Proceedings of the 5th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/99/20251748

Research on Comparison of Security Protocols for RFID Systems

Zheng An[1,a,*]

[1]*College of Electronics and Information Engineering, Tiangong University;Tianjin, 300387, China*
a. zanzel117z@gmail.com
**corresponding author*

Abstract: As the adoption of Radio Frequency Identification (RFID) technology continues to expand, concerns about its security have grown in significance. And the study of RFID security protocols aims to enhance system security and to provide solutions that can be applied to a variety of scenarios. Therefore, this paper delves into the security protocols employed in RFID technology, investigating their applications across a range of domains such as logistics tracking, financial payments, and access control systems. Besides, through a combination of literature review and comparative analysis, the study provides an in-depth exploration of the working principles, strengths, weaknesses, and suitable use cases of protocols based on cryptography, challenge-response, and time-based mechanisms. The results indicate that cryptography-based protocols perform well in high-security environments such as financial payments, albeit with high computational complexity. Challenge-response-based protocols enhance authentication in access control systems, while time-based protocols successfully mitigate replay attacks through timestamping mechanisms, making them ideal for intelligent transportation systems. In short, each security protocol presents distinctive strengths, and the selection or integration of these protocols should be tailored to specific application scenarios to create more secure and reliable RFID systems.

Keywords: RFID Technology, Security Protocol, Timestamp, Security Mechanism.

1. Introduction

RFID technology, or Radio Frequency Identification technology, is an automatic identification method that facilitates non-contact data communication via radio waves. It utilizes the characteristics of radio frequency signals and their spatial coupling to facilitate the automatic identification and data exchange of both stationary and moving objects. The RFID system primarily consists of three components: tags, readers, and data processing systems. Tags are affixed to the objects to be identified and store specific information about those objects. Readers emit radio waves at a specific frequency to activate the tags and retrieve their internal data. The data processing system then processes the collected information to facilitate data recognition, transmission, and management. [1]. Despite its extensive application, RFID technology still encounters research gaps in security protocols, particularly regarding adaptability and performance optimization for various application scenarios. RFID tags may be vulnerable to security risks, including unauthorized reading, data tampering, and tracking and positioning threats [2]. Thus, the paper employs literature

DOI: 10.54254/2755-2721/99/20251748

review and comparative analysis to investigate the working principles, advantages, disadvantages, as well as applicability of those protocols in various scenarios. Also, it can present optimization strategies for the secure design of RFID systems, thereby enhancing their overall security and efficiency.

2. Classification and Mechanism of RFID Security Protocol

2.1. Cryptography-based Security Protocol

Cryptography-based protocols achieve secure services in network environments by applying various cryptographic algorithms and protocol logic, including entity authentication, key distribution, as well as information non-repudiation. Core cryptographic algorithms such as symmetric keys, asymmetric keys, hash functions, and pseudo-random number generators can provide encryption and decryption capabilities, and the protocol logic ensures the accurate application of these functions to achieve the desired security goals. They are widely used in financial, commercial, and military applications to safeguard the confidentiality, integrity, authentication, and anonymity of networked information. In specific security protocols, hash-lock protocols and DES-RFID mutual authentication protocols are prominent [3]. In the hash-lock protocol, the reader initiates an authentication request, and the target tag responds by sending its identifier from internal memory. Upon successful verification, the backend system sends only a key fragment to the reader. In contrast, the DES-RFID mutual authentication protocol generates a random number encrypted by the tag, which the reader verifies to enable a reverse request. If the match is successful, data operations can proceed. If the match is successful, data operations can continue [4]. These protocols greatly enhance security, securing data transmission through encryption and hashing mechanisms, while also supporting mutual authentication. They are also scalable and adaptable to various needs. However, there are challenges, including computational complexity and resource consumption, especially in the resource-constrained RFID system. Despite their intention to enhance security, hash-lock protocols can be susceptible to impersonation and replay attacks, while protocols based on DES algorithms run the risk of insufficient security.

