Efficient and Timely Mutual Authentication Scheme for RFID Systems

Hesham A. El Zouka, Mustafa M. Hosni

***Abstract*—**The Radio Frequency Identification (RFID) technology has a diverse base of applications, but it is also prone to security threats. There are different types of security attacks which limit the range of the RFID applications. For example, deploying the RFID networks in insecure environments could make the RFID system vulnerable to many types of attacks such as spoofing attack, location traceability attack, physical attack and many more. Therefore, security is often an important requirement for RFID systems. In this paper, RFID mutual authentication protocol is implemented based on mobile agent technology and timestamp, which are used to provide strong authentication and integrity assurances to both the RFID readers and their corresponding RFID tags. The integration of mobile agent technology and timestamp provides promising results towards achieving this goal and towards reducing the security threats in RFID systems.

***Keywords*---**RFID, security, authentication protocols, privacy, agent-based architecture, time-stamp, digital signature.

I. Introduction

LOW frequency RFID systems consist of many transponders (tags) and one reader which several antennas are connected to. Contactless programmed RFID technology is normally used to supplant existing standardized identification plan, since it has the ability of accessing huge amounts of information from many tags at the same time in an accessible range. Though, an RFID technology is a comprise of a back-end server connected with many readers. Readers and tags are connected in a remote access which is vulnerable to attack. In contrast, RFID is the wireless use of radio frequency electromagnetic fields to transfer data, for the purposes of identifying and tracking tags attached to or implanted in an object. The tags electronically stored information that can be accessed at short range via radio signals. Some tags can be powered by a local power source such as a battery and may operate at hundreds of meters from the RFID reader [1]. However, many tags are powered by the electromagnetic induction from magnetic fields produced near the reader. In other words, most tags stay in idle mode most of the time, and when an RFID reader waves over them, it provides enough power for the data on the tags to be read and act as a passive transponder. Unlike a barcode, the tag does not necessarily need to visually see the reader or be within line of sight of the reader. Tags can be read only if the reader is nearby, and sometimes may be embedded in the tracked object, or even used as a unique identification code [2].

RFID tags are used in many industries. For example, RFID tags are used in modern passports to protect against unauthorized reading or tracking of the passport when it is not in use. It may allow also the border agent to read the personal data from the embedded RFID chip. RFID chips are also used in credit cards, where the reader machine scans an RFID chip that is embedded in the card. Some other examples involve the use of tags in vehicle tracking systems. The world RFID market is worth $8.9 billion in 2014 and registered 10% growth over 2013 and nearly 8% growth over 2012. The RFID market is expected to rise to more than $25 billion by 2020. This includes tags, readers, and any supporting hardware/software systems such as RFID cards, labels, fobs and all other form factors for both passive and active RFID. However, the use of RFID technologies has raised serious privacy concerns since data on the RFID chips could be potentially picked up by an unauthorized reader without the knowledge of tag's holder. The security of RFID tags and the information transferred between the tags and the reader is of prime concern to the RFID industry. Hence, there are some security issues in RFID framework which have to be addressed, for example, tracking of tag location; backward traceability; replay attack; spoofing and forward security. In this paper, we proposed an algorithm based on the timestamp and mobile agent based architecture to overcome such security problems. The proposed algorithm appends an extra random number to the tag in a manner that will be used to enhance the security compared with current security systems; despite the fact that processing power of the tag will be slightly increased comparing to the existing related works.

In this paper, the potential threats to tag data security and tag-to-reader communication are examined, and then the authentication issues in RFID system are investigated as identity of the tag can be verified at the RFID reader, and design the lightweight security model that is independent from specific RFID hardware and cryptographic algorithms. Two protocols based on the proposed model which guarantees the authentication and privacy in RFID systems are introduced. The rest of the paper is organized as follows: In Section II a brief overview of the RFID systems and their security implications will be given. The security requirements of RFID systems are listed in Section III. In Section IV, the proposed authentication is described. The security analysis is summarized in Section V with extensive simulation results. Section VI concludes the paper.

Hesham A. El Zouka is with the Computer Engineering Department, College of Engineering and Technology, Arab Academy for Science, Technology, and Maritime Transport, Alexandria, Egypt, (e-mail: helzouka@aast.edu, helzouka@gmail.com).

