# Addressing Relay Attacks Without Distance-Bounding in RFID Tag Inclusion/Exclusion Scenarios

Selwyn Piramuthu(✉)

Information Systems and Operations Management, University of Florida, Gainesville, FL 32611-7169, USA
selwyn@ufl.edu

**Abstract.** With the widespread adoption and use of RFID tags, a valid scenario is one in which an RFID-tagged object includes several components that each have their own individual RFID tags. Under such a context, each of the components are bound to be included in or excluded from the main object over its lifetime. In order for only the tags that are a part of the main object to be authenticated by the main object, there is a need for a secure protocol that ensures that no other tag has access to the shared secrets among the main object and the component objects. Moreover, there is also a need to address relay attacks by adversaries under such scenarios. Existing authentication protocols address relay attacks through round-trip distance measurements in such inclusion/exclusion scenarios. While this works in principle, distance-bounding approaches are not always reliable. We consider another approach for inclusion/exclusion scenarios and develop a protocol sketch for this context. We also provide related security analysis.

**Keywords:** RFID · Tag inclusion/exclusion
Authentication protocol · Non distance-bounding

## 1 Introduction

An object with its own RFID (Radio-frequency IDentification) tag is not uncommon. For example, in a retailing context, item-level tags are used (e.g., Levi's jeans at Kohls, shoes at Macy's, most items at American Apparel stores) to identify and to individually consider each item at the store. The benefits of item-level RFID tags are many, and include tracking and tracing of each such tagged item, customized handling of each item (e.g., perishables, based on experienced ambient conditions), among others. The use case for item-level RFID tags is clear. In addition to objects with a single RFID tag, there are cases where an object can possibly be associated with several RFID tags. For example, any object with multiple components has this possibility where each of the components have their own RFID tags.


S. M. Thampi et al. (Eds.): SIRS 2018, CCIS 968, pp. 147–156, 2019.
https://doi.org/10.1007/978-981-13-5758-9_13

Under such a scenario, it is necessary for all the components' tags to have something in common (e.g., a shared secret) that allows them to communicate with the main object. Such a commonality would facilitate coordination among the components and the main object with the exclusion of tags that do not belong to this constellation. Moreover, such a main object-components scenario generally does not remain static. Over the lifetime of the main object, each of the components could possibly be a part of the main object only during a fraction of the time. This necessitates the possibility of components joining as well as leaving the main object of interest. For example, a computer system can have the monitor replaced by a new monitor; an automobile can have its tires replaced by new tires; a printer can have its almost empty ink cartridge replaced by a new ink cartridge.

As the name suggests, relay attacks are operationalized as messages are simply relayed between multiple entities. In the RFID system context, one or more adversaries relay the messages without any modification between RFID tag and reader. To the reader, it is as if the RFID tag is in close physical proximity and the RFID tag assumes that the reader is in close physical proximity. This is because almost all extant RFID authentication protocols do not specifically check or account for any delay in response from the recipient of a message. Since the messages themselves are not modified, the authentication protocols proceed to successful completion. The extent of the harm done through relay attacks depends on the specific application of interest. For example, it has been shown that RFID-based car keys are vulnerable to relay attacks [1] and allow adversaries to gain entry to a car that is physically parked farther away from the car key.

Although there are dozens of protocols that have been proposed to provide defense against relay attacks for RFID-based systems in general, almost all of them are based on the distance-bounding idea where the time taken for a bit to travel between two entities (usually the tag and reader) is taken as proxy for the distance traveled by that bit. While this works perfectly in principle, there is one major concern with these authentication protocols. The issue is that when tag and reader are expected to be at the most a few meters apart, it is rather difficult to tell reader and tag that are meters apart from those that are miles apart since bits don't just travel between two entities. The receiving entity needs to receive the bit, identify it as something that the receiving entity should send back to the sending entity, and send it back. This process involves time. When the time involved is somehow more than an order or two in magnitude over nanoseconds for whatever reason, distance measurement based on the time taken for the bit to travel between tag and reader becomes unreliable and inaccurate.

We develop a sketch of a non-distance-bounding authentication protocol that is resistant against relay attacks for inclusion/exclusion scenarios. As with similar authentication protocols, we also consider the use of ambient conditions for the proposed authentication protocol that is designed to be resistant against relay attacks, but for the inclusion/exclusion scenario.

