Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 891584, 8 pages
doi:10.1155/2012/891584

Research Article

Prevention and Detection Methods for Enhancing Security in an RFID System

Jing Huey Khor, Widad Ismail, and Mohammad Ghulam Rahman

Auto-ID Laboratory, School of Electrical and Electronic Engineering, Universiti Sains Malaysia (USM), 14300 Nibong Tebal, Penang, Malaysia

Correspondence should be addressed to Widad Ismail, eewidad@eng.usm.my

Received 27 April 2012; Accepted 29 June 2012

Academic Editor: An Liu

Low-cost radio frequency identification (RFID) tag is exposed to various security and privacy threats due to computational constraint. This paper proposes the use of both prevention and detection techniques to solve the security and privacy issues. A mutual authentication protocol with integration of tag's unique electronic fingerprint is proposed to enhance the security level in RFID communication. A lightweight cryptographic algorithm that conforms to the EPCglobal Class-1 Generation-2 standard is proposed to prevent replay attack, denial of service, and data leakage issues. The security of the protocol is validated by using formal analysis tool, AVISPA. The received power of tag is used as a unique electronic fingerprint to detect cloning tags. t-test algorithm is used to analyze received power of tag at single-frequency band to distinguish between legitimate and counterfeit tag. False acceptance rate (FAR), false rejection rate (FRR), receiver operating characteristic (ROC) curve, and equal error rate (EER) were implemented to justify the robustness of t-test in detecting counterfeit tags. Received power of tag at single frequency band that was analyzed by using t-test was proved to be able to detect counterfeit tag efficiently as the area under the ROC curve obtained is high (0.922).

1. Introduction

Radio frequency identification (RFID) tags that conform to EPC Class-1 Generation-2 (Gen 2) standards are broadly used in supply chain management, logistic, person identification, and access control. Global RFID market is expected to grow at a compound annual growth rate (CAGR) of roughly 17% to a value of approximately $9.7 billion in the period 2011–2013. However, the privacy and security of the usage of RFID technology are not guaranteed. The issues that raise security concerns are possibility of tag cloning issue, denial of service (DoS) attack, replay attack, and data leakage.

Gen 2 tags are susceptible to cloning attack due to lack of explicit authentication and security functionalities. Complex cryptographic algorithms, including hash function, and symmetric and asymmetric algorithms, are not supported by Gen 2 tags [1–3]. This is because Gen 2 tags have low-computation capabilities that are only able to support simple mathematical functions. Hence, strong adversaries are capable of skimming on transmission channels to obtain tag information [4]. This information may be used to create counterfeit tags that bear the same information as that of a legitimate tag. Counterfeit tags can be attached to bogus products and disguise these as authentic products in the market. The counterfeit tag issue is very serious because it is capable of causing a menace ranging from public privacy and safety issues to loss of industry revenues.

Lightweight cryptographic algorithm (i.e., CRC, PRNG, and XOR functions) can be used to prevent data leakage problem in Gen 2 tag. In addition, received power of tag can be used as tag's unique electronic fingerprint to detect counterfeit tags. Detection techniques are deployed to minimize the negative effects of tag cloning threats [5]. Counterfeit tags can be detected by employing the electronic fingerprinting system in an RFID system since each RFID tag is unique, based on their radio frequencies and manufacturing differences. Received power of tag at

single frequency band is analysed by using t-test to distinguish between legitimate and counterfeit tag. Hence, the combination of prevention and detection methods could be the countermeasure to the privacy and security issues being faced by Gen 2 tags.

The remaining of this paper is structured as follows: Section 2 describes the related works and Section 3 illustrates the overview of proposed lightweight cryptographic mutual authentication protocol. Section 4 outlines the experiment setup and data collection for fingerprint-matching method. Section 5 explains the t-test algorithm in details and Section 6 analyzes the accuracy and performance of fingerprint-matching method. Section 7 shows the overall security analysis and Section 8 concludes the paper.

Table 1: Notations used in the protocol.

Notation	Interpretation
E_T	Tag's electronic product code
Rn	Random number
CRC	Cyclic redundancy code
PRNG	Pseudorandom number generator
K_i	Current session key
K_{i+1}	New session key
K_t	Tag's temporary key
K_s	Server's temporary key
$\oplus$	XOR function
$\|\|$	Concatenation