Mustafa M. Hosni is with the Electrical Engineering Department, Faculty of Engineering, Managing Director of OMIKRON Technologies, Alexandria, Egypt, (e-mail: mustafa.hosni@omikrontechnologies.com).

II. Challenges and Limitations

RFID refers to a system that utilizes radio frequency to communicate wirelessly. An RFID system typically consists of a tag, a reader, middleware software, and a host computer (Campbell). In particular, there are two types of tags used: passive tags and active tags. A passive tag consists of an antenna and an application specific integrated circuit. It is powered by an electromagnetic field generated by the RFID reader. As the signal is relatively weak to propagate, the tag must be close to the reader to be detected.

Every RFID tag has a unique identification number associated with it. The identification number includes a unique serial number for that tag, which is impossible to change or duplicate, and the manufacturer guarantees that no duplicates are ever present.

RFID tags, readers, and communications software interact with each other to provide an interface for users to obtain meaningful data. The reader gathers information from the RFID tags by sending out radio signals through one or more antennas. Then, the RFID tag will respond to the received signal by sending back its tag's ID and other stored information. The reader converts data from the tag into digital form and the communication software formats the stream of bits obtained from the tags. The reader sends out transmissions thousands of times per time resulting in a lot of information to read through. The host system then filters the multiple signals and begins processing this data and storing it in a database for analysis.

The market for RFID tags and readers has experienced significant growth in recent years, and is finding applications in many different areas including personal authentication, access control, inventory management, counterfeit prevention and the tracking of goods. Therefore, there are many types of risks associated with the security of RFID technology. Some of the important risks are associated with RFID tags. For example, RFID tags could be easily cloned and tracked by an adversary that has read access. Reverse engineering can even clone them through advanced physical layer analysis. The attacker can use the cloned tags to replace the original ones and inject a large amount of fake messages. He can also trace the previous messages sent. In another likely instance, the attacker can perform denial of service attack at all its neighboring tags by just cloning one of them, subjecting the reader to distributed denial of service attack. Hence, attackers can use such an attack to make the reader authenticate the cloned tag as a legitimate tag and update other tag IDs. Another and more serious types of risks are affecting the communication between readers and tags. For example, inadequate RFID security could threaten the communication signals and cause unauthorized eavesdropping. Many other RFID security breaches lead to leakage of sensitive information such as identifiers of cryptographic key of tags, location and user identity, security numbers, and individuals' financial information. There are other many threats associated with RFID systems that range from physical attacks on tag and reader devices including sniffing, location tracking, spoofing, replay, and many more. In the flowing examples we will survey some of these attacks will be surveyed and the effectiveness will be evaluated [3].

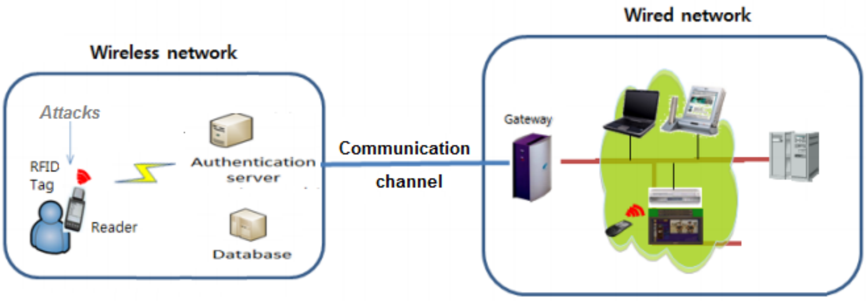

Fig. 1 Overview of RFID System Interaction

A. Sniffing Attack

Sniffing attacks represent one of the largest and potentially damaging attacks to almost all wireless networks that are currently in use. Thus, this attack is not unique to RFID technology. Hence, all the communication between RFID tags and readers can be easily intercepted if not well protected by a proper security scheme. Therefore, sniffing attacks can capture secret keys or other stored information in the tag through eavesdropping and even able to tamper with the secrecy and confidentiality of the data communicated. Furthermore, sniffing attack can reveal all the encoding settings used to query tags.

