IJCTA, 9(20), 2016, pp. 69-74
© International Science Press

Comparative Security and Privacy Analysis of RFID communication System

Monika Sharma*, **Kavita Saxena**** **and P. C. Agrawal*****

ABSTRACT

RFID system main security and privacy threats are eavesdropping, location tracing, forward security, replay attack, tag/reader collision, counterfeit, and consumer/user data privacy or information leakage.Authentication is the process of guaranteeing that sender would be the one whom they claim to be. Here, the main objective for authentication is to authenticatethe tag and the reader both, So that only authentic reader getsaccess of data of the authentic tags.

This paper gives a brief focus onthe analysis of existing RFID security and privacy schemes and also focus on the comparative analysis of these schemes with the proposed one.

Keywords: *ECC, Security, Privacy, RFID, Encryption, Decryption PIR*.

1. INTRODUCTION

RFID tag is a microchip which is connected to an antenna that is embeds in a way that it can be connected to article/individuals. The three main components of an RFID system are tag, reader, and antenna. A tag is a kind of device that facilitates attachment with the produced object or to a person to enable their distinctive identity, while a reader, being an electronic gadget, forwards a radio sign to a tag, which again retransfers its information to the reader.

In RFID framework, individual information can be secured by cryptography (symmetric and public key methodology), and reader authentication implies tag may just yield their IDs to determined reader after it gets a particular key from the reader [3].Major limitation of the tag is that it cannot perform carrier sensing. Various protocol neglect that there may be multiple readers at a particular time and can send ID request to a single tag [17].

2. PREVIOUS PROTOCOL ANALYSIS

A few works have been performed and given an account of RFID authentication. Some authentication plans utilize the hash function one-way property in explaining the security and privacy issues of RFID frameworks. In any case, dominant part of them is under security risk. Couple of case of standard authentication plans relying upon hash property i.e.hash-chain,hash-lock, and randomized hash-lock scheme. Due to one way restricted hash property, Weis et al. [20] presented the hash-lock scheme that endeavors to offer two way (shared) authentications forthe reader and a tag. In this method, the metaID replaces the tag's genuine ID with a specific end goal to ensure its privacy. At the time of authentication, transmission of the IDof a tag as a plain content done between the tags and the readers, and the metaID is settled. Thus, with the assistance of replaying and eavesdropping in return messages between the readers and tags, an adversary easily compromise the common confirmation. Furthermore, a rival can track the tag holder with the assistance of the altered metaID.

* Research Scholar Mewar University Department of Computer Science & System Studies, Chittorgarh, Raj., INDIA & Faculty AIIT, Amity University (U.P.), *Emails: monika.sh.81@gmail.com, msharma5@amity.edu*

** Associate Professor, R & D Dept, Mewar University, Chittorhgarh, Raj., INDIA, *Email: ksaxena72@yahoo.com*

*** Guest Professor Mewar University & Retired Scientist form Ministry of IT & Communication

Weis et al. [20] proposed the randomized hash-lock method that could surprise the issues of the hash-lock convention, which randomizes the trade messages between the tags and the readers by utilizing the pseudorandom number generator (PRNG). The tags creates an irregular number worth, then hash its ID linked with arbitrary esteem, and send both the values to the reader as an answer to the reader request. A brute-force search in pursuit of its perceived IDs by a substantial reader helps in recognition of one of its tags. Such-recognized tag's ID is sent by the reader to the tag utilizing plaintext. Be that as it may, a rival can without much of a stretch get to the character information of the tag by spying, which makes it defenseless to fake and replay attack. Additionally, simple following of the tag holder can't guarantee the forward security.

Ohkubo et al.Introduced a scheme named hash-chain[13, 14], which makes utilization of two sorts of hash values G ( ) and H ( ). This method offers stand out way authentication, that is, confirmation of the tag by the reader done however not the other way around. Utilizing the hash fasten method to reintroduce the privacy information put away in the tag, this system offers the forward security. Be that as it may, it doesn't works against replay and desynchronization attack. Yeo and Kim [22] proposed another plan that guaranteed a hypothetically basic yet very much outlined answer for beat the following issue and to guarantee forward security. This scheme warrants each tag to support two hash functions. The tag exchanges the hash estimation of its present identifier, by a hash function, G ( ), on questioning by the reader and afterward reintroduces its identity information with the second hash function, H ( ). As two sorts of hash are being utilized by this scheme, ease RFID frameworks can't support this scheme.

