Enhancing the Security of RCIA Ultra-Lightweight Authentication Protocol by Using Random Number Generator (RNG) Technique

Shaymah Akram Yasear, Nur Haryani Zakaria, and Mohd. Nizam Omar
School of Computing, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia.
shayma1985akram@gmail.com

***Abstract*—This study is an attempt to enhance the security of Robust Confidentiality, Integrity, and Authentication (RCIA) ultra-lightweight authentication protocols. In the RCIA protocol, IDs value is sent between reader and tag as a constant value. This makes RCIA susceptible to traceability attack which lead to the privacy issue. In order to overcome this problem, Random Number Generator (RNG) technique based on Bitwise operations has been used in the tag side. The idea of this technique is to change the IDs of a tag on every query session so that it will not stay as a constant value. The implementation of Enhanced RCIA has been conducted by using a simulation. The simulation provided the ability to show that the operations of RCIA protocol as to compare with the enhanced RCIA. The outcome shows that the enhanced RCIA outperforms existing one in terms of privacy.**

***Index Terms*—RCIA; Ultra-Lightweight Protocol; Authentication; Random Number; Technique; Traceability; Attack.**

I. INTRODUCTION

Radio frequency identification (RFID) is a non-contact automatic identification technology uses radio waves to achieve the object identification and data exchange. The RFID system consist of tag which wirelessly communicate with the reader and back-end database stores items of the tag.

The nature of communication in the RFID system makes it susceptible to a wide range of attacks. One of them is the attack that affects the communication channel between reader and tag. Therefore, the authentication protocols which were applied in this system are very important. Depending on the level of complexity of the operations it carried out, the RFID classification of authentication protocols can be divided into four different classes.

The first class is full-fledged authentication protocol which allows application classics cryptographic functions such as symmetric encryption, public and private key and one-way hash functions. The second one, simple authentication protocol which supports the generation of random numbers and hash functions. The third category is a lightweight authentication protocol that supports random number generator, simple functions such as Cyclic Redundancy Code (CRC) and simple bitwise operations (hash function is not included). The last one is ultra-lightweight authentication protocol can support simple bitwise operations (XOR, AND and OR) [1].

II. PRIVACY ISSUE OF ULTRA-LIGHTWEIGHT AUTHENTICATION PROTOCOL

This study aims to enhance the security of ultra-lightweight authentication protocol. Therefore, the related work introduced in this section, only focus on these protocols. Several studies reviewed and evaluated the security issues of RFID ultra-lightweight authentication protocols. In these studies, high level of vulnerabilities was detected. These vulnerabilities include, common threats, such as desynchronization and DoS attack, in addition to, tracking the location of the tag.

In 2006, Peris-Lopez et al. proposed an Ultra-Lightweight Mutual Authentication Protocol family (UMAP). This family includes two protocols which are: Lightweight Mutual Authentication Protocol (LMAP) [2] and Efficient Mutual Authentication Protocol (EMAP) [3]. The analysis of UMAP family, pointed out that the protocols vulnerable to malicious attacks. In 2008, Li and Wang [4] proposed two attacks (desynchronization and full disclosure) on LMAP and EMAP and successfully refute security claims of both protocols. In these protocols, the previous IDs value was not stored in the reader. If the attacker interrupts the communication among reader and tag, and block D message, the tag will update its values while the reader will not and it will remain using its previous values. In this case, in the next query from reader to tag, the tag will respond with its current IDs which is quite different from the IDs stored in the reader. As a result of that, the tag will become useless. This indicates that the UMAP protocols cannot prevent desynchronization and disclosure attack.

Furthermore, UMAP can neither resist disclosure nor de-synchronization and cannot resist traceability attack. In UMAP, since the eavesdropper can pretend to be legitimate reader, when the reader sends a query to the tag, the eavesdropper gets the response with IDs. In the next query, when the legitimate reader sends a request, the tag will respond with same IDs, so that UMAP cannot resist traceability attacks. In 2007, Chien[1] proposed the Strong Authentication and Strong Integrity (SASI) protocol. This protocol reported in [5]-[7], their findings provide confirmatory evidence that SASI has several vulnerabilities such as desynchronization and secret disclosure attacks. In 2011, a successful desynchronization attack was shown on SASI protocol [7]. Thus, in 2013, Avoine, Carpent & Martin proposed a successful passive full-disclosure attack [8]. In 2009, a new ultra-lightweight authentication protocol called (Gossamer) was proposed [9]. This protocol proposed as an