2. Related Works

In Chien and Chen [2], PRNG, CRC, and XOR are used as the fundamentals in the protocol. Two sets of authentication and access keys are designed to defend DoS attack. However, the scheme is vulnerable to replay attack and information leakage. Chien and Huang [6] presented a lightweight mutual authentication protocol to solve replay attack and secret disclosure problem of Li et al. [7] scheme. But cloning attack problem is not resolved in this scheme. Song and Mitchell [8] proposed an authentication protocol that uses challenge-response approach and simple functions such as right and left shifts and bitwise XOR operation in the scheme. However, the scheme is vulnerable to tag impersonation attack and server impersonation attack. Song [9] presented an authentication protocol for tag ownership transfer that meets new owner privacy, old owner privacy, and authorization recovery requirements. However, the ownership transfer protocol is vulnerable to a desynchronization attack that prevents a legitimate reader from authenticating a legitimate tag, and vice versa. Burmester and Munilla [10] proposed a lightweight mutual authentication protocol that supports session unlinkability, forward and backward secrecy. The protocol is optimistic with constant key lookup, and can easily be implemented on a Gen 2 platform. However, the scheme is susceptible to replay and cloning attacks. Chen and Deng [11] proposed mutual authentication protocol that is able to reduce database loading and ensure user privacy. But the authentication protocol did not take into consideration cloning attack issues.

In [12], minimum power responses measured at multiple frequencies are used as unique electronic fingerprint. The power is measured at the range from 860 MHz to 960 MHz in increments of 1 MHz. Two-way analysis of variance (two-way ANOVA) is used to test the equality of means of two groups in terms of minimum power response and different physical characteristic of tags. 10-fold cross-validation on the classifier is used to validate the result obtained, and the AUC is 0.999. The average true positive rate and false positive rate are 0.905 and 0.001, respectively. The research focused on using minimum power responses at multiple frequencies as a unique electronic fingerprint for RFID tags. Hence, this paper extends the idea to show that received power of tag at single frequency band can be used to fingerprint RFID tags. Physical-layer identification of passive UHF RFID tags from three different manufacturers is analyzed in [13]. RFID reader that is capable to simulate an inventory protocol is built to activate tags. RF signal features are extracted from the preambles of tags' replies. Time domain and spectral features of the collected signals are analyzed. The tags can be classified with an accuracy of 71.4% from different locations and distances to the reader based on the time domain features. In addition, UHF RFID tag that is proved can be uniquely identified in controlled environment based on the signal spectral features with 0% of EER. The physical-layer identification method is complex, and the reader used in conducting the experiment is purposely built. In contrast, the proposed method in this paper is simple and applicable to any Gen 2 reader.

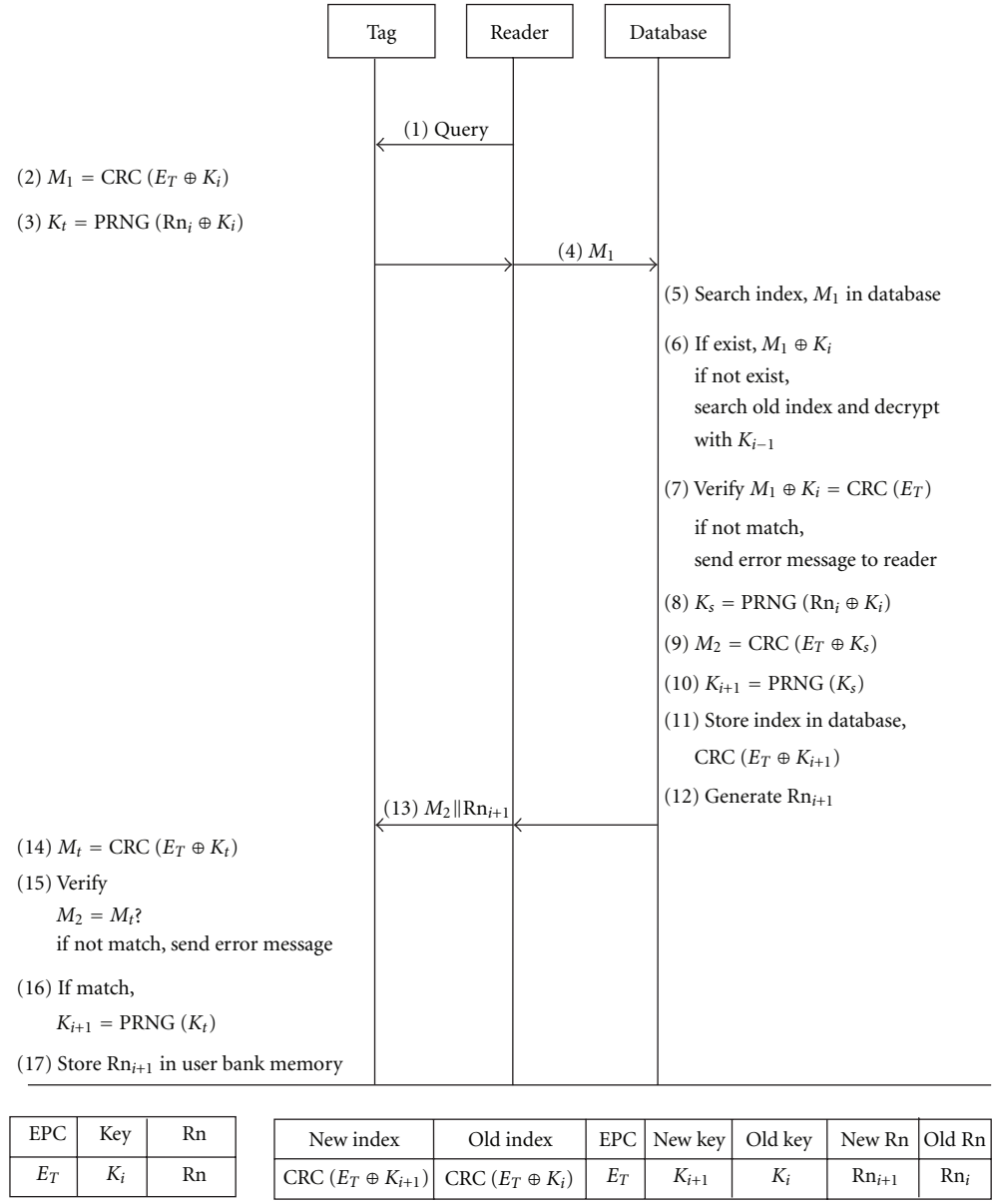
3. Lightweight Cryptographic Mutual Authentication Protocol