We include brief discussion on relay attacks in Sect. 2. We provide an overview of inclusion/exclusion protocols in Sect. 3. We then include a sketch of the

proposed protocol in Sect. 4. We consider the security properties of the proposed protocol in Sect. 5. We conclude the paper in Sect. 6.

## 2 Relay Attacks

Almost all extant RFID system authentication protocols generally operate with the assumption that the tag and reader are next to each other. When this requirement is satisfied, it allows for minimal opportunities for an adversary to wedge in-between the tag and reader and accomplish a relay attack. Even if an adversary manages to squeeze in-between the tag and reader within this short separation, it is more difficult for the adversary to get away without being noticed. However, unfortunately, for relay attacks to be accomplished, the reader and tag can physically be miles apart. In addition, such relay attacks are oftentimes mounted without the knowledge of the reader or tag.

Hancke and Kuhn's (2005) (Fig. 1) distance-bounding protocol is divided into two phases. The first phase does not include a time component and the second phase includes a time component [2] that is accomplished through the clock at the reader's end. The second phase is done iteratively where a single bit is sent from the reader to the tag and the round-trip taken by this bit is measured. The time taken by several such single bits are measured. The primary purpose of the first phase is to generate $R^0||R^1$, which is then used in the second (timed) phase where either $R^0$ or $R^1$ is randomly chosen and its $(i-1)^{th}$ position bit is sent to the tag at the $i^{th}$ iteration. Before completion of the protocol, the following are ensured: (a) each of the $n$ round trip times is at most $(\Delta t_{max})$ and (b) the

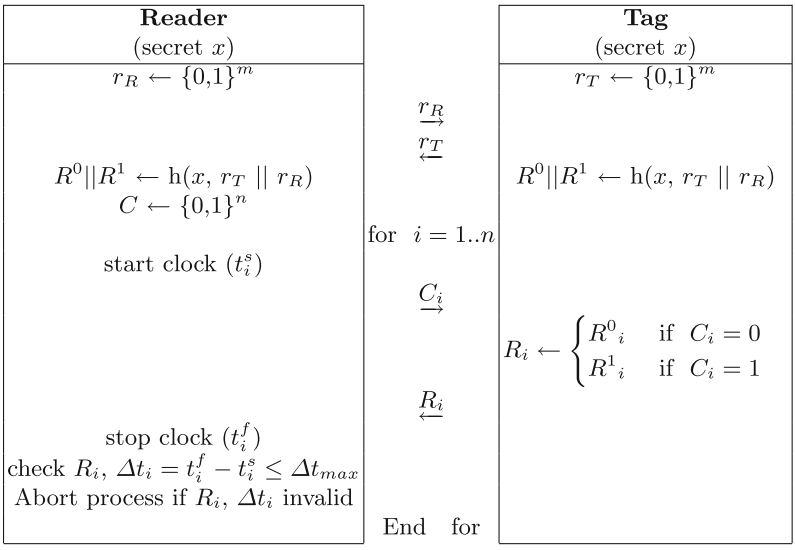


**Fig. 1.** Hancke and Kuhn's (2005) protocol

$R$ ($R^0$ or $R^1$) values are valid. Both of these tests need to be successfully passed for ensuring the absence of a relay attack.

This protocol has several vulnerabilities as was identified in later publications (e.g., Tu and Piramuthu 2017). Reid et al. (2007) avoid the scenario where the dishonest tag shares its secrets with the adversary [10]. Other researchers have developed variants of the distance-bounding protocol such as a different outer loop [11], mixed challenges [3], and pre-computing response [4]. A few other protocols indirectly measure distance (e.g., Rasmussen and Čapkun 2008, which is vulnerable to mafia fraud attack [5,9]).

## 3 Protocol for Multi-tagged Object

The notations used in this paper include:

$N_t, N_p, N_r, N_u, N_T, N_R, N_R^{'}, N_P, N_T, r_A, r_B$: random n-bit nonce
$s_c, s_{c+1}$: Tag's current and subsequent keys
$f_k^{'}$, $f_k$, $\{\}_k$: keyed (with key $k$) encryption function
$H_k$: keyed (with key $k$) one-way hash function
$t_j$: shared secret between tag$_i$ and TTP, Reader
$r_i$: shared secret between Reader $R_i$ and TTP
$id_{t_j}$: tag $t_j$ identifier
$T_{AC}, R_{AC}$: Measured ambient condition at tag and reader respectively

Piramuthu [8] develops a inclusion/exclusion protocol with no consideration for the possibility of relay attacks (Fig. 2). Clearly, then, this protocol is vulnerable to relay attacks.