One defense to this attack involves tamper-proofing the tag's physical package by placing the tag in a well shielded enclosure when not in use. Blocking all tag emissions will play essential roles in preventing information leakage to unauthorized readers. However, this defense mechanism is not effective when the tag remains in query mode all of the time.

B. Spoofing Attack

A spoofing attack occurs when an attackers uses a fake tag in order to pretend to use a legitimate tag. Tag cloning is another type of spoofing attack, which produces unauthorized copies of legitimate tags. For example, in the shopping centers the original tags can be replaced with the cloned one to fool the system and purchase the items at cheaper prices. Similarly, toll transponders can be cloned, allowing drivers to pass for free, making the system vulnerable to fraud. Countermeasures to spoofing attacks include shielding RFID tags in a manner similar to the sniffing attack. Clearly, the traditional public key encryption approach and other strong encryption models are not suitable to RFID systems.

C. Replay Attack

Replay attacks combine spoofing and sniffing types of attacks. During the authentication process between tags and readers, the data can be captured and replayed by the attacker. Indeed, replay attacks compromise the integrity and confidentiality of the RFID system [4]. A possible countermeasure to this type of attack is to utilize the read-write risk assessment before deploying a new tag. Following that, the new tag is authenticated and authorized. Hence, this enables to establish secure communication channel and to enhance the expected security mechanisms of uploading new code into the target tags.

D. Physical Attack

Low-cost RFID tags are vulnerable to various kinds of attacks especially the physical attack. One important physical attack is the introduction of cloned tags into the RFID system. Tampering is another type of physical attack, which targets the actual hardware of the RFID tags. Due to the low-cost architecture of RFID system, it is difficult to know whether this attack is caused intentionally or unintentionally. One solution to physical attacks is to use tamper-resistant hardware and secure RFID tags. However, using tamper-resistant tags for securing communication in RFID system cannot be considered as a solution against these attacks as it increases the complexity of the system.

E. Location Traceability Attack

If the location of the tag is exposed to an attacker, all its stored information will be revealed. There are several ways to trace the location of tags. For example, the attacker can deduce the location of a tag if the tag always outputs a fixed value or by analyzing the content of the tags. In order to defend against location attacks, some secure localization algorithms have been used recently [5]. However, this attack is a challenge to location verification in general and cannot be easily prevented as the attacker defines the precise location of the tag based on analysis of the received information. In addition, most of the RFID system entity is located in a space that is part of a building, and hence the location of the tag can be easily identified when the attacker can extract some information about the containment relationship.

F. Cloning Attack

In a cloning attack, an attacker compromises genuine tags and use their replicas to impersonate genuine tags. Cloning attacks thus threaten many RFID applications that use the genuineness of tags to validate the authenticity of the tagged products. Some of the existing solution to clone attack involves prevention of clone attack by using encryption technology to make tags hard to compromise. However, this solution cannot be implanted by most of the existing low-cost tags due to their hardware constraints. Other solutions involve identifying clone attack with a high detection probability rather than preventing it. However, this solution is ineffective in terms of scalability.

G. Denial of Service Attack

The attacker can perform denial of service attack at all its neighboring tags by just cloning one of them, subjecting the reader to distributed denial of service attack. Hence, attackers can use such an attack to make the reader authenticate the cloned tag as a legitimate tag and update other tag IDs. Whoever the tag receives an identification ID from the reader, it compares the received ID with the id stored in the database server. Therefore, both the reader and the backend server of the RFID system are vulnerable to denial of service attacks. When such an attack takes place, the RFID tags fail to verify their identities with the reader and as a result the RFID system can be subject to many other malicious attacks. In order to avoid denial of service attack without increasing the complexity of the tags, some researches proposed a technique that uses session keys. The session keys could be established in a way that synchronizes the update at both the tag and the reader to allow location privacy communications [6]. Despite of the complexity underlying such low cost systems, the problem of distributing the session keys remains to be solved.

