# Security Analysis on RFID Mutual Authentication Protocol

You Sung Kang[1(✉)], Elizabeth O'Sullivan[2], Dooho Choi[1], and Maire O'Neill[2]

[1] Cyber Security Research Division, Electronics and Telecommunications
Research Institute, Daejeon 305-350, Korea
{youskang,dhchoi}@etri.re.kr
[2] Centre for Secure Information Technologies,
Queen's University Belfast, Belfast BT3 9DT, UK
e.osullivan@qub.ac.uk, m.oneill@ecit.qub.ac.uk

**Abstract.** Radio frequency identification (RFID) has received much attention both in industry and academia in recent years. To this extent, the international standards group, ISO/IEC JTC 1/SC 31, is in the midst of standardization activity to define the security extension to the EPC-global Generation 2 (Gen2) ultra high frequency (UHF) air interface protocols for secure RFID communications. In this paper, we investigate a vulnerability of an RFID mutual authentication protocol that was highlighted in a recent letter [5]. Our analysis presents that the attack on the mutual authentication protocol is just a relay operation between a legitimate reader and a legitimate tag. We also propose the threshold values of data rate between a reader and a tag based on link timing parameters of passive UHF RFID systems.

**Keywords:** RFID security · Mutual authentication · RFID Gen2 · ISO/IEC 29167-6 · Man-in-the-middle attack

## 1 Introduction

Radio frequency identification (RFID) technology is rapidly emerging as a leading ubiquitous computing technology. RFID systems provide the ability to automatically identify and track objects and/or personnel in a non-contact, non-line-of-sight manner. This enables the development of very efficient automated item management frameworks and as such provides a compelling business case for the rapid adoption of RFID systems. However, due to the very nature of being able to read an RFID tag without line-of-sight, presents significant security challenges that must be addressed in order for this technology to transfer seamlessly and securely into industry.

A typical RFID system consists of a reader, $R$, composed of a set of transceivers together with a backend database, and a set of tags, $T_i$ ($1 \leq i \leq N$, $N$ is the total number of tags), where each tag is a passive transponder identified by a unique ID. The communication between a reader and the tags is defined by

H. Kim and D. Choi (Eds.): WISA 2015, LNCS 9503, pp. 65–74, 2016.
DOI: 10.1007/978-3-319-31875-2_6

the EPCglobal Generation 2 (Gen2) specification. This specification includes the physical layer and medium access control parameters for ultra high frequency (UHF) RFID passive tags operating in the frequency band between 860 MHz and 960 MHz [1]. The international standard group, ISO/IEC JTC 1/SC 31, is in the process of standardizing the security extension to the ISO/IEC 18000-63 standard that is based on the EPCglobal Gen2 protocol [2]. Amongst several candidates, ISO/IEC 29167-14 that is based on advanced encryption standard-output feedback (AES-OFB) mode of operation has been proposed to define a variety of authentication protocols and session key generation applicable to the ISO/IEC 18000-63 standard [3].

The initial proposal that defines an RFID mutual authentication protocol and session key generation was ISO/IEC working draft (WD) 29167-6 [4]. ISO/IEC 29167-6 WD proposal describes three security protocols, namely **Protocol 1**, **2**, and **3**. ISO/IEC 29167-14 succeeds this and includes the authentication protocols and main contents of ISO/IEC 29167-6 WD proposal. **Protocol 1** considers the RFID mutual authentication and secure communication in security mode. In a recent letter [5], it was highlighted that **Protocol 1** is vulnerable to an attack that results in the manipulation of a communication parameter, called the *Handle*, such that the tag and the reader fail to share the same *Handle* for subsequent communications during a run of the protocol. This attack is named as a man-in-the-middle attack in the letter. In the same letter, a cryptographic countermeasure was presented that introduced dependency between security parameters in a message using a more complex variable length shift technique, and constructed the *Handle* as the concatenation of the challenge from the reader and the challenge from the tag.