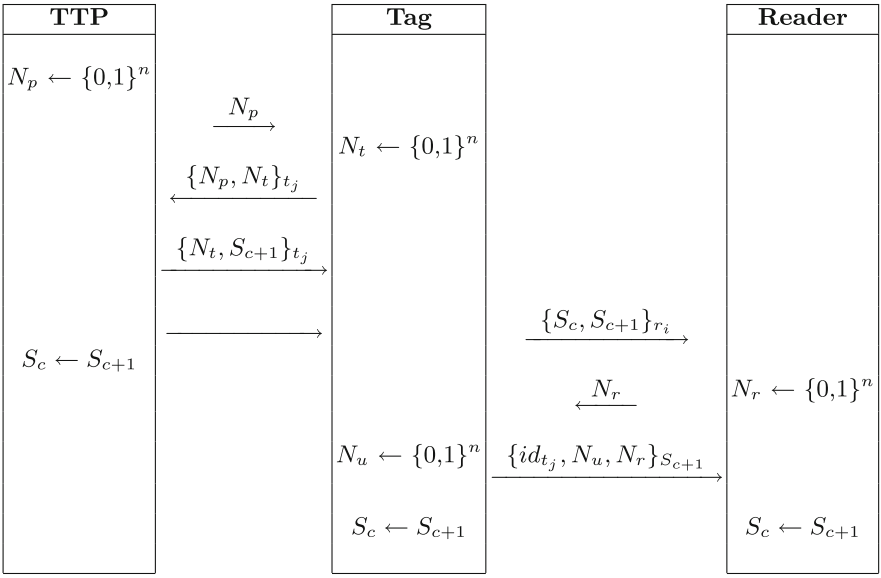


**Fig. 2.** The inclusion/exclusion protocol of Piramuthu (2018)

Although there are a few studies that have considered the inclusion/exclusion scenario, only one of the existing protocols explicitly considers the issue of relay attacks for the inclusion/exclusion aspect of component RFID tags as a part of a larger ensemble. Piramuthu [6,7] developeds a protocol (Fig. 3) that involves a reader, a trusted third party and the RFID tags. These protocols use a variant of the distance-bounding method to address relay attacks.

This protocol (Fig. 3) is for a scenario where RFID tags are allowed to join as well as leave an ensemble of RFID tagged items (components). A trusted third party (TTP) is assumed to be present in order to mediate communication between the reader and tags, specifically with respect to secret key updates as and when a tag either enters or leaves the ensemble. This protocol assumes that all component RFID tags share the same common secret, which is simultaneously updated for every tag that belongs to the ensemble whenever a change in the ensemble composition occurs. The purpose of the key update is to ensure that all