A lightweight cryptographic mutual authentication protocol that conforms to Gen 2 standards is proposed. The proposed protocol consists of initialization phase and authentication phase. The channel between a back-end server and a reader is assumed secure. On the other hand, the channel between a reader and a tag is assumed insecure.

The notations used in the description of proposed protocol are shown in Table 1.

In the initialization phase, a back-end server and tag store information are required to perform authentication. The back-end server initially stores seven values of each tag in its database. These are new index denotes as CRC ($E_T \oplus K_{i+1}$), old index denotes as CRC ($E_T \oplus K_i$), tag's electronic product code denotes as E_T, new session key denotes as K_{i+1}, old session key denotes as K_i, new random number denotes as Rn_{i+1}, and old random number denotes as Rn_i. On the other hand, three values that are stored in the tag are E_T, K_i, and Rn_i. Session key of current session is denoted as K_i, and the session key after a successful session is denoted as K_{i+1}. The tag's temporary key is denoted as K_t, and server's temporary key is denoted as K_s. The overall protocol scheme is shown in Figure 1.

In authentication phase, the reader will send query command to the tag. The tag computes $M_1 = \text{CRC}(E_T \oplus K_i)$.



EPC	Key	Rn
E_T	K_i	Rn

New index	Old index	EPC	New key	Old key	New Rn	Old Rn
CRC ($E_T \oplus K_{i+1}$)	CRC ($E_T \oplus K_i$)	E_T	K_{i+1}	K_i	Rn_{i+1}	Rn_i

Figure 1: Lightweight cryptographic mutual authentication protocol.

At the same time, PRNG generates tag's temporary key, K_t, based on the seed number, $\mathrm{Rn}_i \oplus K_i$. The encrypted message, M_1, is sent via the reader to the back-end server. The back-end server searches for an index, CRC ($E_T \oplus K_i$), in its database that is matching with the encrypted message. If matching index is found, the encrypted message is decrypted using the session key, K_i, that is in the same row as indicated by index. Otherwise, the server searches the matching of M_1 with the old index, CRC ($E_T \oplus K_{i-1}$). If the matching of old index is found, old session key, K_{i-1}, is used to decrypt the message. The authentication of the message is then verified. If the decrypted message does not match the message recorded in the database for both new and old indexes, an error message will be sent to the reader. On the other hand, if the server successfully authenticates the tag, a server's temporary key, K_s, is generated. If the M_1 is decrypted with old index, then K_s is generated by XOR K_{i-1} and Rn_{i-1} as a seed. Then, the back-end server computes M_2 = CRC ($E_T \oplus K_s$). A new session key, K_{i+1}, is generated, and CRC ($E_T \oplus K_{i+1}$) is computed and updated as a new index in the database. In addition, a new random number, Rn_{i+1}, is generated and concatenates with M_2. The new session key and random number are stored in the row that indicated by the new index. Afterwards, the back-end server forwards $M_2 \| \mathrm{Rn}_{i+1}$ to the tag through the reader. The tag computes M_t = CRC ($E_T \oplus K_t$), and the authentication of the reader is verified by the tag where a comparison of M_2 and M_t is made. If both messages are matched, then the tag will update a new session key, K_{i+1}, where K_{i+1} = PRNG (K_t). Otherwise, the key will be maintained as current session key, K_i. The tag stores the