In this paper, we review the vulnerability to the man-in-the-middle attack proposed in [5] and introduce different points of view about the man-in-the-middle attack presented in [6,7]. In addition, we point out that the effect of the man-in-the-middle attack on the RFID mutual authentication protocol is just a relay between a legitimate reader and a legitimate tag. We also analyze a correlation between link timing parameters and the man-in-the-middle attack. The remainder of this paper is organized as follows. We review the man-in-the-middle attack together with an improved mutual authentication protocol proposed in [5] in Sect. 2. In Sect. 3, we analyze the attack effects in terms of security weakness and link timing parameters. Finally, we conclude the paper in Sect. 4.

## 2 Review of *Handle* Manipulation Attack

For the sake of completeness, we review **Protocol 1** of ISO/IEC 29167-6 WD (shown in Fig. 1) and the *Handle* manipulation attack together with the associated countermeasure presented in [5]. **Protocol 1** assumes that the tag shares the same 128-bit master key with the reader and that the key stream is produced using AES algorithm as the encryption engine. Step 0 to step 9 (see Fig. 1) are concerned with the setting up of the secure channel. During this exchange of messages, the security parameters *RnInt* (step 7) and *RnTag* (step 8), which are

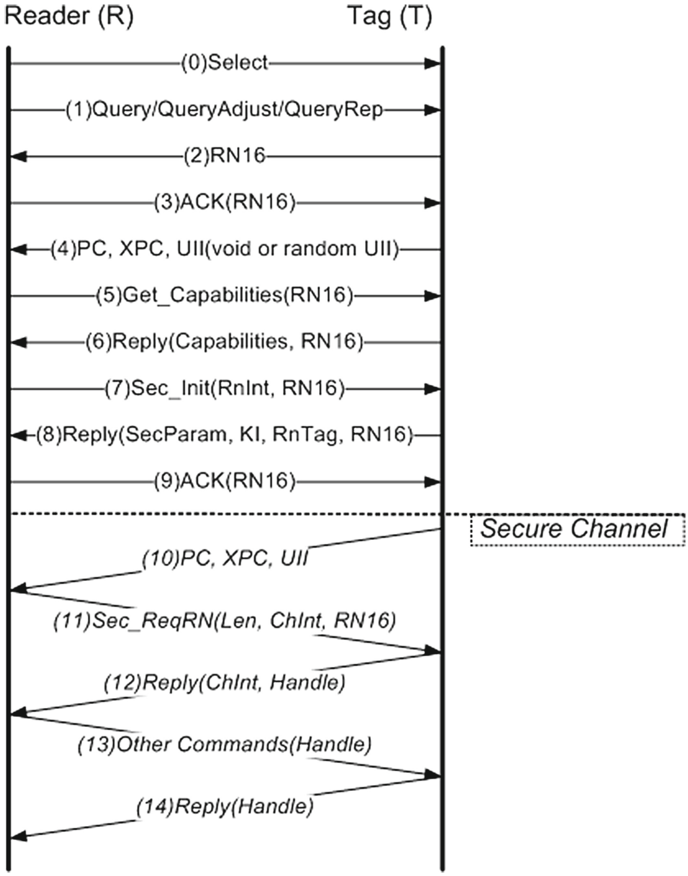
Reader (R)
Tag (T)
(0)Select
(1)Query/QueryAdjust/QueryRep
(2)RN16
(3)ACK(RN16)
(4)PC, XPC, UII(void or random UII)
(5)Get_Capabilities(RN16)
(6)Reply(Capabilities, RN16)
(7)Sec_Init(RnInt, RN16)
(8)Reply(SecParam, KI, RnTag, RN16)
(9)ACK(RN16)
Secure Channel
(10)PC, XPC, UII
(11)Sec_ReqRN(Len, ChInt, RN16)
(12)Reply(ChInt, Handle)
(13)Other Commands(Handle)
(14)Reply(Handle)

**Fig. 1. Protocol 1** - RFID mutual authentication protocol.

64-bit random numbers, are generated and exchanged by the reader and tag, respectively. $RnInt$ and $RnTag$ are then concatenated to create the initial vector (IV) as input to the AES algorithm and the master key is used as the AES key for the first iteration of key stream generation. Subsequent iterations of AES uses the output generated from the previous iteration as the input to AES algorithm. We note that even though $RnInt$ and $RnTag$ are sent in the clear, without knowledge of the master key the key stream cannot be determined.