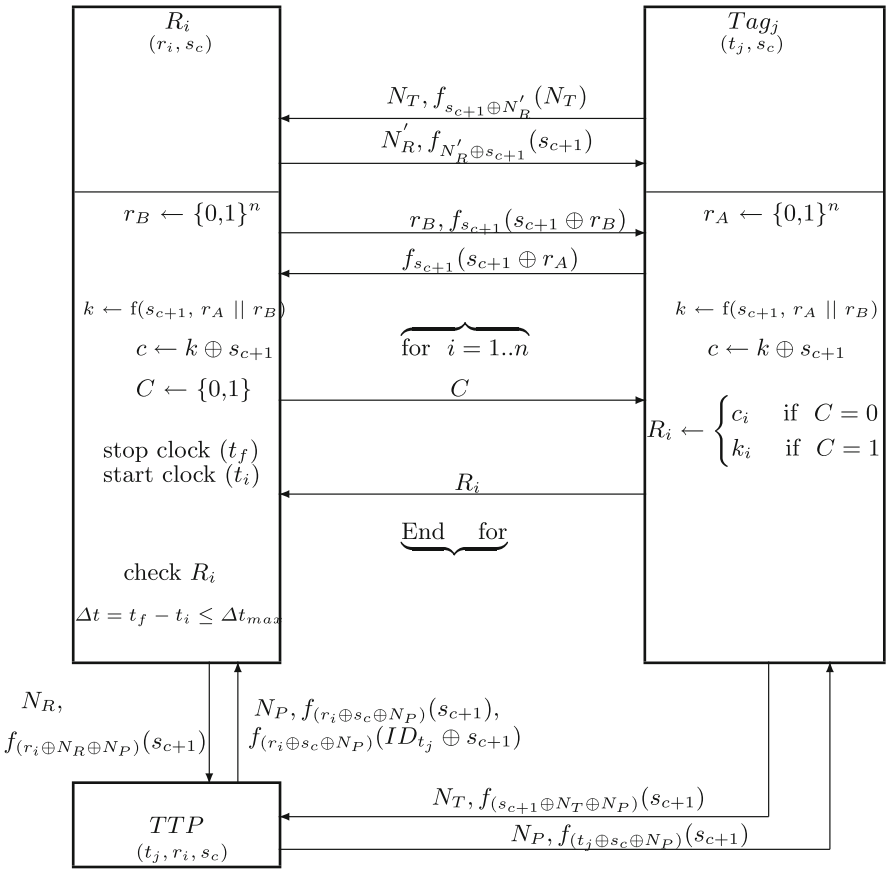


**Fig. 3.** Tag inclusion/exclusion protocol (Piramuthu 2011)

tags that belong to the ensemble of tags share a common secret while excluding any tag that does not belong to this ensemble from knowledge of this shared secret. A component that leaves this ensemble is not allowed to have knowledge of the updated shared secret as soon as it leaves.

## 4 The Proposed Protocol

We modify the protocol presented in Piramuthu (2018) to include resistance against relay attacks. The same three set of entities (TTP, tags, reader) are involved in the process. To provide resistance to relay attacks, we make use of ambient condition information [12]. There are several ambient conditions that can be used in this context. However, some of the ambient conditions suffer from directionality issues. The directionality issue results in different ambient condition readings. Other ambient condition facets include pressure, temperature, magnetic field, and location (GPS). Some of these are context specific. For example, GPS readings are not appropriate/accurate for use in locations that block GPS signals (e.g., inside buildings, under tree cover). Moreover, it is not difficult to mess with GPS signals. Given these reasons, we do not specify a specific ambient condition for the proposed protocol. We assume that an appropriate ambient condition sensor is chosen for the application of interest, taking the context into full consideration. The proposed protocol (Fig. 4) is a variant of the protocol developed in Piramuthu (2018).

The TTP begins with a nonce ($N_r$) that is sent to each of the tags. In response, each of the tags generate their own nonce ($N_t$) that is sent along with the TTP's tag encrypted with the shared secret ($t_j$). The TTP sends the encrypted (with $t_j$) new group shared key ($S_{c+1}$) along with $N_t$. This concludes new group key sharing by the TTP with the tags. The next part of the protocol is to ensure that the tag and reader are next to each other and to ensure that both the tag and reader have the new group key. The TTP then sends the previous and new keys encrypted with the shared key ($r_i$) to the reader and then updates the new key as its current key. It keeps the previous key in memory just in case an adversary blocks any of the messages and attempts to cause desynchronization. The reader sends nonce ($N_r$) to the tag. The tag generates another nonce ($N_u$). It then measures its ambient condition ($T_{AC}$). The tag sends the encrypted (with $S_{c+1}$) message with $id_{t_j}, N_u, N_r, T_{AC}$ to the reader. The reader measures its ambient condition ($R_{AC}$) and verifies if its ambient condition measurement is close to the tag's ambient condition measurement. When they are next to each other, these two measurements should not be significantly different from each other. When this is not the case, the reader aborts the protocol. If not, the reader encrypts $id_{t_j}, N_u, R_{AC}$ (with $S_{c+1}$) and sends it to the tag as evidence that its measured ambient condition value is close to that of the tag's measured ambient condition value. The reader then updates its group shared secret while storing the previous key. The tag does the same once it receives and confirms the last message from the reader. This ends one round of the protocol and all