extension to SASI protocol to overcome its weakness [10]-[11]. Although this protocol shown resistance to a passive full disclosure attack, nevertheless, the desynchronization and Denial of Service (DOS) attacks still exist in this protocol [12]-[13]. The operations of Gossamer protocol are similar to other previously proposed protocols, except that, in Gossamer, they add two new functions; Double Rotation and MixBits [9]. In 2012, Zubair, Mujahid and Ahmed [14] improved the performance of Gossamer protocol by proposed a counter based methodology. Combination this counter in Gossamer protocol makes it resilient against DOS and desynchronization attacks. In 2009, David and Prasad [15] presented a new ultra-lightweight authentication protocol based on Bitwise operations. This protocol uses only two Bitwise logical operations AND and XOR, which contributed to reduce computational power at tag side. In David-Prasad protocol, reader needs to get one-day certificate from CA (Certificate Authority) before inquiring the tag. Reader initiates the protocol by sending "Hello" message to the tag. Tag then responds with its current IDs, reader matches this IDs with IDs stored in the back-end database; if a match found, it will produce two random numbers (n1, n2), calculate and send (A, B and D) to the tag. However, in 2010, a group of researcher [16] proposed full disclosure attack (Tango) on the David-Prasad protocol. Tango attack requires GA (good approximations) equations based on hamming distance with unknown variable. Later on, Barrero, Hernández-Castro, Peris-Lopez and Camacho [17] presented genetic tango attack to improve Tango attack and later on, resolved the exhaustive searching of GA equations. In 2012, a new ultra-lightweight authentication protocol called RFID authentication protocol with permutation (RAPP) was proposed [10]. Unlike previous protocols, this protocol relied on the new technique. In this protocol the tag has the ability to perform three simple functions: Bitwise XOR operation, left rotation Rot(), and Per() function. All these functions are cheap to implement in the tag [10]. However, in 2012, a group of researcher highlighted two attacks on RAPP, desynchronization and traceability attack [18, 19]. Avoine & Carpent (2013) indicated that, the protocol RAPP- contrary to the claim of its designers -prone to desynchronization attack18. In 2013, Ahmadian, Salmasizadeh & Aref [20], launched a desynchronization attack on this protocol and highlighted the poor composition of RAPP messages. In the same year, Shao-hui, Zhijie, Sujuan and Dan-wei [19] highlighted some weaknesses of the newly proposed permutation function [12], which can be easily exploited to uncover secrets in the tag.

In 2015, robust confidentiality, integrity, and authentication (RCIA) protocol has been proposed [21]. The RCIA protocol [21] was able to solve some of the weaknesses in the previous protocols, such as desynchronization and full disclosure attack, by introducing and using a new ultra-lightweight primitive Recursive Hash function (Rh) [13]. However, it still suffers from traceability attack which raised privacy issue. In the RCIA protocol the authors claimed that RCIA resists against traceability attack since the messages (A, B, C, and D) combined with random numbers (n1 and n2). In the RCIA protocol, the update operation for IDs value is performed only after each successful session. In this case, this update will prevent the attacker from tracking the tag with the assumption that the tag was read by legal reader. Unfortunately, if the tag was read by illegal reader (i.e.: an attacker can pretend to be legitimate) traceability attack can happen in this scenario. In this case, when illegal reader sends a query to the tag, the attacker gets response from the tag by sending its IDs. In the next illegal query, the tag will send the same IDs which make it prone to traceability attack. The main reason for this risk is when the illegal reader initiates a query to the tag, the responses of the tag each time are constant IDs. Figure 1 describes the operations of RCIA protocol.

