications, it is of paramount importance to ensure the privacy and security of these systems. Unlike barcodes that generally identify objects at the *class* level, RFID tags identify objects at the *item* level and this exposes the RFID tagged object to potential privacy and/or security issues. Item-level object identification precipitates in rendering the situation more serious. This is especially notable as it occurs without the knowledge of the tagged object, its holder, or owner as is the case with RFID since adversaries can communicate with these tags even without direct line-of-sight and when the object is not even visible to an outside entity. Messages that are passed between RFID readers and tags are generally encrypted to avoid much of the issues that are associated with communication between RFID tags and unauthorized parties. Authentication protocols play the role of ensuring safe and secure communication between RFID tags and readers. Given the importance of such authentication protocols, when an authentication protocol is proposed it is critically evaluated for the presence of vulnerabilities. It is a necessary process that attempts to ensure the absence of at least the obviously identifiable vulnerabilities although no authentication protocol is guaranteed to be 100% secure simply because (1) such protocols depend on the difficulty of decryption of its messages due to several reasons such as prime factorization (discrete logarithm problem), and (2) the most commonly used passive RFID tags are resource-constrained devices and do not allow the use of complex operations.

We considered the authentication protocols presented in Lee et al. (2019) and identified several vulnerabilities in all the proposed protocols. We summarize the identified vulnerabilities and their consequences in Table 1. We do not attempt to *patch* these vulnerabilities since such an endeavor requires protocol design from the ground up because patching a part of the protocol could expose the protocol to other vulnerabilities (possibly at) its other parts. The purpose of our paper is not to design a new set of authentication protocols as it is outside the scope. We now discuss a few steps that could be taken toward the development of relatively secure authentication protocols.

The following recommendations are in no order of importance. To prevent easy tracking and tracing of RFID-tagged objects, identification information (e.g., tag ID) should never be sent in the open. For the same reason, any message between a tag and reader must not be predictable. It is better to make these messages seem random through any of the available number of ways (e.g., use of nonce during every authentication round). To reduce the possibility of replay attacks, it is better to include dependencies among messages in addition to removal of predictability in messages. Secrets (e.g., tag or reader shared keys) must never be disclosed or sent in the open as knowledge of such secrets could result in impersonation of tag to reader and/or reader to tag. Impersonation of a party to another is a serious issue. Relay attacks are difficult to prevent as these attacks just relay messages between parties and are difficult to

Table 1 A summary of found vulnerabilities

Vulnerabilities	Examples	Consequences
Tracking and tracing	observing the messages including M_3 in Fig. 1 and M_9 in Fig. 2	privacy violation
key/full disclosure	exposing the shared secrets including those in Figs. 1, 2, 3, and 4	confidentiality violation
tag/reader impersonation	manipulating the messages including M_3, M_5 in Fig. 1 , M_9 in Fig. 2, and M_{13}, M_{14} in Fig. 3;	accountability violation
de-synchronization	manipulating the counters including e, u in Fig. 4	availability violation
modification	manipulating the time difference of message M_1 in Fig. 4	integrity violation
relay attack	falsifying the distance between readers and tags in Figs. 1, 2, 3, and 4	accountability violation

prevent through cryptographic means. Therefore, additional measures (Tu & Piramuthu, 2020) should be taken (e.g., distance-bounding, ambient conditions) to prevent or at least the identification of such an attack when it occurs.

References

Bose, I., Lui, A., & Ngai, E.W.T. (2011). The impact of RFID adoption on the market value of firms: an empirical analysis. *Journal of Organizational Computing and Electronic Commerce*, *21*(4), 268–294.

Kapoor, G., & Piramuthu, S. (2012). Single RFID tag ownership transfer protocols. *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, *42*(2), 164–173.

Lee, C.-C., Li, C.-T., Cheng, C.-L., Lai, Y.-M., & Vasiakos, A.V. (2019). A novel group ownership delegate protocol for RFID systems. *Information Systems Frontiers*, *21*, 1153–1166.

Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A.S. (2010). Classifying RFID attacks and defenses. *Information Systems Frontiers*, *12*(5), 491–505.

Tu, Y.-J., & Piramuthu, S. (2020). On addressing RFID/NFC-based relay attacks: an overview. *Decision Support Systems, 129*.

Yu-Ju Tu is Associate Professor of Management Information Systems in the College of Commerce at National Chengchi University (NCCU) in Taipei, Taiwan. He received his Ph.D. from University of Illinois at Urbana–Champaign (UIUC), USA and his research interests include RFID systems.

Gaurav Kapoor is Assistant Professor of Information and Communication Technology (Information Security) at the Singapore Institute of Technology, Singapore. He received his Ph.D. from the University of Florida, USA and his research interests include RFID systems, and IT governance and compliance.

Selwyn Piramuthu is Professor of Information Systems at the University of Florida. His research interests include RFID systems.