III. Security Requirements

In this paper, it is assumed that the channel between the reader and back-end server is secure, while the communication between tags and their reader is insecure. The analysis will take care of the authentication and the trust between RFID tags and reader by using trust links and authenticated communication [7]. Any authentication protocol for RFID technology must be designed by keeping the fact that the tags have constrained hardware architectures [8]. Thus, it remains a great challenge to design RFID authentication protocols that are immune to malicious attack, and allow the reader to efficiently verify the integrity of the tags [9]. Therefore, there are some security aspects that the RFID system designer should consider in order to implement an authentication protocol that provides both security and privacy. These aspects are as follows:

RFID Randomization: In order to meet the demands of privacy in RFID system, which is achieved by randomizing the outputs of the tags, the associated reader must have an algorithm to differentiate between those tags. By randomizing the outputs of the tags, the intruder cannot compromise the RFID tags, as he will not be able to distinguish between tags and to know which tag he is currently interacting due to the random output of the tags. Meanwhile, the legitimate reader will not be able to read the responding tag as well because the outputs were randomized. The associated reader thereby has to search among all the RFID tags in the system to identify the tag being inserted. Unless the reader has specific mechanisms to achieve that, such a brute-force search would not be practical or applicable for large large-scale RFID system.

RFID Confidentiality: Data confidentiality is one of the vital security requirements for RFID system. Indeed, illegal access to the tags is the origin of most attacks that affect the function of the RFID system. That is why the authentication of the tags appears as stone angle of secured RFID system. Clearly, confidentiality and integrity of messages exchanged between tags and readers would enhance the authentication mechanism and prevent the attacker from eavesdropping. Therefore, authentication mechanisms and strong encryption models need to be implemented to protect the data transferred between the tags and the readers in the RFID system so that only legitimate reader or tags were able to process the encrypted messages. However, it is widely accepted that strong cryptography algorithms cannot be implemented in RFID system due to its hardware constraints [10].

Forward and Backward Security: An attacker that compromises a tag can easily identify a tag's past interactions from the previous communications. Hence, to ensure future security, the compromised tag should not reveal any information about previous tag-reader communication. On the other hand, backward security protects future tag transactions from traffic analysis attacks. Some researchers apply acknowledgment schemes to detect both forward and backward attacks.

If the sender tag does not hear any acknowledgment from the reader in certain period of time, it will re-transmit the setup request signal. This protocol shows a strong resilience against tag capture as the key management shame generates the pair-wise keys between the tags and associated reader randomly. However, the pair-wise key algorithms may require high computing complexity which is limited in such low-cost RFID systems.

Mutual Authentication: Mutual authentication protocols are those where both communicating parties authenticate each other. In RFID system, mutual authentication can be implemented by simply using a hash function or message authentication code. Moreover, in RFID systems, the mutual authentication can even be performed without the reader being connected to back-end server. Failure in mutual authentication protocol can expose the underlying system to vulnerabilities and security risks. However, to guarantee the privacy of information and solve the problem of RFID certificate, the back-end server must be involved in this process, which leads to increase to overall time complexity [11], [12]. Hence, mutual authentication is the process where both communicating parties prove their identities to each other. The authentication could be strengthened by adding a second cryptography layer which ensures protection for all the communications between the tags and their reader in the RFID system. Basically, two cryptographic models are needed to for privacy and authentication protocols; namely symmetric key encryption and asymmetric key encryption [13].

A weakness of using symmetric encryption model in RFID system is that the tag and the reader share common private key to run the authentication process, where the tag uses this key for response generation while the reader use it for verification, which requires the readers to store all the secret keys of their tags or establish an online connection between the readers and the back-end server to store those secret keys in a reliable and secure manner. However, symmetric encryption is computationally less expensive than asymmetric ones.

In Asymmetric cryptography which use pair of keys, the private key is used to sign the tags identifiers, but the public key is used in the verification process at the reader. One of the advantages of using asymmetric encryption models over symmetric ones is their ability to authenticate the tags and to verify their identities. This could also prevent malicious tags from masquerading as legitimate tags. In addition, asymmetric cryptography uses certificates to address the problem of mutual authentication in RFID systems. This certificate is used to establish a trust relationship between tags and their associated readers. However, it will be difficult for the tags to store all the individual public keys of the readers. In addition, by using stronger and longer keys the processing delay will be increased exponentially. The long processing delay caused by public key authentication gives the intruders an opportunity to perform denial of service attacks against tag authentication. Hence, an intruder can exhaust tag's computational power by sending arbitrary authentication requests, which will result in exhaustive process by the receiving reader. The proposed mutual authentication solution presented in this paper protects contactless RFID tags from unauthorized access. This in turn prevents a range of attacks from affecting the RFID system. In addition, the proposed authentication protocol will reduce the delay and improve the throughput of the RFID network. In this protocol, the mobile agent technology is employed to achieve high efficiency and secure authentication. The delay associated with the mutual authentication protocol will also be reduced by reducing the communication overhead incurred by using public key based solutions [14].