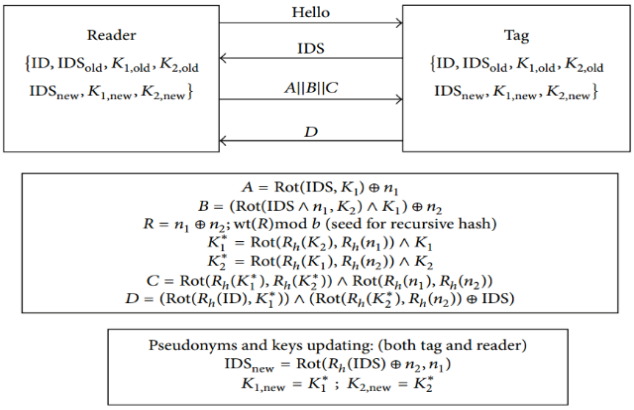

Figure 1: The operations of RCIA protocol

In the second step of RICA protocol, it can be clearly seen that the (IDs) value of the tag sent as a fixed value, and this value cannot updated only by legitimate reader [21], as shown in the fifth step. As a result of that, the attacker can easily track the location of tag's carrier by sending a multi query to the tag and the tag will response by sending the same IDs to the illegitimate reader. These reasons pointed out that the RCIA protocol vulnerable to traceability attack. The next Table1 shows a simple comparison of main attacks resistance, between the most recent ultra-lightweight authentication protocols.

Table 1
Attacks Resistance Comparison between ultra-lightweight authentication Protocols

	Traceability Attack	Desynchronization Attack	Disclosure Attack
UMAP family	X	X	X
SASI	X	X	X
Gossamer	X	X	√
David-Prasad	X	√	X
RAPP	X	X	√
RCIA	X	√	√

X: Susceptible to attack
√: Resists such an attack

III. Random Number Generator (RNG) Technique

Enhancing the security of ultra-lightweight authentication protocols in the RFID system is a challenge; due to it supports only simple operations like Bitwise [1]. This is because ultra-lightweight protocols were designed for low cost RFID system and this makes it unable to have complex cryptographic methods (e.g.: one way hashed function). This is a distinct characteristic of ultra-lightweight protocols which also serves as a limitation to it. With this limitation, the RNG needs to consider the usage of Bitwise operations to generate random number (Rn) which can effectively be implemented in the tag side [1].

Random Number Generator (RNG) is an algorithm uses to produce a sequence of unpredictable random numbers. The RNG is very important to increase the security of any system due to using the same value for each session will lead to possible traceability attack. The RNG can be generated using various algorithms in order to produce random numbers (Rn). The RNG technique proposed in this study is based on Bitwise XOR and shifts (left and right). The following section will discuss further on the algorithm used in the RNG called the XOR-Shift* Algorithm.

IV. XOR-SHIFT* ALGORITHM

In 2003, XOR-Shift algorithm has been proposed by Marsaglia22, as a very fast and high quality random number generator. This algorithm is based on repeatedly applying exclusive-OR (XOR) and shift operations (left and right) [22]. However, in 2014, Vigna [23], proposed XOR-Shift* algorithm following suggestion in Marsaglia's paper. The suggestion is multiplying the result of an XOR-shift generator by a suitable constant. This constant makes possible to generate a permutation of the sequence by the underlying XOR-Shift generator.

Based on rigorous experimental procedures, this XOR-Shift* generators successfully passed strong statistical test suites tool (i.e.: BigCrush and Dieharder) and was recognized as the fastest generator between all tested generators (i.e.: MT19937, xorgens4096, WELL1024a and WELL19937a) 23. XOR-Shift* algorithm acts as the main components of RNG. This algorithm takes into account the characteristics of ultra-lightweight authentication protocols and thus can be used in RCIA [23].

Without RNG in the RCIA protocol, when the illegal reader send request to the tag, it will respond with same IDs in each query session. This makes RCIA protocol vulnerable to traceability attack, which leads to privacy issue. With the RNG, the random numbers (Rn) are generated by using XOR-Shift* algorithm and concatenates with IDs to produce a new one (i.e.: newIDs). This will enable the tag to send different IDs in each query session. With the assumption that the query comes from illegal reader (i.e.: attacker), the tag will respond with different IDs in each query session. For example, in query session (1), the tag returns X as IDs while in query session (2), the tag returns Y as IDs. In this case the attacker will not be able recognize whether the IDs belongs to which tag. Thus this prevents traceability attack and solves the privacy issue.