2.2. Challenge-Response-based Security Protocol

Challenge-response-based security protocols aim to enhance the security of communication between two parties through mutual authentication mechanisms. The challenger generates a random challenge and sends it to the responder, who encrypts or hashes the challenge using a pre-determined algorithm or key and identity information. This produces a response that is returned to the challenger, who confirms the authenticity of the respondent's identity by verifying the response, thereby preventing man-in-the-middle and replay attacks. Key examples of these protocols include the random hash-lock protocol and LCAP (Lightweight Authentication Protocol based on Cryptography) [5]. The random hash-lock protocol incorporates random numbers and hash functions; during each verification process, the tag generates a random number and hashes its identifier, sending both to the reader. The reader forwards this information to the backend database for validation. Because of the variation in random numbers, an attacker cannot carry out subsequent attacks even if they intercept one set of verification data. LCAP enhances security by automatically updating the tag's ID. In this protocol, the reader generates a random secret and sends it to the tag, which calculates a hash value based on the random number and its identifier and returns this to the reader for database verification. Both protocols strengthen defenses against impersonation attacks by introducing random numbers and dynamic identifiers, improving resistance to forgery or replay, thus ensuring the security and integrity of RFID systems. However, these protocols have drawbacks, including higher computational complexity and resource requirements, which can increase

DOI: 10.54254/2755-2721/99/20251748

hardware costs and energy consumption. The increased hardware requirements may limit their use in low-cost RFID systems. The added complexity may present implementation and maintenance challenges, potentially leading to increased communication overhead and latency. In addition, LCAP may be susceptible to security risks associated with database synchronization, which could result in data inconsistencies and delays in synchronization.

2.3. Time-based Security Protocol

Time-based security protocols aim to enhance communication security by utilizing timestamps or time-related mechanisms. These protocols prevent replay attacks by ensuring the timeliness and freshness of information. During the transmission of information, timestamp data is included. When verifying information, the receiver not only checks the accuracy of the content but also confirms that the timestamp falls within an acceptable time range to validate the information's integrity and the sender's authenticity [6]. Taking the TIMELINE protocol as an example, the workflow is as follows: first, the reader generates a timestamp T and sends it to the tag. Upon receiving timestamp T, the tag processes it based on predefined conditions. If T minus a specific value is less than or equal to 0, or greater than the set maximum value Tmax, the tag uses a pseudorandom number generator (PRNG) to generate a new random number P, which becomes one of the tag's attributes. If neither condition is met, the tag retains the original timestamp T and applies HMAC encryption, resulting in the same P [7]. In the protocol's real-time mode, the reader immediately proceeds to the next step after receiving the P value; in batch mode, the reader may wait a period before continuing. The reader then sends the timestamp T and the processed P value to the server. The server searches for the combination of T and P in a hash table (HASH_TABLE). If the combination is not found (return value -1), the server generates an error message TAG-ERROR and sends it back to the reader. If found, the server generates a verification message, which could be an encrypted value or simply VALID, indicating successful verification, and ultimately sends the result to the reader. The advantages of this protocol include reduced protocol overhead, simplified implementation, rapid verification, and effective prevention of replay attacks. Compared to methods using Nonce (one-time random numbers), the timestamp mechanism lowers the additional information exchange required, thus reducing overhead. Its implementation is relatively straightforward, requiring only the inclusion of timestamps in the information and verification on the receiving end, with timestamp validity checks typically being quick, especially beneficial in distributed systems for improving response speed. Furthermore, by checking the freshness of timestamps, it effectively prevents the replay of outdated information, thereby enhancing system security. However, timestamp-based protocols also have drawbacks. First, they have a high requirement for clock synchronization. Second, the system clock must be sufficiently accurate. Third, timestamp-based protocols are vulnerable to timing attacks [8].