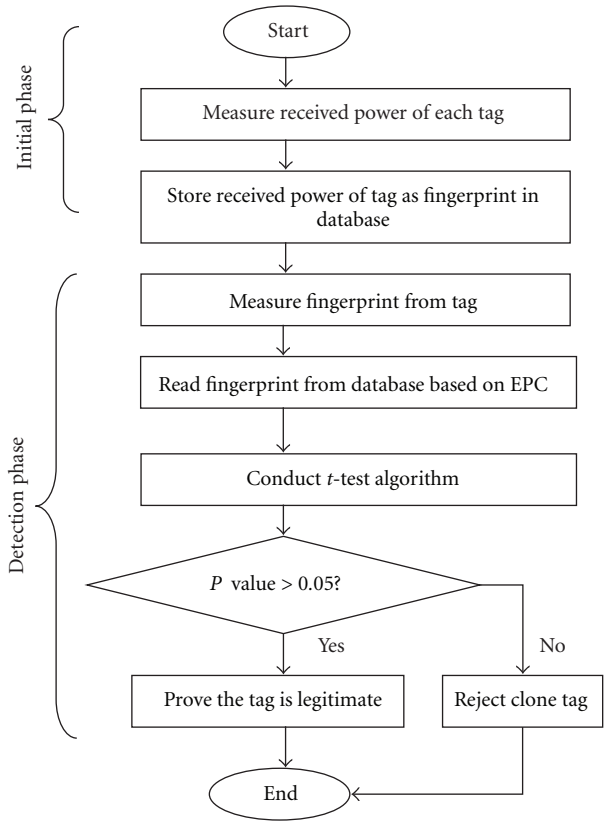


Figure 2: Overall process of fingerprint-matching method.

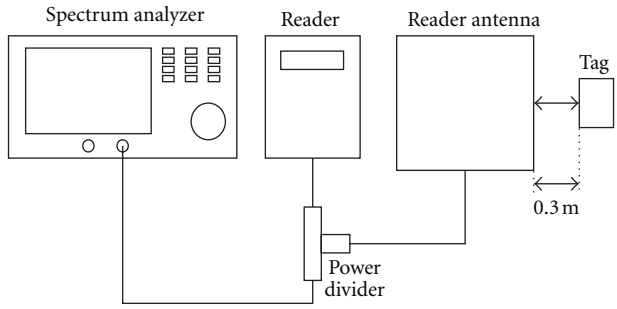


Figure 3: Measurement of received power of tag platform.

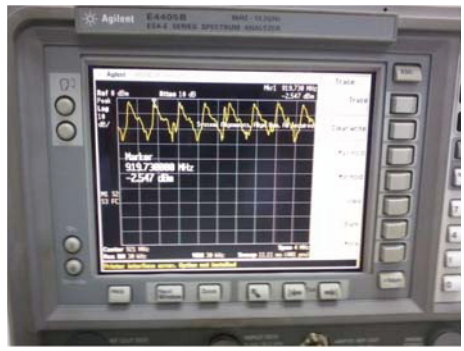


Figure 4: Reader transmitted power measured with spectrum analyzer.

received Rn_{i+1} in the user memory bank for the usage in the next session.

4. Experimental Setup and Fingerprint Data Collection

The proposed RFID tag fingerprint-matching method illustrated in Figure 2 consists of initial phase and detection phase. In the initial phase, received power of each EPC tag is calculated using Friis transmission equation. Reader transmitted power used in the equation is measured using a spectrum analyzer. The received power is measured once the power is held constant. Each tag received power is stored in database. In the detection phase, stored fingerprint and measured fingerprint are compared using t-test algorithm. The tag being measured is proved to be a legitimate tag if P value of t-test algorithm is greater than 0.05. Otherwise, the tag is proved to be a counterfeit tag.

The received power of tag is calculated based on the reader's transmitted power, which is measured at 919–923 MHz. The frequency band is used based on the Malaysian UHF RFID standard governed by Malaysian Communications and Multimedia Commission (MCMC) [14]. However, the measurement is still applicable to other countries, RFID frequency band. The transmitted power of tag is measured for 100 passive RFID tags at fixed temperature and controlled environment. The legitimate tag fingerprint template is determined by obtaining the average received power of 50 readings per tag. The received power that acts as a unique fingerprint for each tag is measured in dBm. The received power is stored in the database only in order to protect the secrecy of fingerprint value from being obtained by adversaries. The unique fingerprint value that stored in the database can be searched based on the EPC. Hence, the stored fingerprint value in database and measured fingerprint value that obtained from experimental measurement can be compared to verify the genuineness of the tag.

Figure 3 shows the measurement of reader transmitted power platform. The setup consists of a passive RFID reader and antenna, passive EPC tag, and spectrum analyzer. The reader operates at UHF 919–923 MHz and supports Gen 2 protocol. The antenna and tag are placed at fixed position to obtain an accurate and reliable result. To determine precise reader transmitted power, cable loss and power loss within the power splitter must be considered. Hence, power value obtained from the spectrum analyzer is added to the total power loss measured to obtain an accurate reader transmitted power. Figure 4 shows a measurement of reader transmitted power using spectrum analyzer.