IV. Proposed Authentication Scheme

The proposed solution is based on the four basic requirements for the RFID security including confidentiality integrity and authentication. Till now a model for security solutions of two basic requirements that are confidentiality and authentication could be designed. Hence the security model is derived as follows:

A. Agent Based Confidentiality Model for RFID System

Confidentiality in RFID system is defined as the ability to keep data secret from all but a set of authorized tags and readers. On the other hand, the integrity is defined as the ability to verify that data has not been altered either accidentally or maliciously. Recent research has demonstrated that these properties can be compromised by physically capturing network tags and extracting their cryptographic keys. Such tag capture attacks are possible due to the unattended operation of wireless tags and prohibitive cost of such low-cost devices. By using the cryptographic keys recovered in tag capture attack, an attacker can compromise the integrity and confidentiality of any secured messages. Thus, in RFID the ability to conceal the messages from an attacker and keep them confidential is the most challenge issue in RFID security. Therefore, neither the tag nor the reader should reveal their data to surrounding entities, and confidentiality should prevent attackers from gaining any access to the legitimate tags or readers. Therefore, establishing and maintaining confidentiality is extremely important when Tag's ID's and keys are being distributed to establish a secure communication channel among RFID entities.

The proposed model has three phases: (1) the key distribution phase, (2) the control phase, and (3) the MA migrating phase. With the help of MA the agent can migrate at any entity during its execution. Furthermore, the mobile agent will propagate itself from the reader to destination tags incrementally, running the mutual authentication processes as shown in Fig. 2. The research work in this paper schedules mobile agent execution in a way that improves the authentication and integrity of tags.

B. The Key Distribution Phase

This phase will take place before the deployment of the tags in the RFID network. In this paper, a secure communication channel between the back-end server and the readers, and insecure communication channel between the readers and their tags is assumed. The back-end server in this phase generates a key range for each tag (Ti) using a lightweight cryptography algorithm such as RC4 \(RC) concatenated with a timestamp (TS) sent to the reader from the database. For each Ti, RC the tag calculates a hash value (H) using its identity (IDi) concatenating with the timestamp TS, where the reader always computes a hash function in response to the reader H{IDi (TS|Ti)}. Then the legitimate tag replies back to reader H(IDi|Ts). Therefore, the tags are authenticated with their ID's and the hash values which is generated in every session making it impossible for malicious tag to predict the response messages. Clearly, the initial key distribution is performed before the deployment of the tags in a manner that minimize the computation power and communication cost.

C. The Control Phase

This phase will take place after deployment of tags in the RFID system, where each tag is associated to a unique secret key (Ki) generated by the back-end server and the reader performs a search ID procedure to retrieve the corresponding secret key to identify and authenticate a given tag. To prevent malicious readers from accessing tag contents, each tag (Ti) assigns a key (Ki), which is hashed and time stamped with H to yield a H(Ki|TS), and the tag just store H, not Ki. Meanwhile, the legitimate readers are given the keys of the tags they can exchange.

The tag responds with the non-reversible hash H whenever the reader queries the tag. Now, the reader can simply identify the authorized tag and respond to it using a generated random number r encrypted with Ki and response to the tag with RC (Ki, ID|r). Only at that point the tag unlocks and sends its true identity ID. The random number is used in this phase to enhance the level of security and to make sure that the reader always gets different response from the tag in each session of authentication.

D. The MA Migrating Phase

To confirm tag's authentication, tag send query to the mobile agent which is a running program that carries out a task on the reader behalf [15]. Therefore, the mobile agent requests tag's ID (IDi) to identify a given tag. After tag's ID is authorized, the mobile agent requires authentication process with hash H to verify the authentication process via the selected reader S1. Upon receiving the request, the reader communicates with the end-back server and checks the validity of the tag and then authenticates the tag.