Lee and Verbauwhede [11] proposed semi-randomized access control (SRAC), a sheltered and minimal effort check plan for the RFID framework, which utilizes metaID as pseudonymsubstituting the tag's ID like hash-lock scheme. It offers both shared authentication and forward security and can keep the RFID frameworks from different issues, for example,tracking, duplicating, and rejection of service. By and by, replay attack can influence this convention. A rival can check viably utilizing listen in and recover of the metaID. Later, a minimal effort RFID authentication scheme (LCAP) utilizing a test reaction plan was overhauled by Lee et al. [12]. Both common confirmation and area security of a tag holder are met by this convention. Also, it offers no traceability by changing tag's accreditations powerfully. Be that as it may, forward security is not offered by this technique, which implies that an adversary can reason past information about the tags and after it gets the present messages.

Cho et al. [4, 5] proposed an authentication novel hash-based proposal to meet the security and privacy difficulties of the RFID frameworks. In any case, Kim [9] demonstrated the powerlessness of this scheme to DOS attack, where he set up that the system by Cho et al. is interested in activity examination and reader/ tag mimic assaults. Precisely, a likelihood of 1/4 exists for an adversary to imitate a legal tag or reader. Additionally, the quick session offers a likelihood of 3/4 for a rival to accumulate couple of information about the mystery estimations of the tag. Khedr [8] showed out that an adversary can assault utilizing desynchronization by hindering and harming the swapped message in step 5. Moreover, he showed that forward security is not guaranteed by the strategy of Cho et al.

RFID security system utilizing the hash-based schemes that can offer forward security was proposed and demonstrated by Ha et al. [6]. Notwithstanding, Sun and Zhong [16] demonstrated the following of the objective tag by seeing fizzled past sessions by an assailant. What's more, they demonstrated that the convention by Ha et al. [6] does not offer forward security as they ensured and proposed another hash-based confirmation capacity to battle the defects the convention by Ha et al. [6]. Be that as it may, as all these proposed methods require two diverse hash properties, they are not relevant for the ease RFID frameworks. Yang et al. [21] set up a RFID secure checked methodology relying upon hash capacity, which offered information privacy and grasped three gathering shared confirmations, that is, among the tag, the reader, and the backend database. Notwithstanding, every check procedure warrants that the tag and the reader call hash work multiple times (5 times) s, separately, which made the method multifaceted and not relevant for the ease RFID frameworks.

Notwithstanding hash function and extra encryption function, RFID frameworks included confirmation strategies that utilized a pseudorandom generator and bitwise operations. Nonetheless, quick to the proposition of these conventions, different inquiries about told the imperfections of these conventions and their wastefulness to battle all the security & privacy issues of RFID frameworks, especially for the ease RFID frameworks.

3. ANALYSIS OF PROPOSED SCHEME

ECC is reasonably faster, inexpensive, and complex than other techniques as it is based on multiplication technique [1,2, 5, 7, and 10]. The shorter length of the key results in faster ECC [19].

Shivkumar and Umamaheswari [15] concluded on the basis of simulation that ECC is best suited for wireless applications where speed, bandwidth, and time are the constraints. ECC gives the security at same level of RSA while using less key size. They found that ECC-based combinations of algorithms are best to perform on encryption, throughput, and end-to-end delay.

