

A lightweight inter-zonal authentication protocol for moving objects in low powered RF systems

C. K. Shyamala*, Anand K. Rajagopalan

Department of Computer Science and Engineering, Amrita School of Engineering,
Coimbatore Amrita Vishwa Vidyapeetham, Amrita University, India

*Corresponding author, e-mail: ck_shyamala@cb.amrita.edu

Abstract

Automatic identification systems represent a wide classification of devices used primarily in commercial settings for inventory/logistics control. Familiar examples of such devices are bar codes, magnetic strips, smart cards, RFID (Radio frequency identification) and biometric and voice recognition. Security is especially lax in low powered RF (radio frequency) systems communicating through an unsecured radio wave channel. Security represents a critical component for enabling the large scale adoption of automatic identification systems. Providing an effective security solution for low powered systems is a major area of concern; it directs research towards 'power consumption aware' computations in security solutions. This paper proposes a Lightweight Inter-Zonal Authentication Protocol for moving objects in low powered RF systems. Formal validation and a thorough analysis of the protocol in SPAN security tool reveals its effectiveness and resiliency to attacks—eaves dropping, reader and tag impersonation, replay and desynchronization.

Keywords: lightweight, RF systems, security, zonal authentication

Copyright © 2017 APTIKOM - All rights reserved.

1. Introduction

Though identification systems may employ smart cards, magnetic strips, RFID (Radio Frequency IDentification), biometric and voice recognition, they are currently predominantly barcode systems. Technological advancements impose the necessity for real-time data acquisition, compelling systems to become assertive in terms of tracking and monitoring. In recent times, there has been an increased deployment of low powered RF systems for tracking and monitoring of different objects like assets, humans, vehicles etc. Low powered RF devices provide considerable advantages over barcodes—data can be read automatically without the object being in line of sight of a reader or system authenticator. Moreover, data can be sent at a rate of hundreds of data units per second, and from a distance of several meters (depending on the area of coverage of the RF system). Open wireless communication channels in RF systems are similar to wireless mobile communications. As a result, the system air interface is susceptible to security threats and attacks similar to those in wireless mobile communications. Security issue becomes a key concern and the systems are designed to provide effective security. Reliable security solutions for RF applications demand security requirements with respect to authentication, integrity, privacy, anonymity, session freshness, synchronization. Interesting threads of research in this direction have been the focus of [1]-[6]. As RF systems are chiefly low-powered, it is important that the security solutions take into consideration computing overheads. Light weight schemas have become the focus of research for securing RF systems [7]-[12].

Survey in [13], [14] examine and bring out several aspects related to low powered RF system security. Security threats to RF systems can be put into several classes [15], [16]; Sniffing (or Eavesdropping), Spoofing, Cloning, Replay, Relay, and Denial of Service attacks. Any form of unauthorized access to the objects fall under the category of eavesdropping/sniffing. A rogue authenticator may read sensitive and confidential data of an object, record it and use it to breach authentication data exchanges. The highest level of security risk to a low powered RF systems network is sniffing/eavesdropping attack [15]. Spoofing attacks involve rogue entities not only secretly scanning and recording data transmissions from a legitimate object but also copying the object's ID and making itself appear to be valid. Replay attack involves using an object's response to an authenticator's challenge to impersonate the object [17]. These attacks can be countered in RF systems by providing privacy protection and authentication [1], [2], [7], [18-20].

RF systems use low cost tag/label for identifying objects and obviously are restricted in terms of storage capacity and computational power [21]. Low powered RF systems need to benefit from light weight solutions to security. Use of simple operations and limited cryptographic functionalities permit minimum levels of computations and energy consumptions, while at the same time supporting cryptographic goals of security. Security solutions for RF systems can be classified by the weight of cryptographic primitives used- Middle-weight, light-weight and ultra-lightweight solutions. Middleweight solutions [22], [23] for applications with higher security requirements such as finance, and military) use full symmetric/asymmetric encryption (e.g., elliptic curve cryptography (ECC)). Lightweight solutions use operations and functions such as cyclic redundancy code (CRC) operator, message authentication code (MAC) and hash function. While research has focused on light weight solutions for RF systems security, the studies from [8]-[10] suggests the use of simple and basic bitwise logical operations, shift operations and pseudo-random number generator (PRNG) which support the least computationally demanding class called the ultra-lightweight.