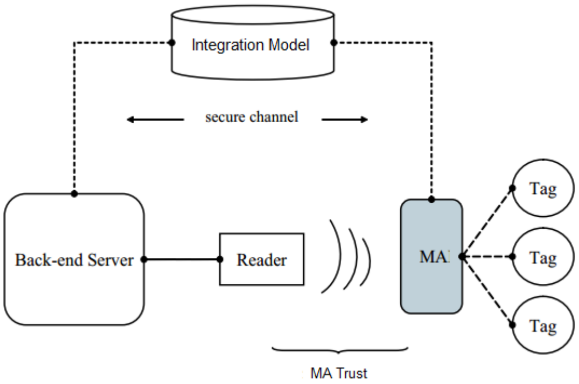

Fig. 2 Mobile agent based architecture in RFID system

Clearly, the server has a lookup table containing the tag's information and its identification (IDi). Therefore, the server receives the tag's information with hashed data from the reader {H{IDi (TS|x)}, where x defines the reader request. Upon comparing the tags data with the information stored in the database of the server, the server would then authenticate the tag. With the help of MA the agent can migrate at any entity during its execution. The MA will propagate itself from the reader to destination tags incrementally, running the mutual authentication processes as illustrated in Fig. 2. Moreover, to ensure integrity and confidentiality, the tag's data must be encrypted with the Ki as mentioned in the second phase of the authentication process. The agent originator signs the final en65capsulated message using the RC algorithm and sends it to the next selected reader S2 with the agent message. The agent form S1 then migrates to S2 with the encapsulated message in order to forward the authenticity and integrity process.

V. Security Analysis and Simulation Results

In order to integrate authentication and integrity features into NS-2 for RFID system, an authentication mobile agent into NS-2 simulation model should be added. Indeed, the built-in class (Authent_Agent) derived from NS2 was used. To ensure the authentication of transferred data, a hash function was implemented within a new class. Also, a security class was built to the encrypted data. The integration is being simulated taking multiples of 100 tags into consideration. Simulation result shows that the paper takes care of cloning attack, sniffing attack, Denial of Service attack, and location traceability attack. By utilizing different integration codes that use mobile agent to authenticate the tags, the RFID created a defense mechanism against these attacks. The simulation result shows that 39% increase in reliability of readers and tags compared to the RFID which utilizes non authentication protocols as shown in Fig. 3.

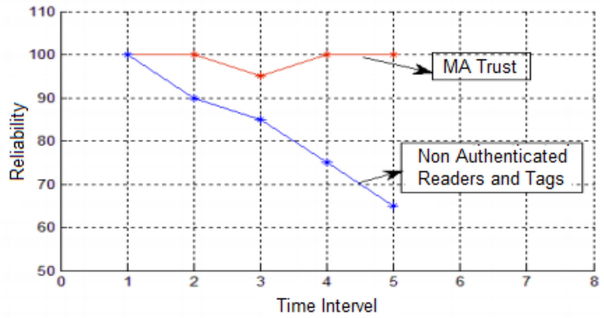

Fig. 3 Authentication characteristics comparison

In cloning attack where attackers compromise genuine tags, the simulation result shows that the tag will be able to validate the authenticity of the reader and its associated tags. The proposed integration solutions were able to identify clone attack with high detection probability, and the defense against clone attack is increased by 34% utilizing mobile agent trust approach as shown in Fig. 4.

To prevent sniffing attack from capturing secret keys or other stored data in the tag, the proposed integration method improves the tamper-proofing system and the encoded settings of the queried tags. With the aid of the hash function which is based on a unique tag ID and timestamp, it is impossible to sniff a tag or tamper with its communicated data. For location traceability attack, the proposed model can detect whether the reader is a legitimate or malicious, because the tag is authenticated in every session of communication, which make it impossible to track a specific tag location.