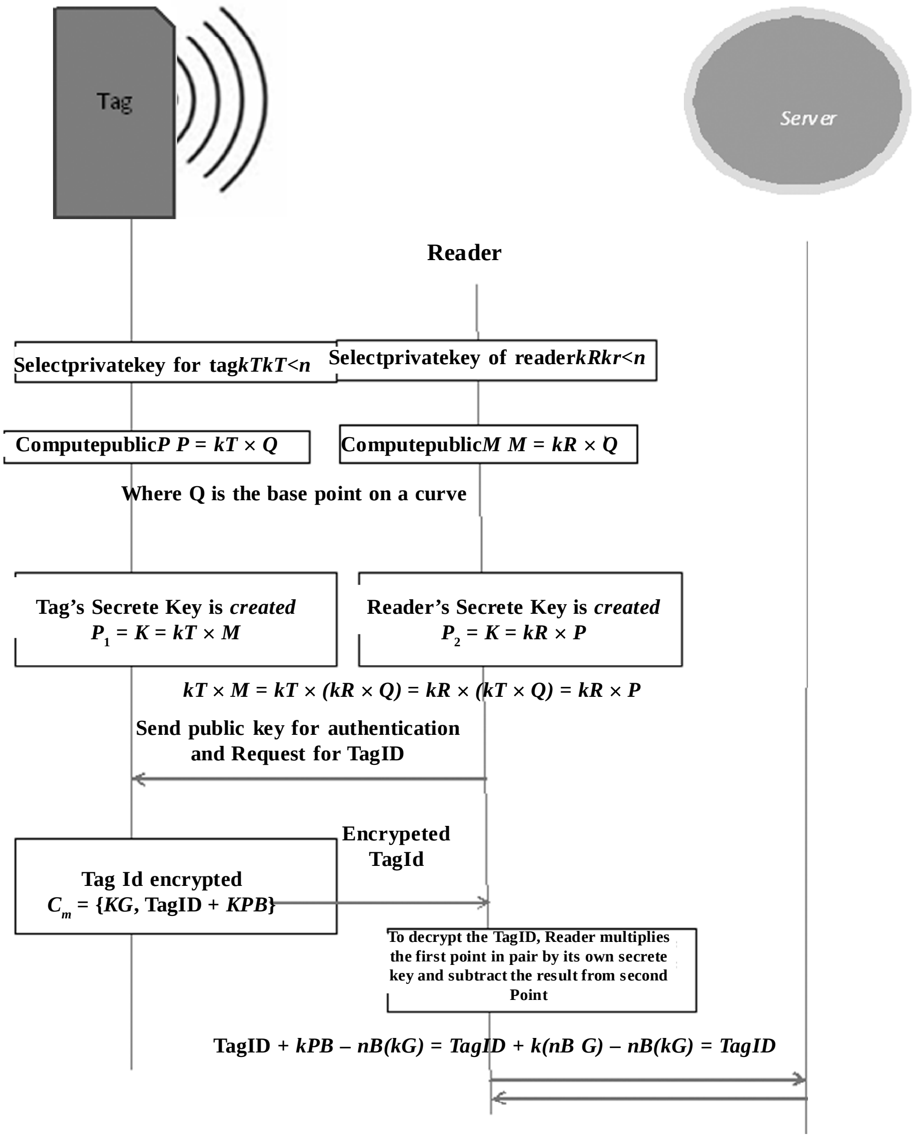
Tag
Server
Reader
Selectprivatekey for tagkTkT<n
Selectprivatekey of readerkRkr<n
ComputepublicP P = kT × Q
ComputepublicM M = kR × Q
Where Q is the base point on a curve
Tag's Secrete Key is created
$P_1 = K = kT \times M$
Reader's Secrete Key is created
$P_2 = K = kR \times P$
$kT \times M = kT \times (kR \times Q) = kR \times (kT \times Q) = kR \times P$
Send public key for authentication and Request for TagID
Encrypeted TagId
Tag Id encrypted
$C_m = \{KG, \text{TagID} + KPB\}$
To decrypt the TagID, Reader multiplies the first point in pair by its own secrete key and subtract the result from second Point
$\text{TagID} + kPB - nB(kG) = TagID + k(nB\ G) - nB(kG) = TagID$

Figure 1: Proposed Protocol for communication of tag and reader

During the authentication procedure portrayed in our protocol, simply after both tag and reader validate, encoded tag uncovers its ID to its reader, and the reader will ready to get to the data from the backend. In this way, it is profoundly trying for a rival to harm or uncover the tag's identity information.

The tag and the reader have their own secrete keys. The secret key of a reader is created from the combination of the private key of a reader and public key of a tag. Likewise, the tag secret key is created from the public key (P) of a reader and the private key (K_T) of a tag. Be that as it may, just public key is imparted to the tags and the readers to guarantee the consistency of the exchanged data between the tags and the readers with a specific end goal to prevent tractability.

The public key of a tag is made by the private key of a reader and the base purpose of the elliptic- curve; comparatively, the public key of reader is made by the private key of a tag and the base point on the elliptic-curve. This guarantees the procurement of forward security by the proposed scheme. Assume that there are n quantities of tags altogether and the backend server possibly complete N correlation operations at the most for a fruitful authentication. For the tag, it just needs public key of the reader to validate it, and likewise, the reader needs the public key of a tag to confirm [18].

Below we are analyzing the proposed authentication scheme:

3.1. Security against eavesdropping

During the authenticating process, all communication between the tags and the readers are encrypted, and attackers cannot access any data about the tag from their attained messages. The privacy security of the RFID system is established by making eavesdropping of the message transfer between the tags and the readers worthless.