The tag received power is calculated using Friis transmission equation, as demonstrated in

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi r}\right)^2, \quad (1)$$

where P_r is the power received by the tag antenna and P_t is the power input to the reader antenna. In addition, G_t is the

Table 2: Notations used in the Protocol.

Parameters	Value
Gain of reader antenna	6 dBi
Gain of tag antenna	2.15 dBi
Gain of reader antenna in power ratio, G_t	3.981
Gain of tag antenna in power ratio, G_r	1.641
Frequency, f	919.73 MHz
Wavelength, λ	0.33 m
Distance between reader and tag antennas, R	0.3 m

Table 3: t-test for Tag A and suspicious tag.

	Tag A	Suspicious tag
Mean	0.167092	0.316192
Variance	0.0492	0.07446
Observations	50	5
Pooled Variance	0.05117	
Hypothesized Mean Difference	0	
df	53	
t Stat	−1.40613	
$P(T \le t)$ one tail	0.082761	
t Critical one-tail	1.674116	
$P(T \le t)$ two-tail	**0.165522**	
t Critical two-tail	2.005746	

antenna gain of the reader antenna, G_r is the antenna gain of the tag antenna, λ is the wavelength, and R is the distance between reader and tag antennas. Friis transmission equation is only applicable in Fraunhofer region. Hence, a minimum Fraunhofer region is determined by using

$$r_{ff} = \frac{2D^2}{\lambda}, \tag{2}$$

where, r_{ff} is the minimum far field distance, D is the diameter of transmitting antenna, and λ is the wavelength. The diameter of transmitting antenna is 0.185 m, and the wavelength is 0.33 m because the frequency chosen is 919.73 MHz. Hence, the minimum far field distance is 0.21 m. The tag should be placed at a distance greater than 0.21 m such that it is in the Fraunhofer region. In this setup, the distance between the tag and reader antenna is 0.3 m in order to satisfy Fraunhofer region condition. Parameters used in the measurement are shown in Table 2.

5. t-test Algorithm

Cloning tags may be detected by comparing extracted received power and stored fingerprint using t-test algorithm, as illustrated in

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{{S_p}^2((1/N_1) + (1/N_2))}},$$
$$S_p{}^2 = \frac{(N_1 - 1){S_1}^2 + (N_2 - 1){S_2}^2}{N_1 + N_2 - 2}, \tag{3}$$

Table 4: t-test for Tag B and suspicious tag.

	Tag B	Suspicious tag
Mean	−0.30055	0.316192
Variance	0.051325	0.07446
Observations	50	5
Pooled Variance	0.053072	
Hypothesized Mean Difference	0	
df	53	
t Stat	−5.70766	
$P(T \le t)$ one tail	2.6E−07	
t Critical one-tail	1.674116	
$P(T \le t)$ two-tail	**5.26E−07**	
t Critical two-tail	2.005746	

where $\overline{X_1}$ and $\overline{X_2}$ are the means of legitimate and suspicious tag groups, N_1 and N_2 are the number of samples for legitimate and suspicious groups, respectively, and $S_p{}^2$ is the pooled variance. t-test algorithm is a statistical test used to identify differences in the means and variances of two populations, namely, legitimate tag and suspicious tag populations. Significant level equals to 0.05 is chosen in conducting the t-test in order to verify the probability of a false rejection. The tag used can be considered as counterfeit if P value obtained from t-test is less than significant level, 0.05. The tag is proved as counterfeit tag because the matching probability between stored fingerprint and measured fingerprint is less.

When a tag is suspected to be counterfeit, comparison of stored and measured tag's fingerprint experiment needs to be conducted. In Case 1, a suspicious tag claims to belong to Tag A based on the stored fingerprint. As demonstrated in Table 3, P value obtained from the t-test within Tag A and the suspicious tag is higher than 0.05. This proves that no significant difference exists between the suspicious tag and Tag A. Hence, the suspicious tag is a legitimate tag. The higher the P value is, the more likely that the two groups will match. Otherwise, the tag is proved to be a counterfeit one. In Case 2, a suspicious tag claims to belong to Tag 4. A t-test is conducted between the suspicious tag and Tag B. The P value obtained from Table 4 is less than 0.05. Hence, the suspicious tag from Case 2 is proved to be a counterfeit.