Proposes a light weight mutual authentication and ownership management scheme by using limited cryptographic functionality [1]. The scheme is done in two phases. Phase 1 covers the mutual authentication between entities in a RF system and Phase 2 covers the delegation and ownership managements. Rahman et.al [7] presents a lightweight mutual authentication protocol to achieve basic security goals, i.e. confidentiality, integrity and authentication using a unique choice of pseudorandom numbers. The authentication process in [2] introduces time stamps to help protect tag privacy and prevent the tracking from an attacker. On the other hand, [18] Osaka et al. proposes a light weight security method for RF systems that achieves the security requirements using hash functions, symmetric cryptography, and the XOR operation. This security system achieves several security requirements: the indistinguishability, the forward security, the security against the replay attack, and the security against the tag killing. Further, the proposed method allows for ownership transfer. The proposed method is reasonably efficient, but vulnerable to tracking and DoS attacks brought out by [24]. This is done by manipulating the value of the random number of the tag. Moreover, as brought out in [25], an attacker can add noise to the final message exchange of [18] resulting in the tag holding incorrect secret information, due to which any subsequent authentication would fail.

While [1], [18] have not considered mobile RF systems, [19] implements a light weight authentication for mobile RF system with grouped tags to identify objects. The authentication for tags is based on PRNG mainly because the low-cost tags are restricted in storage capacity and computational power. The Authentication readers are based on hash-function, as reader obviously are not restricted by storage capacity and computation power. The protocol provides security against reader impersonation attack, tag impersonation attack and tracking. Weis et.al [26] proposed a RF system in which the object's identification is hidden using random numbers in the object's responses to avoid its reuse. This system addresses traceability by applying an exhaustive search, but at the cost of an increase in the work load of the back-end server to identify and verify the object. This scheme is vulnerable to impersonation attacks by querying the object for a valid pair and then forwarding this pair to an authenticator for validation. Yu et al.'s [27] protocol uses a 128-bit key set that is dynamically updated by the server. It uses the least significant 30 bits of the tag ID used to identify the object for authentication. However, this results in the possibility of compromising the security of the system as a whole, as the uniqueness aspect of a tag ID to identify an object is reduced, by reducing the number of bits used by the tag ID for authentication.

This paper proposes a Light-weight Inter-zonal Authentication Protocol for moving objects in low powered RF systems. The protocol is designed for 'power consumption aware' computations in security solutions. The work presented in this paper is divided into 3 phases: System Registration phase, zonal authentication phase and mutual authentication phase. In phase 1, the object must register itself to the system authenticator (SA). The RFID network is partitioned into various zones based on the coverage of the authenticator of the RF system in a particular area. In phase 2 and phase 3, several events of handshakes are performed between both the object and ZA, object and IZA to mutually authenticate each other and start communicating. This protocol can be adopted by object monitoring and tracking systems for providing secure and reliable data exchanges. The protocol has been verified against security attacks which include eavesdropping, spoofing, authenticator and object impersonation, replay and desynchronization by using the SPAN security tool for formal validation of the protocol.

The contributions of the work presented in the paper are: (i) A multi-zonal authentication schema resilient to eavesdrop, replay, authenticator and impersonation and desynchronization (ii) An inter-zonal authentication protocol that mutually verifies both the tracked object and the authenticator/reader (iii) A light-weight authentication schema performing PRNG, XOR, XTEA with very less computation overhead [28]. The work presented in this paper contributes to 'power consumption aware' computations in

security solutions. A Lightweight Inter-zonal Authentication protocol for moving objects in low powered RF systems is proposed. The protocol uses ultra-light weight XOR and PRNG functions for passing and decoding random numbers. Time stamps are used in interactive sessions between an object and an authenticator to keep the freshness of the challenge-response information in each communication round. Two or more handshakes between the communicating devices is defined as an event. LC (Logical Clock) value present in the communicating devices increments simultaneously on verification of every event. Each communicating device maintains its own LC value. A mismatch in LC value between communicating devices terminates the communication between them. XTEA (Extended Tiny Encryption Algorithm) is used for both encryption and decryption. Wheeler and Needham in [29] made extension to TEA algorithm (XTEA) which is a lightweight block cipher. The rest of the paper is organized as follows. The proposed work, a 3-phase Light-weight Inter-zonal Authentication scheme is discussed in length in Section 2. Analysis of the proposed protocol in terms of resiliency to security attacks and performance is presented in Sections 3. The formal validation of the proposed protocol using the SPAN security tool is presented in Section 3.5. The paper is concluded in Section 4.