3.2. Security against location detection or tracing

The major privacy issue of the RFID system is the exposure of a constant value for every verification, which results in the disclosure of the user's location. This attack can be avoided by generating every time a dissimilar code, which can be done using elliptic curves base point, thereby assuring that every session between the tags and the readers is different so that attackers remain unaware of the location of their received data.

3.3. Security against replay attack

Replay attack involves repeating the data gathered by eavesdropping to compromise the RFID system. Tracking issues and privacy security issues occur because of the exposure of identical or constant values from the tag during the resending process. Such attack can be combatted by making the content of every session between the tags and the readers dissimilar; thus, ECC range operations ensure the encoding of tagID each time using the random number and the base point of the curve. Hence, when an attacker resends their gathered message later, there is no meaning for this message because of generation of novel random number using base point on the curve and the corresponding messages in every new session.

3.4. Forward security

The pair of new random numbers generated by the readers and the tags in every verification process has no association with the previous verification, randomizing all the exchanges between the tags and the readers. Thus, gathering of valid data of the previous verification by the attackers cannot deduce anything from the present received messages, and guessing of the previous behaviors of tags or readers by the attackers is not possible.

3.5. Security against counterfeit attack

In this sort of attack, a tag can be cloned if the secret key shared among the tag and the authorized reader is uncovered. Our plan guarantees the privacy by authentication of the tag and the reader. (Tag secrete key is created by private key of the tag and public key of the reader and reader secrete key is produced by private key of the reader and public key of the tag). where, just the public key is send while authentication, and the tag's public key is made by tag's private key and an arbitrary no. on the curve base point and same way reader computes its public key while utilizing private key and construct indicate with respect curve. The tag and the reader have their own particular secret keys. Every one of the interchanges between the readers and the tags are encoded by elliptic curve secret base point, which is more secure. An attacker can't get to any character information of a tag; in this way, a rival can't emulate a legitimate tag to spoof the RFID framework.

3.6. Tag/reader collision

In this type of attack, the integrity and availability of a system can be hampered by electronic collisions. In our scheme, collision of tag/reader may not occur as authentic reader can get access of authentic tag ID only. Although there may be multiple readers querying a tag ID, communication will be possible only with the authentic tag and readers.

3.7. Security against consumer/user data privacy

This type of attack is possible when the use of RFID chip is done by unlawful parties to obtain personally identifiable information, along with location information of the tag holder; thus, privacy of the consumer is said to be under invasion. But as the tag ID in the tag encrypted with the random positive number using elliptic curves will be accessed only by the authentic reader, intruder cannot get access the tag information.

Table 1
Shows the comparison of the previous authentication protocols with our proposed scheme

Protocols	Eaves dropping	Location tracing	Replay attack	Forward security	Counterfeit attack	Tag/reader collision	Data privacy	Scalability
Deterministic hash-lock	No	No	No	No	No	No	No	No
Randomized hash-lock	No	No	No	No	No	No	No	No
Improved randomized hash	Yes	Yes	Yes	Yes	No	No	Yes	No
Hash-chain protocol	Yes	Yes	No	Yes	No	No	Yes	No
Semi-randomized access protocol	No	Yes	No	Yes	Yes	No	Yes	No
Our proposed scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

4. CONCLUSIONS

While analyzing the security and privacy, randomization of the correspondence between the tags and readers provides security, and they are diverse for each confirmation strategy, despite the fact that the secret key is not revealed during authentication of tag and reader. Just the public key is utilized by the tag and the reader in the authentication procedure. Nonetheless, as there is no change in the tagID, the proposed scheme can be connected to the distributed processing environment. In the meantime, it is seen clearly that each time correspondence between the tags and readers just incorporates the arbitrary number, public key, and random base point with tag's ID for data during the encryption, so it is troublesome for the adversary to procure the entire data about the tag's ID. Then again, the ID may all the while be utilized by the backend server or ID might be again encrypted with the same procedure at server side.

5. FUTURE SCOPE

In future work can be done on more secure elliptic curves. So that communication between tag and reader will be stronger. Fuzzy techniques may introduce to enhance the research in this field.

REFERENCES

[1] Ahmad, Y.:"A study on the application of elliptic-curve cryptography in implementing smart cards". *International Journal of Modern Engineering Research (IJMER), 2*(1), 155–159(2010).

[2] Amin, F., Jahangir, A.H., &Rasifard, H.: "Analysis of public-key cryptography for wireless sensor networks security". *World Academy of Science, Engineering and Technology, 41*, 529–534(2008).