6. Fingerprint-Matching Performance Analysis

The accuracy of proposed fingerprint-matching method in distinguishing between legitimate and counterfeit tags as shown in Case 2 is analyzed by using FAR, FRR, ROC, and EER. A 2 × 2 contingency table is used to verify four outcomes from the data obtained from Case 2. The outcome is a true acceptance (TA) when measured fingerprint is verified as a genuine value and the tag identity is found in the database. When the measured fingerprint has genuine value but the tag identity is not found in the database, the outcome is false acceptance (FA). Conversely, true reject (TR) is obtained when measured fingerprint has bogus value and the tag identity is not found in the database. False reject

Table 5: Four outcomes from fingerprint matching method.

		Existence of measured fingerprint in database	
		Yes	No
Genuineness of measured fingerprint	Yes	True acceptance (TA) 50	False acceptance (FA) 2
	No	False reject (FR) 0	True reject (TR) 48

Table 6: FAR and FRR for Case 2.

Measurement	Percentage (%)
FAR	4
FRR	0

Table 7: Accuracy of test categorization.

AUC range	Categories
0.50–0.60	Failure
0.60–0.70	Poor
0.70–0.80	Fair
0.80–0.90	Good
0.90–1.00	Excellent

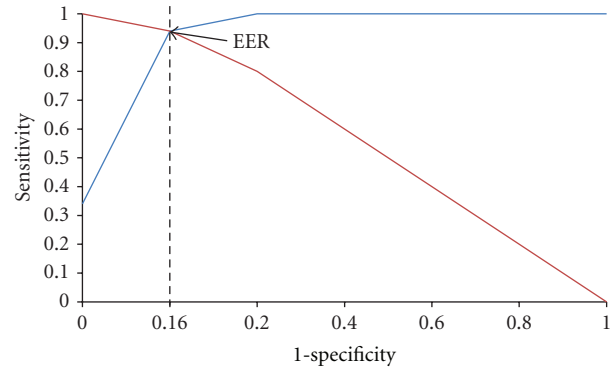


Figure 5: Receiver operating curve with equal error rate.

(FR) is obtained when measured fingerprint is verified as a bogus value but the tag identity is found in the database. Table 5 illustrates four outcomes obtained from fingerprint-matching method for Case 2.

False acceptance rate (FAR) is the measurement of probability in which the fingerprint-matching method falsely verifies different tags as identical. False rejection rate (FRR) is the measurement of probability in which the fingerprint-matching method falsely verifies identical tags as different. FAR and FRR are calculated using (4) and (5), respectively [15],

$$\text{FAR} = \frac{\text{FA}}{\text{FA} + \text{TR}}, \tag{4}$$

$$\text{FRR} = \frac{\text{FR}}{\text{FR} + \text{TA}}. \tag{5}$$

FAR and FRR for Case 2 are shown in Table 6.

ROC curve and EER are used to evaluate the performance of t-test algorithm in verifying measured fingerprint with stored fingerprint. ROC curve illustrated in Figure 5 plots the true acceptance rate (TAR) versus its false acceptance rate (FAR). EER is the rate at which both FAR and FRR are equal. Based on the ROC curve, EER for Case 2 is 0.16, which is considered as a low value. The lower the EER is, the more accurate will be the fingerprint-matching method.

The area under curve (AUC) of the ROC curve is a measurement of the performance of t-test algorithm in distinguishing between two fingerprint data sets. The accuracy of the t-test algorithm is verified using a rough guide for classifying the accuracy of a test as shown in Table 7 [16, 17].

AUC for Case 2 that obtained from SPSS statistical analysis result is 0.922 as shown in Table 8, which is considered an excellent performance according to the accuracy guide. This proves that the t-test algorithm offers high accuracies in distinguishing fingerprints between data sets of two tags.

7. Security Analysis

The security of proposed protocol that is written in HLPSL is validated using AVISPA tool. The intruder under the Dolev-Yao model has capability to full control over the network [18]. The intruder may intercept and analyze transmitted message as well as impersonate one of the agents (tag, reader, and server) to send modified message to others. Data secrecy and mutual authentication are the security goals that needed to achieve in AVISPA tool. The E_T as well as session keys K_i and K_s are kept secret in the transmission channel. An attack is considered happened if intruder is able to obtain any secret values. In addition, tag and back-end server are only allowed to reveal their identity information to the authorized parties. Back-end server needs to ensure that the current session's message, M_1, is the message that computed by legitimate tag. This is to prevent replay attack where intruder sends previous session's message to the legitimate reader. Same case is applied to M_2. The authentication of M_2 must be verified by the tag as a legitimate message that sent by the legitimate reader. Figure 6 shows that OFMC and CL-AtSe back-ends found no man-in-the-middle attacks and the stated security goals were satisfied for a bounded number of sessions as specified in environment role. The strong authentication between the tag and back-end system is established and the secrecy of the EPC and session keys are protected from eavesdropping. The analysis using SATMC and TA4SP on the proposed protocol is inconclusive because the back-ends only support protocols that are free of algebraic equation.