3. Frequency of Protocol Utilization and Contextual Applications

3.1. Frequency of Protocol Utilization

The security protocols can be classified according to their application scenarios, characteristics, and practical requirements [9]. Cryptography-based security protocols boast high encryption strength and are widely used in scenarios requiring a high level of security, such as financial payments. And they leverage complex encryption algorithms and keys to effectively ensure the confidentiality, integrity, and availability of data. Due to the maturity and reliability, cryptography-based protocols have become one of the fundamental technologies in network security. Though their computational complexity may pose limitations in certain scenarios with high performance requirements, their broad applicability across various applications and the trust accumulated over the years have

DOI: 10.54254/2755-2721/99/20251748

maintained their frequency of use at a high level. Challenge-response-based security protocols enhance security through a mutual authentication mechanism, making them widely used in areas such as access control systems and logistics tracking. The mutual authentication feature of these protocols can effectively prevent replay attacks and man-in-the-middle attacks. The challenge-response mechanism can be customized according to different application requirements, providing flexible security solutions. While their computational complexity is moderate, the security and flexibility of these protocols maintain a medium to high frequency of use in practical applications. Time-based security protocols are suitable for scenarios requiring high real-time performance and security, such as intelligent transportation systems and real-time inventory management. However, these protocols have high requirements for clock synchronization, which can pose challenges in distributed or complex network environments. Issues related to time synchronization and potential timing attacks contribute to a moderate frequency of use for this type of protocol. Additionally, implementing time-based security protocols may require additional network protocols or hardware support, increasing system complexity and costs.

3.2. Contextual Applications

In financial payments, cryptography-based, challenge-response-based, and time-based protocols each have their own characteristics, but cryptography-based protocols are usually more appropriate given the security, efficiency, and complexity. Financial payment systems require a high level of security to ensure the confidentiality, integrity and availability of transaction data. Cryptography-based security protocols, such as AES and RSA, provide robust password protection, effectively prevent data leakage and tampering, and fulfill high standards of security requirements [10]. Challenge-response-based protocols, though excellent in authentication, cannot provide comprehensive cryptographic protection for transaction data, while time-based protocols, although preventing replay attacks, may increase complexity due to clock synchronization issues. In access control systems, challenge-response-based protocols are considered to be more appropriate than password-based and time-based protocols [11]. While the focus of access control systems is on fast and accurate authentication, challenge-response protocols effectively improve the security of authentication by dynamically generating challenges and requesting an immediate response, which can prevent replay attacks and impersonation. In addition, the challenge-response protocol has moderate implementation complexity, easy integration, and a fast response process, which meets the requirements for efficiency and real-time performance. In contrast, password-based protocols, while excellent in cryptographic protection, are cumbersome in access control, and time-based protocols ensure the freshness of information but may not be as direct and real-time as challenge-response mechanisms. In intelligent transportation systems, cryptography-based and challenge-response-based security protocols each have significant advantages, time-based security protocols are more suitable for some specific scenarios. ITS emphasizes real-time data processing and decision-making, and has strict requirements on the timeliness and freshness of information. By introducing the timestamp mechanism, time-based security protocols effectively verify the freshness of information and prevent replay attacks, especially in scenarios such as vehicle position update, traffic signal control, and emergency event notification. ITS involves collaboration between devices on a large scale, and time-based security protocols can strengthen this foundation. Thus, considering the requirements of ITS for real-time, data freshness and system coordination, time-based security protocols show higher applicability and advantages in ITS applications [12].