2. Research Method

2.1. RF System Architecture

RF systems largely consist of authenticator and objects; both of which are responsible for verifying the identity of each other invariably ensuring communication with only the intended parties. This paper proposes a Light-weight Inter-zonal Authentication Protocol for moving objects in low powered RF systems. The protocol uses a ticket based authentication approach using cryptographic operations-XOR, PRNG (Pseudo Random Number Generation) and XTEA (Extended Tiny Encryption Algorithm). The multi zonal architecture of the proposed protocol is shown in Figure 1. The architecture includes one SA (System Authenticator) for the entire system. On the onset, the SA registers all the objects to be identified to the system -1 as shown in Figure 1. It is structured to encompass many zones, where each zone defines a geographical region of authentication. The system is partitioned into multiple zones, each employing a ZA (Zonal Authenticator) to authenticate inbound registered objects -2 as shown in Figure 1. Each zone allows communication between objects and Inter Zonal Authenticator (IZA) only after mutual authentication -3 as shown in Figure 1.

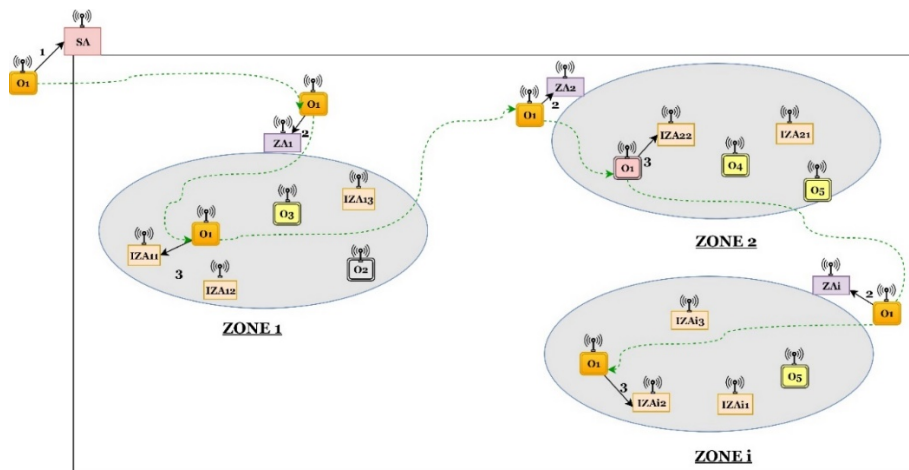


Figure 1. Multi zonal architecture

The proposed mutual authentication protocol is organized to operate in three phases- System Registration phase, Zonal Authentication and Mutual Authentication phase. System registration of an object with the SA generates an encrypted system ticket and sets the identification of the source zone (ID_{ZONE-S}), identification of tag (ID_{OBJECT}) and LC (Logical Clock) value for the object. The Zonal Authentication of an object with the ZA verifies the system ticket and generates an encrypted zonal ticket. The zonal ticket is used for further authentication of the object by an inter-zonal authenticator. The entities and their roles of the multi zonal RF system are explicated in Table 1.

Table 1. Entities and roles

Entity	Role	Data/Information stored and handled
SA	Registers an unregistered object to the RF networked system.	1. A list of registered objects with their identification (ID_{OBJECT}) and default zone identification (ID_{ZONE}) 2. System ticket
ZA	Authenticates the object for the zone.	1. A list of access passwords and LC values for all the registered objects. 2. A list of registered objects and their identification 3. A list of ticket keys (k_{ZA-IZA}) used between the ZA and IZA.
ZR	Communicates with the object after mutual authentication.	1. A list of LC values for all the registered object. 2. A list of registered object and their identification
		ID_{ZONE} , ID_{OBJECT} , LC, System Ticket, Zone Ticket $Ticket_{SYSTEM} = (ID_{OBJECT}, ID_{ZONE-S}, T_0, T_{max}, Timestamp, R+S)k_{ZA-IZA}$
Object	Entity to be authenticated	$Ticket_{ZONE} = (ID_{OBJECT}, ID_{ZONE}, T_0, T_{max}, Timestamp, R+S)k_{ZA-IZA}$

2.2. Proposed Light-weight Inter-zonal Authentication Protocol

The assumptions made in designing the protocol are:

1. All entities in the RF system namely, objects and authenticator trust the System Authenticator (SA) and Zonal authenticator (ZA).
2. The Authenticators (SA and ZA) maintains the list of ticket keys of all the inter-zonal authenticators in the setup.
3. Only the Authenticators (SA and ZA) can access the memory contents of the object to be identified.