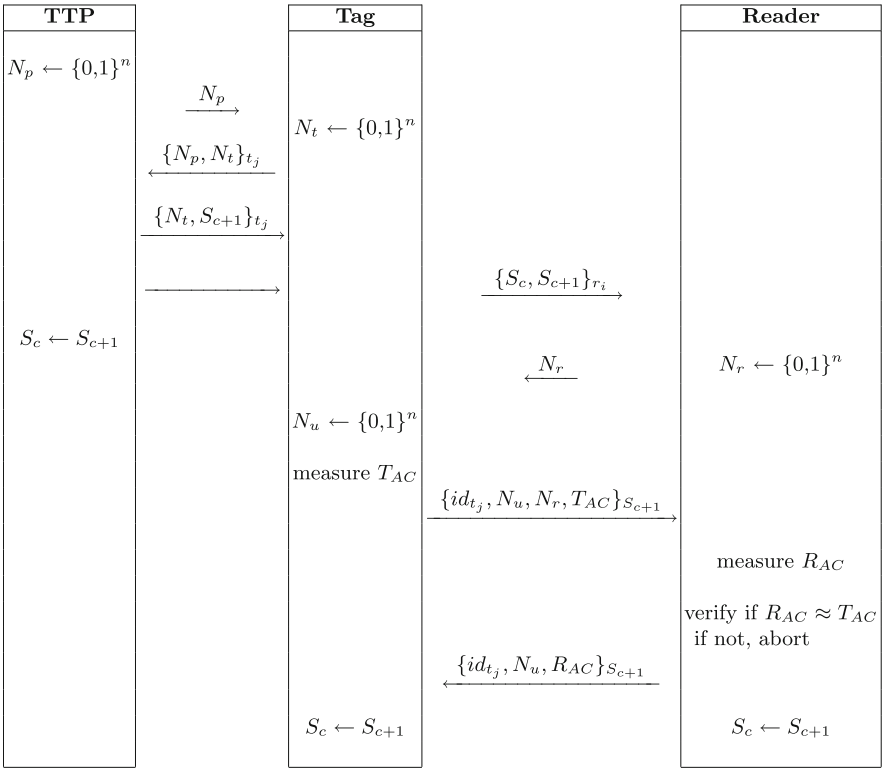


**Fig. 4.** The proposed inclusion/exclusion protocol

the entities (reader, TTP, and tags) have the same updated shared group secret ($S_{c+1}$). Both the reader and the TTP wait for response from the recipient of its message. When the response does not arrive on time, the protocol is aborted.

## 5 Security Analysis

Any pair of the entities are assumed to communicate with each other in an environment that is not assumed to be secure. The proposed protocol is executed when there is a change in the group constellation - when at least one entity (component tag) enters or leaves the ensemble regardless of the reason. We assume the existence of resourceful active adversaries who are able to block, modify, resend any of the messages that are passed between any two entities. Freshly-generated nonce ($N_p, N_r, N_u, N_t$) are used during each run of the protocol. The adversary cannot learn anything that is usable with knowing one of ($t_j, r_i$) since both the secrets are required for successful authentication.

Other possible attacks include the following.

*Tag/Reader Anonymity:* The information that is unique to each tag and reader include their shared secret keys $(t_j, r_i)$ and the group shared secret $(S_c)$. With knowledge of these, it is possible for an adversary to impersonate as well as clone a tag. To protect the tags and reader from such attacks, we ensure that none of this information is made available to adversaries regardless of their attempt(s) to retrieve this information.

*Forward Security:* The proposed protocol is not forward-secure since knowledge of all shared secrets (i.e., both $t_j$ and $r_i$) will allow an adversary to decrypt all earlier messages that are sent between any two entities. The group keys are also vulnerable to such attacks.

*Secrecy/Data Integrity and Authenticity:* None of the identifiers are sent in the open.

*DoS/Desynchronization:* The purpose of this protocol is to update the shared secret key whenever a change in the constellation of the ensemble of tags occurs. An adversary could potentially block messages after one entity has changed the key to the updated key and cause desynchronization. Since the shared group key is updated during every round of the protocol, both the reader and the TTP store the previous group key just in case a desynchronization attack is mounted in the future. The group key update is accomplished by the reader and tag and in the middle of the protocol by the TTP after it has sent out its last message in the protocol.

*Reader/Tag Impersonation Attack:* For successful impersonation attack to occur, the adversary should be able to generate messages that are successfully validated by the recipient of those messages. Since the messages that are sent later are dependent on those that are sent earlier (e.g., through use of freshly generated nonce), simply replaying captured messages from an earlier run of the protocol will not work.