DOI: 10.54254/2755-2721/99/20251748

4. Comparison of Protocols and Recommendations for Improvement

4.1. Comparative Analysis

In terms of security, password-based security protocols ensure data confidentiality, integrity and availability through complex encryption algorithms and key management mechanisms, providing a high level of security that is difficult to crack. Challenge-response based security protocols enhance authentication by dynamically responding to challenges, can effectively prevent replay attacks and man-in-the-middle attacks, and are highly flexible and applicable to different scenarios. Time-based security protocols, on the other hand, rely on the freshness of timestamps to ensure the timeliness of information, but clock synchronization issues may affect their security. In terms of performance, cryptographic-based security protocols may consume a large amount of computational resources during encryption and decryption operations, especially when dealing with large amounts of data. The efficiency problem is gradually mitigated as hardware performance improves and cryptographic algorithms are optimized. Challenge-response based security protocols generally exhibit high efficiency due to the relatively simple process, while time-based security protocols are also efficient, but the complex clock synchronization may affect the overall efficiency. In terms of applicability, password-based security protocols are the most commonly used due to their wide range of application scenarios and mature technology base, while challenge-response-based protocols rank second and are suitable for security needs in specific situations. Time-based security protocols, on the other hand, are used less frequently and are mainly constrained by factors such as application scenarios and cost. Password-based protocols are prioritized for high security requirements; challenge-response-based protocols are appropriate choices when fast authentication is required; and time-based protocols should be considered when ensuring information freshness or preventing replay attacks.

4.2. Recommendations for Improvement

For cryptography-based security protocols, optimization strategies should include adopting more advanced encryption algorithms (such as AES-256) to enhance encryption strength and strengthen the security of key management systems, especially introducing centralized management and automatic update mechanisms to improve the confidentiality and integrity of keys. In addition, the use of hardware acceleration technologies can significantly improve the speed of encryption and decryption, optimize the protocol process to reduce unnecessary steps, and integrate other security mechanisms to build a more comprehensive security protection system [13]. For challenge-response-based protocols, optimization measures include designing diverse challenge mechanisms and introducing dynamic elements to enhance the randomness and unpredictability of challenges and increase the difficulty of cracking [14]. Meanwhile, strengthen the response verification mechanism to ensure the accuracy and integrity of the response, and combine multi-factor authentication technologies to enhance the security of identity authentication. Optimizing the protocol process, eliminating unnecessary interaction steps, and implementing a cache mechanism can improve execution efficiency, and design a reasonable error handling and retry mechanism to solve the problem of challenge failure or response error. For time-based protocols, improvement strategies include using high-precision time synchronization technologies (such as NTP and PTP) to ensure system time consistency and prevent time errors from affecting protocol validity. At the same time, design a secure timestamp generation and verification mechanism to ensure the accuracy and uniqueness of timestamps and prevent replay attacks. Adjusting the accuracy and validity period of timestamps according to application requirements can enhance the adaptability of the protocol, and optimizing protocol performance to reduce the

DOI: 10.54254/2755-2721/99/20251748

additional overhead caused by time processing is also an important measure to improve overall efficiency.

4.3. Impact of Future Technologies on Security Protocols

As technology continues to advance, future changes will have a profound impact on existing security protocols. The rise of quantum computing poses a threat to cryptographic-based security protocols and may crack encryption algorithms that rely on large number factorization and discrete logarithms (such as RSA and ECC) [15]. Therefore, there is an urgent need to develop post-quantum cryptographic algorithms, such as lattice-based cryptography and multivariate cryptography. Meanwhile, emerging technologies such as homomorphic encryption and hash-based digital signatures also provide options for enhancing security. In terms of challenge-response security protocols, the integration of biometric technology has significantly improved the accuracy and security of authentication [16]. Mature fingerprint, facial and iris recognition technologies can enhance the reliability of challenge-response protocols. Besides, with the rapid growth of IoT devices, traditional protocols face new authentication challenges, and lightweight solutions need to be designed to adapt to resource constraints to ensure efficiency and security. For time-based protocols, advances in time synchronization technology have improved their accuracy and reliability. High-precision time synchronization methods ensure system time consistency, thereby improving protocol effectiveness. At the same time, blockchain technology provides a new solution for timestamps, enhancing their credibility and overall security, and improving the traceability of protocols by recording timestamps and transaction information [17].