The proposed protocol is a three phase mutual authentication protocol. The first phase is the System Registration Phase that registers an object with the RF networked System, generating a System Ticket. The subsequent phase is the Zonal Authentication phase. It authenticates a registered object when it is inbound into a zone, generating a Zonal Ticket. The last phase of the protocol is the Mutual Authentication phase. It mutually authenticates the object in a zone and the inter-zonal authenticator before any application processing is performed by the reader. Notations and terms used in the proposed protocol as shown in Table 2.

Table 2. Notation and Terms

Notation	Description
ID_{ZONE}	Identification number of Zone
ID_{OBJECT}	Identification number of Object
$PRNG()$	Pseudo Random Number function
R, S, U	16-bit Random numbers
$TICKET_{ZONE}$	Ticket for a particular Zone
K_{ZA-IZA}	Key shared by Zonal authenticator and the inter Zonal authenticator
LC	Logical clock-16-bit integer value
T_0	Time of connection establishment
T_{max}	Maximum time until the connection holds without disconnecting
ZA	Zonal authenticator
IZA	Inter zonal authenticator
RN	Random Number
SA	System authenticator

2.2.1. Phase I: System Registration Phase

This phase writes significant data in the memory of the object for authentication to be performed by ZA and IZA. The SA writes ID_{ZONE-S} - Identification number of start zone, ID_{OBJECT} - Identification number of object and LC-Logical clock (16-bit integer value, initially zero) into the objects memory. The SA then sends the system ticket to the object thus registering it in the RF networked system. As shown in Figure 2.

A registered tag contains the following after the system registration phase:

1. ID_{ZONE-S} - Identification number of start zone
2. ID_{OBJECT} - Identification number of object
3. LC – Logical clock (16-bit integer value, initially zero)
4. $Ticket_{SYSTEM} = (ID_{OBJECT}, ID_{ZONE-S}, T_0, T_{max}, Timestamp, R+S)k_{ZA-IZA}$.

A ticket in the proposed protocol is encrypted using the shared secret key K_{ZA-IZA} , between ZA and IZR of a Zone. The encryption with K_{ZA-IZA} is performed to prevent alteration of the contents by any unauthorized entity. ID_{OBJECT} and ID_{ZONE} allow verification of the object and zone. The values T_0 , T_{max} and Timestamp permits verification of ticket validity. A ticket is valid only if (Current timestamp –

Timestamp in the ticket) $< (T_{\max} - T_0)$. The value $(R+S)$ are 16 bit random numbers generated by ZA. $(R+S)$ serves as one of the components for mutual authentication and is available to IZA via the ticket. LC is logical clock that keeps track of the number of times handshakes have been performed for an object in a zone.

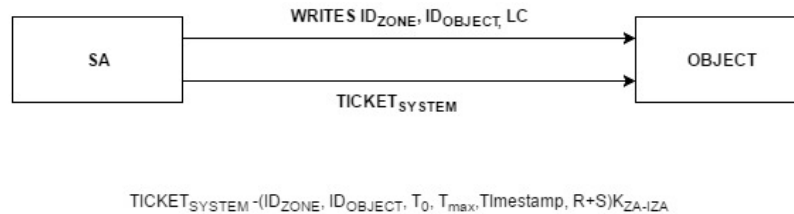


Figure 2. Phase I–system registration: registration of an object with the RF system