The secure channel commences upon a successful acknowledgement of the 16-bit random number $RN16$ at step 9. Taking $k_i$ to be consecutive blocks of the key stream whose block length is determined by the length of the parameter it is XOR'd with, the first message of the secure channel (step 10) is sent from the tag to the reader and is given as,

$$T \rightarrow R : (PC, XPC, UII) = (PC \oplus k_1, XPC \oplus k_2, UII \oplus k_3) \qquad (1)$$

where $PC$ is the protocol control, $XPC$ is the extended protocol control and $UII$ is the actual unique item identifier (note a random or void $UII$ was sent earlier in step 4 of the protocol procedure). It is at the next step that the attack described in [5] begins.

The message sent from the reader to the tag in step 11 is

$$\begin{aligned} R \rightarrow T : &\textbf{Sec\_ReqRN}(Len, ChInt, RN16) \\ &= (Len \oplus k_4, ChInt \oplus k_5, RN16 \oplus k_6) \end{aligned} \tag{2}$$

where $RN16$ is the encrypted version of $RN16$ that was sent earlier in the clear, $ChInt$ is a random challenge from the reader and $Len$ is a 3 bit indicator of the wordlength of $ChInt$ (one word is 16 bits). Hence the value of $Len$ can range from 0 to 7, where all zeros are interpreted as a value of 8. This implies that the length of $ChInt$ can range from 16 bits to 128 bits. In the attack, the adversary intercepts and changes the random parameter 2 of this message denoted by Eq. (2), with a different random number, so that the message becomes

$$R \rightarrow T : (Len \oplus k_4, R_1, RN16 \oplus k_6) \tag{3}$$

Upon receiving this message the tag will decrypt using the key stream and check that the $RN16$ parameter matches the $RN16$ that was sent earlier in the clear, if true the tag authenticates the reader. At this point, however, the tag does not contain the actual challenge that was sent by the reader, but instead it registers $R_1 \oplus k_5$ as the challenge.

Step 12 contains the reply from the tag to the reader and according to **Protocol 1** the message is intended to be

$$T \rightarrow R : \textbf{Reply}(ChInt, Handle) = (ChInt \oplus k_7, Handle \oplus k_8) \tag{4}$$

however, because of the manipulation of the previous message (shown in Eq. (3)), which results in the tag registering $R_1 \oplus k_5$ as the challenge from the reader, the actual message sent from the tag is

$$T \rightarrow R : ((R_1 \oplus k_5) \oplus k_7, Handle \oplus k_8) \tag{5}$$

where $Handle$ is defined as a 16 bits temporary tag identification number, that the tag generates and backscatters to the reader, and is thus used in subsequent communications by the tag and the reader.

The adversary continues with the attack by manipulating parameter 1 of Eq. (5) with $ChInt \oplus k_5$, observed in step 11 of the protocol (see Eq. (2)), together with the random number $R_1$ that was injected in step 11 (see Eq. (3)), and further manipulates parameter 2 of Eq. (5) to produce

$$T \rightarrow R : ((R_1 \oplus k_5) \oplus k_7 \oplus (ChInt \oplus k_5) \oplus R_1, R_2) = (ChInt \oplus k_7, R_2) \tag{6}$$

The reader decrypts using the key stream and checks that the $ChInt$ sent from the tag matches the reader's $ChInt$, if true the reader authenticates the tag. However, at this point the reader and the tag fail to share the same $Handle$

as the reader's $Handle$ is now $R_2 \oplus k_8$. Note here that the manipulation of $ChInt$ in steps 11 and 12 does not contribute to the manipulation of the $Handle$, the $Handle$ manipulation attack would have just as easily occurred had the adversary only intercepted and manipulated parameter 2 of the message in step 12. Also note that at no point in the attack is the security of the key stream compromised.