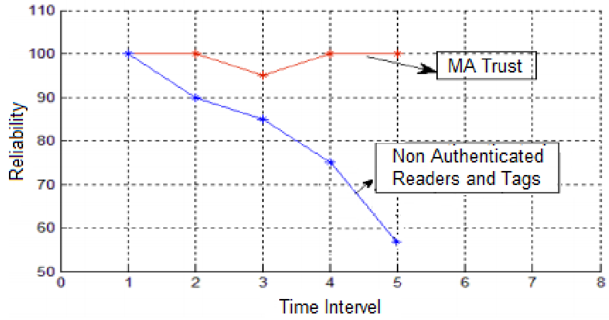

Fig. 4 Architecture and operation of the sensor node

VI. Conclusion and Future work

In this paper, firstly the attacks were summarized, corresponding security requirements and challenges in RFID systems. Then, a secure mutual authentication scheme for RFID systems based on mobile agent technology integrated with timestamp information to authenticate and secure the communication between RFID readers and tags was proposed. Additionally, to ensure confidentiality and integrity, the tag's data were encrypted with a lightweight cryptography algorithm (RC4).

The simulation results showed that the proposed mutual authentication protocol can be used to validate the authenticity of the RFID readers and their associated tags. The results showed also the effectiveness of the proposed algorithm in identifying clone attack with high detection probability. To prevent sniffing attack from capturing sensitive information from the RFID tags, the proposed method improved the authenticity of the tags and provided better tamper-resistance. The authentication approach described in the paper will hopefully motivate future researchers to come up with more effective authentication protocol and make the RFID network safer.

References

[1] R. Weinstein "RFID: A technical overview and its application to the enterprise," IEEE IT Prof., vol. 7, no. 3, pp.27 -33, 2005.

[2] Young-Jae Park and Young Beom Kim, “Accelerating RFID Tag Identification Process with Frame Size Constraint Relaxation,” Journal of Information and Communication Convergence Engineering, vol.10, no.3, pp. 242-247, 2012.

[3] Antonio, F.S.; Ramos Jose, L.H., Moreno, M.V. “A decentralized approach for Security and Privacy challenges in the Internet of Things,” In Proceedings of the IEEE World Forum on Internet of Things, Seoul, Korea, pp. 67–72, 2014.

[4] Kim, K., Jeon, J., and Yoo K. “Efficient and secure password authentication schemes for low-power devices,” International Journal of Security Network, vol.2, no.4, pp.77-81, 2006.

[5] Y. Lee, L. Batina, D. Singelee and I. Verbauwhede "Low-cost untraceable authentication protocols for RFID," Proc. of 3rd ACM Conf. Wireless Network Security (WiSec 2010), pp.55 -64, 2010.

[6] Miao, J.; Wang, L., “Rapid Identification Authentication Protocol for Mobile Nodes in Internet of Things with Privacy Protection,” J. Netw, vol.7, no.3, pp. 1099–1105, 2012.

[7] Liu and A. Bailey "A privacy and authentication protocol for passive RFID tags,” Computer Communication, vol. 32, no. 7, pp.1194 -1199, 2009.

[8] Y. Tian, G.L. Chen, and J.H. Li, “A new ultra lightweight RFID authentication protocol with permutation,” IEEE Communications Letters, vol. 16, no. 5, pp. 702–705, May 2012.

[9] Tagra, D., Rahman, M., and Sampalli, “Technique for preventing DoS attacks on RFID systems,” In 18th international conference on software telecommunications and computer networks (SoftCOM’10), IEEE Computer Society, 2010.

[10] T. Eisenbarth, S. Kumar and C. Paar "A survey of lightweight-cryptography implementations," IEEE Des. Test Comput., vol. 24, no. 6, pp.522 -533, 2007.

[11] J. Lim, H. Oh and S. Kim, "A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection,” Proc. of 4th Int. Conf. Inf. Secur. Pract. Exper. (ISPEC), pp.278 -289, 2008.

[12] S. Kang, D. Lee and I. Lee "A study on secure RFID mutual authentication scheme in pervasive,” Computer Communication., vol. 31, no. 18, pp.4248-4254, 2008.

[13] Stallings W., “Cryptography and network security, principles and practices”, Practice Hall., 2006.

[14] Y. Liao and C. Hsiao “Advances in Intelligent Systems and Applications,” Springer-Verlag, pp.1 -13, 2013.

[15] Shen J, Choi D, Moh S, Chung I. “A novel anonymous RFID authentication protocol providing strong privacy and security. In Multimedia Information Networking and Security (MINES),” International Conference on., pp. 584-588., 2010.