5. Conclusion

The results demonstrate that the analysis of the three main security protocols in RFID systems, cryptography-based, challenge-response-based, and time-based, reveals their respective advantages and disadvantages in different application scenarios. Cryptography-based security protocols dominate in high-security-demand fields such as financial payments due to their high encryption strength and reliability, albeit with higher computational complexity. Challenge-response protocols achieve a balance between security and efficiency in scenarios like access control and logistics through a two-way verification mechanism. Meanwhile, time-based security protocols effectively prevent replay attacks through timestamp mechanisms in real-time-critical scenarios like intelligent transportation. In the future, as RFID technology becomes more widely applied and security threats continue to evolve, there is a need to continually optimize existing protocols and integrate new technologies such as quantum cryptography, biometrics, and time synchronization, so as to build safer, more efficient, and flexible RFID systems that cater to the diverse security needs across various scenarios.

References

[1] *Rong, C., et al. (2013) RFID security. In Computer and Information Security Handbook, Morgan Kaufmann, 345-361.*

[2] *Singh, A.K. and Patro, B.D.K. (2021) Security Attacks on RFID and their Countermeasures. In Computer Communication, Networking and IoT: Proceedings of ICICC 2020, 509-518.*

[3] *Song, Y. and Long, Z. (2020) Design of Authentication Protocol Based on Hash Function. Scientific Journal of Technology, 2(07).*

[4] *Alaoui, H.L., et al. (2023) Authentication Protocol for RFID Systems: A Survey. In 2023 IEEE 6th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), 1-11.*

[5] *Huo, L., Jiang, Y.L. and Hu, L.Q. (2014) Research on hash-based low-cost RFID security authentication protocol. Advanced Materials Research, 846: 1524-1530.*

DOI: 10.54254/2755-2721/99/20251748

[6] *Tewari, A. and Gupta, B.B. (2020). Secure timestamp-based mutual authentication protocol for IoT devices using RFID tags. International Journal on Semantic Web and Information Systems (IJSWIS), 16(3): 20-34.*

[7] *Liang, Z.P. and Wang, Y.L. (2007) A RFID Authentication Protocol Based on Increasing Timestamps. Proceedings of the 17th National Information Security Conference , 187-193.*

[8] *Jha, S.K., Panigrahi, N. and Gupta, A. (2020) Security threats for time synchronization protocols in the internet of things. Principles of Internet of Things (IoT) ecosystem: insight paradigm, 495-517.*

[9] *Munoz-Ausecha, C., Ruiz-Rosero, J. and Ramirez-Gonzalez, G. (2021) RFID applications and security review. Computation, 9(6), 69.*

[10] *Habibi, S., et al. (2024) Design and implementation of a cryptographic algorithm based on the AES advanced encryption standard for UHF RFID systems. Telecommunication Computing Electronics and Control, 22(3): 576-586.*

[11] *Zheng, L., et al. (2018) A new mutual authentication protocol in mobile RFID for smart campus. IEEE Access, 6: 60996-61005.*

[12] *Choy, J.L.C., et al. (2020) Ubiquitous and low power vehicles speed monitoring for intelligent transport systems. IEEE Sensors Journal, 20(11): 5656-5665.*

[13] *Abebe, A.T. (2023) Lightweight and Efficient Architecture for AES Algorithm based on FPGA. i-ETC: ISEL Academic Journal of Electronics Telecommunications and Computers, 8(1).*

[14] *Dai, B., et al. (2020) Research and implementation of cross-chain transaction model based on improved hash-locking. In Blockchain and Trustworthy Systems: Second International Conference, BlockSys, 218-230).*

[15] *Xu, H., et al. (2019) A Novel RFID Data Management Model Based on Quantum Cryptography. In Third International Congress on Information and Communication Technology, London, 437-445.*

[16] *Rukhiran, M., Wong-In, S. and Netinant, P. (2023) IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach. IEEE Access, 11: 22767-22787.*

[17] *Fan, K., et al. (2022) Blockchain-based trust management for verifiable time synchronization service in IoT. Peer-to-Peer Networking and Applications, 15(2): 1152-1162.*