We now turn our attention to the proposed countermeasure presented in [5]. The idea here is to create a dependency between the parameters of the message by using a variable length shift to build integrity into the message. In the countermeasure the message in step 11 becomes,

$$\begin{aligned} R \rightarrow T : (Len, ChInt \ll k_5, RN16 \oplus L_{16}(ChInt)) \\ = (Len \oplus k_4, (ChInt \ll k_5) \oplus k_6, RN16 \oplus L_{16}(ChInt) \oplus k_7) \end{aligned} \tag{7}$$

where now parameter 2 contains a bitwise rotation by $k_5$ whose bit length is determined by the value of $Len$ and is given as $\lceil \log_2(Len \times 16) \rceil$, hence the bit length of $k_5$ can range from 4 bits to 7 bits. The left-most 16 bits of the challenge parameter $ChInt$ (i.e., $L_{16}(ChInt)$) is included in parameter 3 XOR'd with $RN16$. Thus $ChInt$ is now contained within two parameters of the message in different formats (one rotated by a secret amount and one not), so that any manipulation en-route may be detected by the tag.

Step 12 of the countermeasure then becomes

$$\begin{aligned} T \rightarrow R : (ChTag \ll k_8, ChInt \oplus ChTag) \\ = ((ChTag \ll k_8) \oplus k_9, (ChInt \oplus ChTag) \oplus k_{10}) \end{aligned} \tag{8}$$

where $\text{BitLen}(k_8) = \lceil \log_2(Len \times 16) \rceil$, and $\text{BitLen}(k_9) = \text{BitLen}(k_{10}) = \text{BitLen}(ChInt)$. Here the tag now also produces a challenge, $ChTag$, which is of the same bit length as $ChInt$ (i.e. from 16 bits to 128 bits). $ChTag$ is bitwise rotated by a secret amount and is delivered to the reader in both the parameters of the **Reply** message, again in different formats so that any manipulation may be detected by the reader. Upon decryption the reader checks for a match on the $ChInt$ and $ChTag$ and the $Handle$ now becomes a shared parameter that comprises both the tag and the reader challenges as,

$$Handle = L_8(ChInt) \| R_8(ChTag) \tag{9}$$

where $\|$ denotes concatenation.

Recently, Bagheri *et al.* [6] showed that the improved protocol presented in [5] suffers from the same man-in-the-middle attack as **Protocol 1**. In [5,6], the attack is considered as an man-in-the-middle attack. However, Kang *et al.* [7] pointed out that the attack of [5] comes from a misunderstanding regarding a communication parameter called $Handle$ and claimed that the attack is not a security threat. In the next Section, we analyze the practical effects of the man-in-the-middle attack in terms of a role of $Handle$ and link timing parameters.

# 3 Analysis of Attack Effects

## 3.1 Attack Effects

We analyze tag access operations and tag authentication under the man-in-the-middle attack. The first analysis is related to tag access operations. In the passive UHF RFID system, tags located within communication range of a reader can receive all access commands from the reader. Tags check whether the received *Handle* is the same as the *Handle* backscattered by them, and only a tag with the same *Handle* executes the access command. A Reader utilizes a *Handle* in the same manner for a tag access operation. In general, the reader and the tag use the same *Handle* value in the same session. It is, however, possible to use dual *Handle*s in a session. That is, all a tag needs to do is to check the *Handle* backscattered by itself and a reader has only to use the *Handle* received at step 12.

Figure 2 illustrates the procedures of the man-in-the-middle attack. Assuming that $E$ can intercept and replace the air interface data, it can replace the tag's $Handle \oplus k_8$ with $R_2$ at step 12. And, $E$ can relay an access command to $T$ and forward the tag's **Reply** to $R$ like Steps 13 and 14 in Fig. 2, respectively. It is, however, a real-time data injection over the radio rather than a man-in-the-middle attack. In the general man-in-the-middle attack, the role of $E$ in a tag access operation is to fake and forward data. In the case that someone can manipulate air interface data, he/she can perform the same operations as the man-in-the-middle attack without *Handle* manipulation. Steps 13 and 14 are the same situation as an attacker intervenes in tag-reader communication to change the payload into fake data over the radio.