V. IMPLEMENTATION OF THE RNG

The implementation of the RNG has been conducted by developing a prototype, due to the lack of hardware components of an RFID system (reader and tag). The prototype consists of three parts, which illustrate the main components of the RFID system, reader, tag and back-end database. The database contains all information that relates to the tag and reader, which is needed to accomplish the authentication processes. The operation of enhanced RCIA (i.e.: RCIA + RNG) is similar to the operations of existing RCIA protocol except that, in the enhanced RCIA, the RNG was used in the tag side. With this, updating IDs at the end of the query session is no longer necessary due to the randomization operations have been done by the RNG.

The implementation involved the processes of RCIA and enhanced RCIA. This is to provide comparison to promote better understanding on the implementation perspectives.

VI. EVALUATION

The aim of evaluation is to show the RNG technique that has been embedded to the existing RCIA; to ensure that the ID values generated will not be the same for each query session. This will help to prevent traceability attack and solve the privacy issue.

The evaluation scenario involved comparing between the existing RCIA and enhanced RCIA along with the traceability attack model adopted from [24].The following Table 2 describes the processes of the traceability attack model.

Table 2
Evaluation scenario

Steps	Attack processes
1	The attacker takes two tags, e.g. T0 and T1 and the identifiers for each one is (IDs)0 and (IDs)1 respectively.
2	The attacker randomly chooses one of the tags (T0 or T1), let's say Ti with the identifier (IDs)i
3	The attacker runs one query session with Ti and stores (IDs)i = X
4	The attacker runs the query session N times by using illegal reader, where N > 1. If (IDs)i in each time is not equal to X, in this case the attacker cannot track Ti . In other words, the attacker is unable to distinguish between T0 and T1. That means the enhanced RCIA successfully prevents the traceability attack. Otherwise, in each time, if the Ti responds with same (IDs)i. In this case the attacker can easily track Ti on the basis that (IDs)i is fixed value.
	Solution – RNG Technique
1	The illegal reader sends query to the tag (Ti)
2	Ti , uses RNG technique to generate a random number Rn and produce newIDs = IDs ⊕ ID | Rn
3	The illegal reader received the newIDs
	The attacker runs the query session N times, where N > 1. In each time, Ti responds with different newIDs. In this case, the attacker is unable to distinguish between T0 and T1. That means the enhanced RCIA successfully prevents the traceability attack.

The simulation has been performed many times (n > 1) to demonstrate the dynamic values of IDs in each query session. In each session, the tag in the RCIA protocol sent the same IDs to the reader. In contrast, the enhanced RCIA sent different IDs (newIDs) to the reader. With this simulated procedures, the enhanced RCIA has able to counter the problem of traceability attack by generating the random number (Rn). The different IDs values indicate that the attackers are now unable to trace the origin of the end users and thus prevent privacy violation issue.

VII. LIMITATION

In this study the operation of simulation tool limited on demonstrate that the RNG technique has successfully achieved its objective in producing the dynamic IDs. In other words, the simulation tool may not operate exactly like an actual device. Therefore, it only shows how the enhanced RCIA preventing the traceability attack by producing the dynamic IDs, using RNG technique.

VIII. Conclusion and Future Work

This study aimed to enhance the security of RCIA ultra-lightweight authentication protocol. This objective has achieved by adopting random number generator (RNG) technique. The RNG produced based on XOR-Shift* algorithm and used to provide a variable value for IDs. The RNG technique helped in preventing a traceability attack and as a result, solves a privacy issue.

The implementation of RNG technique has been conducted by using simulation technique. In order to provide a comparison between RCIA and enhanced RCIA, the simulation included simulating the operations of both protocols. Furthermore, the simulation used to evaluate the enhanced RCIA. The result of simulated enhanced RCIA, showed that the RNG technique has successfully prevented the traceability attack.

In the near future, the ultra-lightweight protocol specifically RCIA can consider other techniques or algorithms that probably may generate better results in enhancing the security. For instance, the RNG can consider another algorithm which may be more efficient. Additionally, other interested researcher can consider hardware implementation to expand the evaluation covering the performance and cost analysis perspective. It would also be useful to work on the adversarial platform, as to come up with several possible attacks so that preventive mechanisms can introduced even before the attacks were identified.

References

[1] H.-Y. Chien, "SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," Dependable and Secure Computing, IEEE Transactions on, vol. 4, (2007) 337-340.

[2] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estévez-Tapiador, and A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags," in Workshop on RFID security, (2006) 12-14.

[3] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "EMAP: An efficient mutual-authentication protocol for low-cost RFID tags," in On the move to meaningful internet systems 2006: Otm 2006 Workshops, (2006) 352-361.