Replay attack can be prevented in this proposed protocol because the value transmitted for each session is different. The proposed protocol is a challenge-response

Table 8: Accuracy of test categorization.

Area	Std. error[a]	Asymptotic sig.[b]	Asymptotic 95% confidence interval	
			Lower bound	Upper bound
0.922	0.027	0.000	0.869	0.975

[a]Under the nonparametric assumption.
[b]Null hypothesis: true area = 0.5.

Table 9: Comparison between schemes.

Scheme	Replay attack	DoS attack	Cloning attack	Forward security	EPC Class-1 Gen-2
Chien and Chen [2]	X	O	X	X	O
Chien and Huang [6]	O	O	X	O	O
Song and Mitchell [8]	X	O	X	X	X
Song [9]	O	X	X	O	X
Burmester and Munilla [10]	X	O	X	O	O
Chen and Deng [11]	O	O	X	O	O
Proposed Scheme	O	O	O	O	O

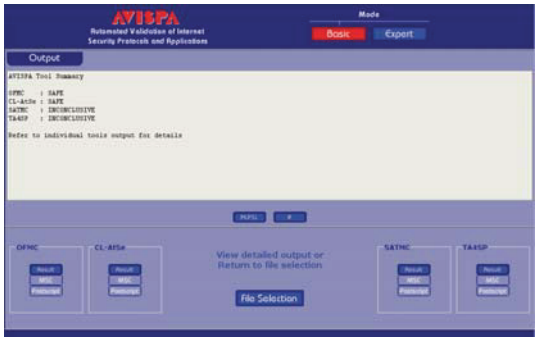


Figure 6: AVISPA validation result.

mutual authentication protocol that is based on one-time pad encryption. Hence, different value of session key is utilized in individual session and PRNG plays a vital role in providing different value of session key to encrypt with E_T. A random number, n, is XOR with K_i to use as a seed of the PRNG. The seed is regenerated for each session to reduce the possibility of successfully cracked by adversaries. For each session, M_1 and M_2 are enciphered by using corresponding session keys, K_i and K_s by the tag and server respectively. These session keys are synchronously updated during mutual authentication by both tag and server. Hence attacker is unable to use the session keys, K_i and K_s, of a particular session to decipher encrypted message for any of the following sessions.

DoS attack can be defended by using updated session key. The legitimate tag can be identified by verifying the encrypted message with message recorded in the database. On the other hand, the authentication of the reader is verified by the tag by comparing the decrypted message with message recorded in the tag. Both new and old indexes, session keys, and random numbers that are stored in the back-end server are used to prevent desynchronized issue. Desynchronization problem occurred when variables stored in the tag are different with the one stored in the database. Hence, the server can use old variables to resynchronize with the tag.

The secrecy of the tag's information is safe from eavesdropping attack. The E_T is enciphered with session key where the session key will be updated after each complete session. In addition, tag is hard to compromise because M_1 and M_2 are enciphered by using different key. If M_1 and M_2 are eavesdropped between legitimate tag and reader, the attacker is unable to obtain any secret information. For example, $M_1 \oplus M_2 = [\text{CRC}\ (E_T \oplus K_i)] \oplus [\text{CRC}\ (E_T \oplus K_s)] = [\text{CRC}\ (E_T \oplus E_T \oplus K_i \oplus K_s)] = [\text{CRC}\ (0 \oplus K_i \oplus K_s) = \text{CRC}\ [(0 \oplus K_i \oplus K_s)]$. Hence, attacker is only able to get enciphered key and is impossible to guess its original key value.

The proposed protocol can prevent the issue of cloning tags by using fingerprint information stored in the database to detect counterfeit tags. Each tag has it own unique received power of tag value. Even though adversaries are able to copy all the data from a tag, they are unable to create a counterfeit tag that has the exact same physical feature as original tag. Thus, any counterfeit tag can be found when the fingerprint of tag detected is not matched with the fingerprint information stored in the tag. The proposed method is analyzed by using one factor only, which is received power of tag at single frequency, whereas two factors, namely, minimum power responses at multiple frequencies and physical characteristic of tags, are tested by using ANOVA in [12]. The accuracy of the proposed method and method of [12] is excellent in both, with the values of 0.922 and 0.999, respectively. The proposed method is simpler but capable to produce comparable accuracy of method [12] which analyses two factors to detect cloning tags.

Table 9 indicates a comparison of results between proposed scheme and related security schemes in terms of replay attack, DoS attack, cloning attack, forward secrecy, and Gen 2 standards compliance. The proposed lightweight

cryptographic mutual authentication protocol is proved to possess more security protection compared to existing security schemes.

8. Conclusions

This paper proposed the use of both prevention and detection methods to enhance the security level in an RFID system. The lightweight cryptographic mutual authentication protocol that consists of lightweight cryptographic algorithm, including XOR, CRC, and PRNG functions, is used as prevention method. The security of proposed protocol is validated using AVISPA tool and is proved safe from replay attack, denial of service threats, and data leakage problem.