Figure 3 is equivalent to Fig. 2. The practical effect of the man-in-the-middle attack is that **Protocol 1** utilizes the dual *Handle*s such as $Handle_T$ and $Handle_R$. The $Handle_T$ is the backscattered *Handle* which is the same as the *Handle* of step 12 in Fig. 2, and the $Handle_R$ is $R_2 \oplus k_8$ which is accepted by $R$. In other words, even though the man-in-the-middle attack manipulates the *Handle* between $T$ and $R$, it is practically only the dual *Handle*s. In addition, $E$ can neither decrypt the original ciphertext nor encrypt any of its own data because it has no session key. Furthermore, it is impossible to reuse the current fabricated information at other sessions or other tags because $E$'s intervention works only when a legitimate reader communicates with a legitimate tag in the current session. As a result, there is no meaning to $E$'s intervention using *Handle* manipulation. That is, the man-in-the-middle attack of [5] does not interfere with tag access operations, but is just a relay using the dual *Handle*s between a legitimate reader and a legitimate tag.

The second analysis is related to tag authentication. In the general man-in-the-middle attack, $R$ authenticates $E$ as $T$ when it receives the returned challenge number which is intercepted and replaced by $E$. However, in the man-in-the-middle attack of [5], despite a successful authentication, $E$ cannot send any data independently of a legitimate reader because it knows neither session key nor original *Handle*. The man-in-the-middle attack manipulates only the encrypted version of *Handle*. That is, there is no effect from fake authentication.

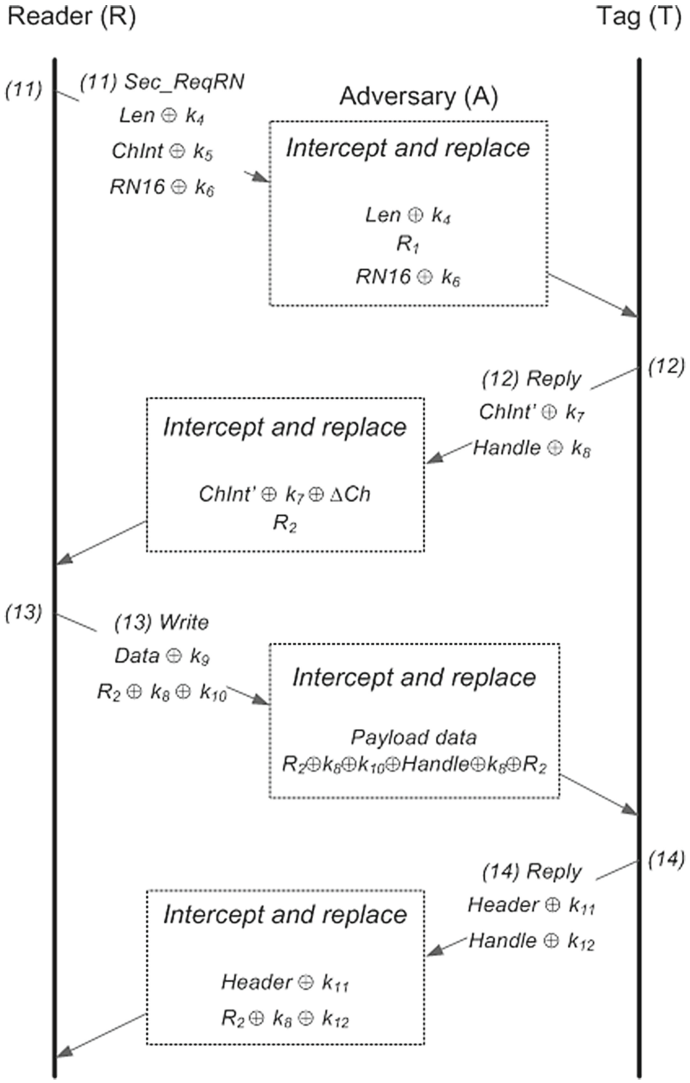

**Fig. 2.** Procedures of the man-in-the-middle attack on **Protocol 1**.

Furthermore, it does not matter whether $E$ intervenes in tag authentication procedure or not, because the fake authentication is successful only if the legitimate tag exists in the authentication procedure at the current session. It is no more than the authentication for the legitimate tag. As a result, the man-in-the-middle attack of [5] does not interfere with tag authentication.