[4] T. Li, G. Wang, and R. H. Deng, "Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols," JSW, vol. 3 (2008) 1-10.

[5] T. Cao, E. Bertino, and H. Lei, "Security analysis of the SASI protocol," Dependable and Secure Computing, IEEE Transactions on, vol. 6, (2009) 73-77.

[6] G. Avoine, X. Carpent, and B. Martin, "Strong authentication and strong integrity (SASI) is not that strong," in Radio Frequency Identification: Security and Privacy Issues, ed: Springer, (2010) 50-64.

[7] H.-M. Sun, W.-C. Ting, and K.-H. Wang, "On the security of Chien's ultralightweight RFID authentication protocol," IEEE Transactions on Dependable and Secure Computing, (2009) 315-317.

[8] G. Avoine, X. Carpent, and B. Martin, "Privacy-friendly synchronized ultralightweight authentication protocols in the storm," Journal of Network and Computer Applications, vol. 35, (2012) 826-843.

[9] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Tapiador, and A. Ribagorda, "Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol," in Information security applications, ed: Springer, (2009) 56-68.

[10] Y. Tian, G. Chen, and J. Li, "A new ultralightweight RFID authentication protocol with permutation," Communications Letters, IEEE, vol. 16, (2012) 702-705.

[11] E. Taqieddin and J. Sarangapani, "Vulnerability analysis of two ultra-lightweight RFID authentication protocols: RAPP and gossamer," in Internet Technology And Secured Transactions, 2012 International Conference for, (2012) 80-86.

[12] K.-H. Yeh and N. Lo, "Improvement of two lightweight RFID authentication protocols," Information Assurance and Security Letters, vol. 1, (2010) 6-11.

[13] Z. Bilal, A. Masood, and F. Kausar, "Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags: Gossamer protocol," in Network-Based Information Systems, 2009. NBIS'09. International Conference on, (2009) 260-267.

[14] M. Zubair, E. U. Mujahid, and J. Ahmed, "Cryptanalysis of RFID Ultra-lightweight Protocols and Comparison between its Solutions Approaches," Bahria University Journal of Information & Communication Technologies, vol. 5, (2012) 58-63.

[15] M. David and N. R. Prasad, "Providing strong security and high privacy in low-cost RFID networks," in Security and privacy in mobile information and communication systems, ed: Springer, (2009) 172-179.

[16] J. C. Hernandez-Castro, P. Peris-Lopez, R. C.-W. Phan, and J. M. Tapiador, "Cryptanalysis of the David-Prasad RFID ultralightweight authentication protocol," in Radio Frequency Identification: Security and Privacy Issues, ed: Springer, 2010, 22-34.

[17] D. F. Barrero, J. C. Hernández-Castro, P. Peris-Lopez, and D. Camacho, "A genetic tango attack against the David–Prasad RFID ultra-lightweight authentication protocol," Expert Systems, vol. 31, (2014) 9-19.

[18] G. Avoine and X. Carpent, "Yet another ultralightweight authentication protocol that is broken," in Radio Frequency Identification. Security and Privacy Issues, ed: Springer, (2013) 20-30.

[19] W. Shao-hui, H. Zhijie, L. Sujuan, and C. Dan-wei, "Security analysis of RAPP an RFID authentication protocol based on permutation," College of computer, Nanjing University of Posts and Telecommunications, Nanjing, vol. 210046, (2012).

[20] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, "Desynchronization attack on RAPP ultralightweight authentication protocol," Information processing letters, vol. 113, (2013) 205-209.

[21] U. Mujahid, M. Najam-ul-Islam, and M. A. Shami, "RCIA: A New Ultralightweight RFID Authentication Protocol Using Recursive Hash," International Journal of Distributed Sensor Networks, vol. 2015 (2015).

[22] G. Marsaglia, "Xorshift rngs," Journal of Statistical Software, vol. 8, (2003) 1-6.

[23] S. Vigna, "An experimental exploration of Marsaglia's xorshift generators, scrambled," arXiv preprint arXiv:1402.6246, (2014).

[24] A. Juels and S. A. Weis, "Defining strong privacy for RFID," ACM Transactions on Information and System Security (TISSEC), vol. 13,(2009) 7.