[3] Cha, S.-C., Huang, K.-J., & Chang, H.-M. : "An efficient and flexible way to protect privacy in RFID environment with licenses". In *2008 IEEE International Conference on RFID* (pp. 35–42), 16–17 April, Las Vegas, NV(2008)..

[4] Cho, J.-S., Yeo, S.S., & Kim, S.K.: "Securing against Brute-force attack: a hash-based RFID mutual authentication protocol using a secret value". *Computer Communications, 34*, 391–397(2011).

[5] Jeong, Y.-S., Cho, J.-S. & Sang, O.-P.:"Consideration on the Brute-force attack cost and retrieval cost: a hash-based radio-frequency identification (RFID) tag mutual authentication protocol". *Computers and Mathematics with Applications, 3*, 1–8(2012).

[6] deMeulenaer, G., Gosset, F., Standaert, F.-X., Vandendorpe, L., & UCL/DICE Crypto Group.: "On the energy cost of communication and cryptography in wireless sensor networks". In *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2008* (pp. 580–585), Avignon, France(2008).

[7] Zhou, J.Y., Ha, J.H., Moon, S.J., & Ha, J.C.: "A new formal proof model for RFID location privacy". In *Proceedings of the 13th European Symposium on Research in Computer Security (ESORICS'08)*, October 6–8, Malaya, Spain(2008).

[8] Kak, A.: "Elliptic curve cryptography and digital rights management". *Lecture Note on Computer and Network Security, 111*, 164–179(2013).

[9] Khedr, W.I.:"SRFID: a hash-based secure scheme for low cost RFID systems". *Egyptian Informatics Journal, 14*, 89–98(2013).

[10] Kim, H.: "Desynchronization attack on hash-based RFID mutual authentication protocol". *Journal of Security Engineering, 9*(4), 357–365(2012).

[11] Lauter, K.: "The advantages of elliptic curve cryptography for wireless security". *IEEE Transactions on Wireless Communications, 8*(2), 882–889(2004).

[12] Verbauwhede, I.&Lee, Y.K. &.:"Secure and low-cost RFID authentication protocols". In *Proceedings of the 2nd IEEE Workshop on Adaptive Wireless Networks*, November 28-December 1, St. Louis, USA(2005)..

[13] Lee, D.H., Lee, S.M., Hwang, Y.J., & Lim, J.I.: "Efficient authentication for low-cost RFID systems". *Lecture Notes in Computer Science, 3480*, 619–627(2005).

[14] Ohkubo, M., Suzuki, K., & Kinoshita, S.: *Cryptographic Approach to "Privacy-Friendly" Tags*. NTT Laboratories, Nippon Telegraph and Telephone Corporation(2003).

[15] Ohkubo, M., Suzuki, K., & Kinoshita, S.: "Hash-chain based forward secure privacy protection scheme for low-cost RFID". In *Proceedings of the 2004 Symposium on Cryptography and Formation Security*, January 27–30, Sendai, Japan (2004).

[16] Shivkumar, S. &Umamaheswari, G.: "Certificate authority schemes using elliptic curve cryptography, RSA and their variants simulation using NS2". *American Journal of Applied Science, 11*, 171–179(2014).

[17] Sun, D.-Z. &Zhong, J.-D.: "A hash-based RFID security protocol for strong privacy protection". *IEEE Transactions on Consumer Electronics, 58*(4), 1246–1252(2012).

[18] Sharma M., Agrawal P.C, "ECC implementation for secured RFID communication", *IJCSEE* 2 (1), 50-54(2014).

[19] Tan, C.C. & Wu, J.: "Security in RFID networks and communications". In *Wireless Network Security*, Chapter 10, pp. 247–267. Springer(2013).

[20] Torii, N. & Yokoyama, K.: "Elliptic curve cryptosystem". *FUJIRSU Scientific & Technical Journal, 36*, 140–146 (2000).

[21] Weis, S.A., Sarma, S.E., Rivest, R.L., & Engels, D.W.: "Security and Privacy aspects of low cost Radio frequency identification system". In *First International Conference on Security in Pervasive Computing* (vol. 2802, pp. 201–202), Springer-Verlag, Boppard, Germany (2003)..

[22] Yang, L., Yu, P., Bailing, W., Yun, Q., Xuefeng, B., Xinling, Y., &Zelong, Y.: "Hash-based RFID mutual authentication protocol". *International Journal of Security and Its Applications, 7*(3), 183–194(2013).