### 3.2 Link Timing Analysis

ISO/IEC 18000-63 defines two link timing parameters related to single tag reply [2,8]. The first parameter, $T_1$, is the time from reader transmission to

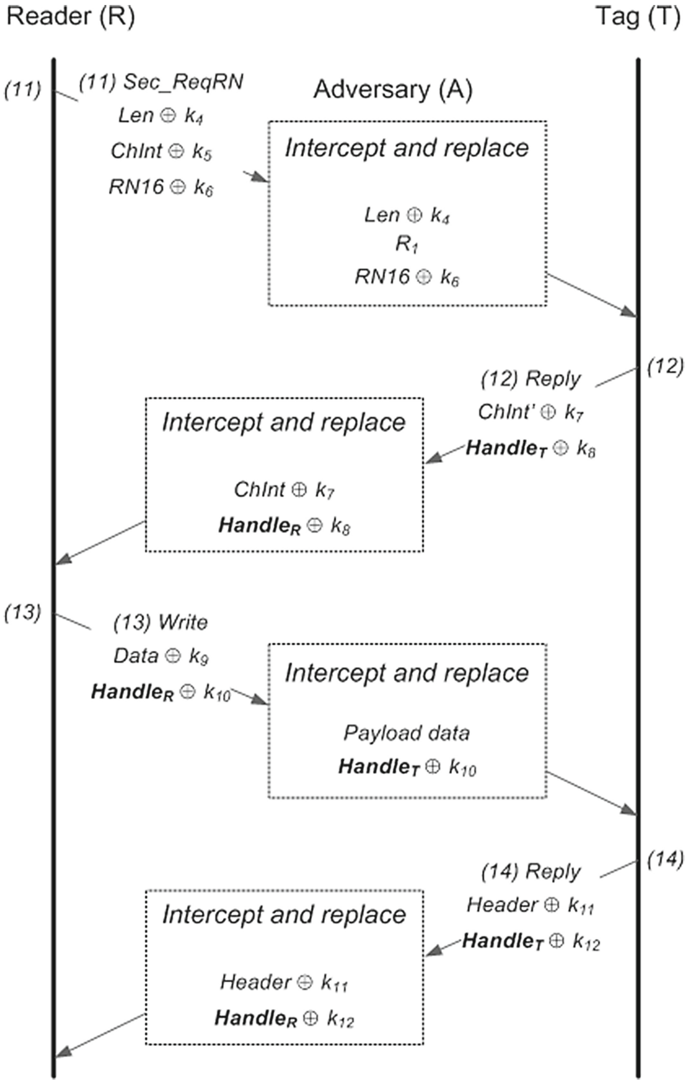

**Fig. 3.** Practical effect of the man-in-the-middle attack on **Protocol 1**.

tag response (specifically, the time from the last rising edge of the last bit of the reader transmission to the first rising edge of the tag response), measured at the tag's antenna terminals. That is, a reader starts a new session if it receives no reply from a tag in defined time. The nominal value of $T_1$ is MAX($RTcal$, $10 \cdot T_{pri}$), where, $RTcal$ is reader-to-tag calibration symbol and $T_{pri}$ is backscatter-link pulse-repetition interval. According to [2], the values for $RTcal$ and $T_{pri}$ are in the range of [15.625$\mu$s, 75$\mu$s] and [1.5625$\mu$s, 25$\mu$s], respectively. The second parameter, $T_2$, is the reader response time required if a tag is to demodulate the reader signal, measured from the end of the last bit of the tag response to the first falling edge of the reader transmission. That is, a tag transitions to the **arbitrate** state if $T_2$ expires. The value of $T_2$ is $3 \cdot T_{pri}$ to $20 \cdot T_{pri}$. (refer to [2] for notations and values.) Therefore, the $T_1$ time is $15.625\mu$s (= minimum $RTcal$) to $250\mu$s (= maximum $10 \cdot T_{pri}$), and the $T_2$ time is $4.6875\mu$s (= minimum $3 \cdot T_{pri}$) to $500\mu$s (= maximum $20 \cdot T_{pri}$). In other words, $E$ shall intercept, replace, and forward **Sec_ReqRN** of step 11 in $T_2$ time (at most, $500\mu$s) and **Reply** of step 12 in $T_1$ time (at most, $250\mu$s).