In addition, tag's fingerprint extraction and matching method is presented as a detection method in detecting counterfeit tags. Each tag received power is measured, calculated, and stored in the database for further reference. Tag received power can be used as unique fingerprint as these are significantly different in the frequency range of 919–923 MHz. t-test algorithm is used to determine the identity of measured tag. Measured tag is proved as counterfeit if the P-value of the t-test conducted is less than 0.05. Accuracy of the fingerprint-matching method is tested, and 4% of FAR and 0% of FRR is achieved. In addition, fingerprint-matching is proved to be an excellent method, as the area under the ROC curve is 0.922 and ERR is 0.16. Hence, t-test algorithm was proved to be able to protect RFID communication system from tags cloning attack by efficiently distinguishing between legitimate and counterfeit tags.

Acknowledgments

The authors would like to thank the School of Electrical and Electronic Engineering, USM and the USM RU (Research University) grant secretariat, for sponsoring this work.

References

[1] D. Bailey and A. Juels, "Shoehorning security into the EPC tag standard," in *Proceeding of Security and Cryptography for Networks*, pp. 303–320, Berlin, Germany, 2006.

[2] H. Y. Chien and C. H. Chen, "Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards," *Computer Standards and Interfaces*, vol. 29, no. 2, pp. 254–259, 2007.

[3] M. Bouet and G. Pujolle, "RFID in eHealth systems: applications, challenges, and perspectives," *Annals of Telecommunications*, vol. 65, no. 9-10, pp. 497–503, 2010.

[4] A. Razaq, W. T. Luk, K. M. Shum, L. M. Cheng, and K. N. Yung, "Second-generation RFID," *IEEE Security and Privacy*, vol. 6, no. 4, pp. 21–27, 2008.

[5] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of RFID devices," in *Proceedings of the USENIX Security Symposium*, pp. 199–214, 2009.

[6] H. Y. Chien and C. W. Huang, "A lightweight authentication protocol for low-cost RFID," *Journal of Signal Processing Systems*, vol. 59, no. 1, pp. 95–102, 2010.

[7] Y. Z. Li, Y. B. Cho, N. K. Um, and S. H. Lee, "Security and privacy on authentication protocol for low-cost RFID," in *Proceedings of the International Conference on Computational Intelligence and Security (ICCIAS '06)*, pp. 1101–1104, October 2006.

[8] B. Song and C. J. Mitchell, "RFID authentication protocol for low-cost tags," in *Proceedings of the 1st ACM Conference on Wireless Network Security (WiSec '08)*, pp. 140–147, April 2008.

[9] B. Song, "RFID tag ownership transfer," in *Proceedings of the 4th Workshop on RFID Security*, Budaperst, Hungary, 2008.

[10] M. Burmester and J. Munilla, "A flyweight RFID authentication protocol," in *Proceedings of the 4th Workshop on RFID Security*, Budaperst, Hungry, 2008.

[11] C. L. Chen and Y. Y. Deng, "Conformation of EPC Class 1 Generation 2 standards RFID system with mutual authentication and privacy protection," *Engineering Applications of Artificial Intelligence*, vol. 22, no. 8, pp. 1284–1291, 2009.

[12] S. C. G. Periaswamy, D. R. Thompson, and D. Jia, "Fingerprinting RFID tags," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 938–943, 2011.

[13] D. Zanetti, B. Danev, and S. Căpkun, "Physical-layer identification of UHF RFID tags," in *Proceedings of the 16th Annual Conference on Mobile Computing and Networking (MobiCom '10)*, pp. 353–364, September 2010.

[14] MCMC, "Strategies for a National RFID Roadmap for The Next Five Years," 2010.

[15] J. Zhou, H. Shirai, I. Takahashi, J. Kuroiwa, T. Odaka, and H. Ogura, "A Hybrid Command Sequence Model for Anomaly Detection," in *Proceeding of 11th Pacific-Asia Conference on Knowledge Discovery and Data Mining*, Nanjing, China, 2007.

[16] Y. Kutlu and D. Kuntalp, "A multi-stage automatic arrhythmia recognition and classification system," *Computers in Biology and Medicine*, vol. 41, no. 1, pp. 37–45, 2011.

[17] C. J. Chevillotte, M. H. Ali, R. T. Trousdale, D. R. Larson, R. E. Gullerud, and D. J. Berry, "Inflammatory laboratory markers in periprosthetic hip fractures," *Journal of Arthroplasty*, vol. 24, no. 5, pp. 722–727, 2009.

[18] Avispa, "HLPSL Tutorial—A Beginner's Guide to Modeling and Analyzing Internet Security Protocols," 2006.