*Mafia Attack:* Since the ambient condition selected and used in the protocol needs to be the same at the reader and the tag end and all the messages (other than just nonce) that are sent between any two entities are encrypted, it is not easy to mount this type of attack.

*Terrorist Attack:* A tag that colludes with an adversary can share the group secret key with the adversary. However, it cannot share its shared key with the reader or TTP $(r_i, t_j)$ with the adversary since doing so will compromise its identity - the adversary can clone the tag and this is not a desired outcome for the tag of interest.

*Replay Attack:* With the presence of freshly-generated nonce that affects messages that are passed between any two entities, a replay attack will not succeed in the proposed protocol.

## 6 Discussion

We considered the inclusion/exclusion scenario for an object with a dynamic ensemble of RFID tags that enter and leave the main object over time. Specifically, we considered the scenario where relay attacks could be mounted on such a system. Relay attacks are especially dangerous since these are rather difficult to detect and address. Almost all of the RFID protocols in existence fall prey to relay attacks unless they are specifically designed to be resistant against such attacks. These attacks are difficult to address since (a) they are passive attacks with no change to the messages that are passed between two entities, and (b) therefore do not depend on cryptography for their success. Among the RFID-based protocols that specifically consider the existence of relay attacks, almost all of them use some variant of distance-bounding means to determine the distance between tag and reader. We did not use the more common distance-bounding means to determine the physical separation between tag and reader since it has serious measurement issues due to (unexpected) delays that could occur at the tag's end which would render the precise measurement of distance between tag and reader useless. We considered the use of ambient conditions for this purpose. We did not consider a specific ambient condition in this protocol since that could be context-specific. The purpose of this paper include creating awareness of the inclusion/exclusion setup in RFID systems and the use of non-distance-bounding means to approach relay attacks in such systems. The hope is that other researchers would study this scenario and eventually develop more secure protocols for this system setup.

## References

1. Greenberg, A.: Radio Attack lets Hackers Steal 24 Different Car Models. Wired, 21 March 2016. https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/
2. Hancke, G.P., Kuhn, M.G.: An RFID distance bounding protocol. In: Proceedings of the IEEE/Create-Net SecureComm, pp. 67–73 (2005)
3. Kim, C.H., Avoine, G.: RFID distance bounding protocol with mixed challenges to prevent relay attacks. In: Garay, J.A., Miyaji, A., Otsuka, A. (eds.) CANS 2009. LNCS, vol. 5888, pp. 119–133. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10433-6_9
4. Mauw, S., Toro-Pozo, J., Trujillo-Rasua, R.: A class of precomputation-based distance-bounding protocols. In: Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), pp. 97–111 (2016)
5. Mitrokotsa, A., Onete, C., Vaudenay, S.: Mafia fraud attack against the RC distance-bounding protocol. In: Proceedings of the IEEE International Conference on RFID -Technologies and Applications (RFID-TA), pp. 74–79 (2012)
6. Piramuthu, S.: Relay attack-resisting inclusion/exclusion protocol for RFID. In: 2nd International Workshop on DYnamic Networks: Algorithms and Security (DYNAS) (2010)
7. Piramuthu, S.: Inclusion/exclusion protocol for RFID tags. In: Meghanathan, N., Kaushik, B.K., Nagamalai, D. (eds.) CCSIT 2011. CCIS, vol. 133, pp. 431–437. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-17881-8_41

8. Piramuthu, S.: Authentication protocols for an object with dynamic RFID tags. In: Doss, R., Piramuthu, S., Zhou, W. (eds.) FNSS 2018. CCIS, vol. 878, pp. 93–101. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-94421-0_7
9. Rasmussen, K., Čapkun, S.: Location privacy of distance bounding. In: Proceedings of the Annual Conference on Computer and Communications Security (CCS), pp. 149–160 (2008)
10. Reid, J., Gonzalez Nieto, J.M., Tang, T., Senadji, B.: Detecting Relay Attacks with Timing-Based Protocols. Queensland University of Technology ePrint (2006). http://eprints.qut.edu.au/view/year/2006.html
11. Tu, Y.-J., Piramuthu, S.: RFID distance bounding protocols. In: 1st International EURASIP Workshop on RFID Technology, pp. 67–68 (2007)
12. Tu, Y.-J., Piramuthu, S.: Non-distance-bounding means to address RFID relay attacks. Decis. Support Syst. **102**, 12–21 (2017)