In Fig. 2, the minimum length of **Seq_ReqRN** is 35 bits (= $Len$ of 3 bits, $ChInt$ of 16 bits, and $RN16$ of 16 bits). The first action of $E$ is to intercept **Seq_ReqRN** over the radio. Assuming the maximum $T_2$ time (that is, $500\mu$s), $E$ needs a reader-to-tag data rate ($RTrate$) of 70 kbps (= 35 bits/$500\mu$s) in order to intercept **Seq_ReqRN** of step 11. In other words, if $RTrate$ is less than 70 kbps, the man-in-the-middle attack cannot work because the $T_2$ time expires during intercepting 35 bits data. Therefore, a simple countermeasure against the man-in-the-middle attack is to adjust the $RTrate$ to less than 70 kbps. Link timing-constrained condition is applied to **Reply** of step 12 in the same way. The minimum length of **Reply** is 32 bits (= $ChInt'$ of 16 bits and $Handle$ of 16 bits). Assuming the maximum $T_1$ time (that is, $250\mu$s), the required tag-to-reader data rate ($TRrate$) for intercepting **Reply** is at least 128 kbps (= 32 bits/$250\mu$s). Therefore, the man-in-the-middle attack cannot work if $TRrate$ is less than 128 kbps. According to [2], the $RTrate$ ranges between 26.7 kbps and 128 kbps and the $TRrate$ ranges between 5 kbps and 320 kbps in case of Miller encoding. The proposed threshold values of 70 kbps for $RTrate$ and 128 kbps for $TRrate$ exist in the allowable ranges. So, the proposed link timing countermeasure has no influence on the existing passive UHF RFID system.

## 4 Conclusion

In this paper, we have reviewed the man-in-the-middle attack on the RFID mutual authentication protocol of ISO/IEC 29167-6 WD and the subsequent countermeasure recently presented in [5]. After reviewing the attack scenario, we have analyzed practical security effects of the man-in-the-middle attack in terms of tag authentication service and link timing conformance. Our analysis shows that the attack does not interfere with tag access operations and tag authentication service, but is just a relay using the dual $Handle$s between a legitimate reader and a legitimate tag. We have also drawn the threshold values of 70 kbps for $RTrate$ and 128 kbps for $TRrate$ which can fundamentally protect the passive UHF RFID system from the data manipulation by any man-in-the-middle attack. We hope that our analysis helps the reader understand security features of the passive UHF RFID system.

**Acknowledgments.** This work was supported by the K-SCARF project, the ICT R&D program of ETRI [Research on Key Leakage Analysis and Response Technologies].

## References

1. EPCglobal Specification for RFID Air Interface, "Radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz - 960 MHz," version 1.0.9, January 2005
2. "ISO, IEC 18000–63, Information Technology - Automatic Identification, Data Capture Techniques - Radio Frequency Identification(RFID) for Item Management - Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C," International Organization for Standardization, February 2013
3. "ISO, IEC FDIS 29167–14, Information technology - Automatic identification, data capture techniques - Part 14: Crypto suite AES OFB security services for air interface communications," International Organization for Standardization, May 2015
4. "ISO, IEC WD 29167–6, Information technology - Automatic identification, data capture techniques - Part 6: Air interface for security services and file management for RFID at 860–960 MHz," International Organization for Standardization, August 2010
5. Song, B., Hwang, J., Shim, K.: Security improvement of an RFID security protocol of ISO/IEC WD 29167–6. IEEE Commun. Lett. **15**(12), 1375–1377 (2011)
6. Bagheri, N., Safkhani, M., Peris-Lopez, P., Tapiador, J.: Comments on "security improvement of an RFID security protocol of ISO/IEC WD 29167–6". IEEE Commun. Lett. **17**(4), 805–807 (2013)
7. Kang, Y., Choi, D., Park, D.-J.: Comments on an improved RFID security protocol for ISO/IEC WD 29167–6. J. ETRI **35**(1), 170–172 (2013)
8. Engels, D., Kang, Y., Wang, J.: On security with the new Gen2 RFID security framework. In: 7th IEEE International Conference on RFID, pp. 144–151. IEEE Press, New York (2013)