2.2.2. Phase II: Zonal Authentication Phase

The RF networked system is partitioned into a number of zones based on the coverage of the RF authenticators, each zone defining a geographical region of authentication. A zone consists of one ZA and multiple IZA's as illustrated in Figure 1. Zonal authentication refers to the authentication of inbound registered objects into any one of the zones in the RF networked system. This process is detailed in Figure 3. ZA of a zone accesses an inbound object by accessing its memory and checks for ID_{ZONE} written in the object at registration or any previous zonal authentication. If the ID_{ZONE} in the object does not match the current zone, then the ZA sets the appropriate ID_{ZONE} , issues a zonal ticket for that zone and resets LC for the registered object. If the ID_{ZONE} matches the current zone, then ZA stores a 16-bit random number S and stores it in the object's memory. It then queries the object for a ticket, this may be a system ticket or a zonal ticket. ZA checks for the ticket's validity and authenticates the object. In case a ticket's validity has expired (invalid ticket), the ticket is renewed at the ZA.

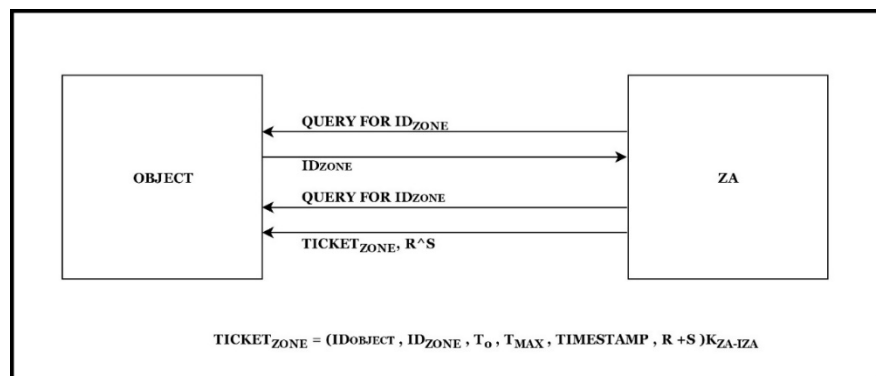


Figure 3. Phase II–zonal authentication phase

After the Zonal Registration Phase, the registered object contains the following:

1. ID_{ZONE} - Identification number of zone.
2. ID_{OBJECT} - Identification number of object.
3. LC – Logical clock (16-bit integer value).
4. $Ticket_{ZONE} = (ID_{OBJECT}, ID_{ZONE}, T_0, T_{\max}, Timestamp, R+S)k_{ZA-IZA}$.
5. S
6. R^S

As depicted in Figure 3 a zonal ticket is issued by ZA along with R^S , the XOR of 16-bit random numbers R and S . XOR operation is commutative and associative in nature. An important property of the XOR operation is the following property: $((A) \wedge (B)) \wedge B = A - (1)$. ZA generates S and stores it in the object's memory. It generates R and sends R^S to the object. The value of R can be

obtained from R^S only if the value of S is known and vice versa. As a result, the object can obtain the value of R from R^S using the value of S stored in it. Using R and S , the object computes $(R+S)$, which serves as one of the components for mutual authentication. It is not possible for an unauthorised entity to obtain R or S from R^S . This property prevents unauthorized/illegal entities from obtaining R and S in order to successfully impersonate as system registered object/authenticator.

2.2.3. Phase III: Mutual Authentication Phase

Registered objects and IZA are mutually authenticated in phase III, before any application processing is performed. Steps 2 and 3 in Figure 4. Account for the handshake performed by the object and IZA towards mutual authentication. IZA queries the object in the zone for $TICKET_{ZONE}$. The object responds by sending $Ticket_{ZONE}$ and $PRNG(R + S + LC)$ to IZA. IZA obtains $R+S$ by decrypting the ticket using the key it shares with ZA. LC of that object is added to $(R+S)$ and $PRNG(R+S+LC)$ sent by the object in step 2 of Figure 4. is verified by IZA by performing the same $PRNG(R+S+LC)$ and comparing the two values. This authenticates the object to the IZA. IZA authenticates itself to the object by sending $PRNG(U)$ and $U^{(R+S)}$. The object obtains U by performing $(U^{(R+S)})^{(R+S)}$. It performs $PRNG(U)$, verifies the $PRNG(U)$ sent by the IZA in step 3 of Figure 4 to authenticate the IZA. After successful authentication, LC is updated by both the object and the authenticators. This phase mutually authenticates the object and IZA ensuring that the communication is with only the intended parties in the RF networked system.

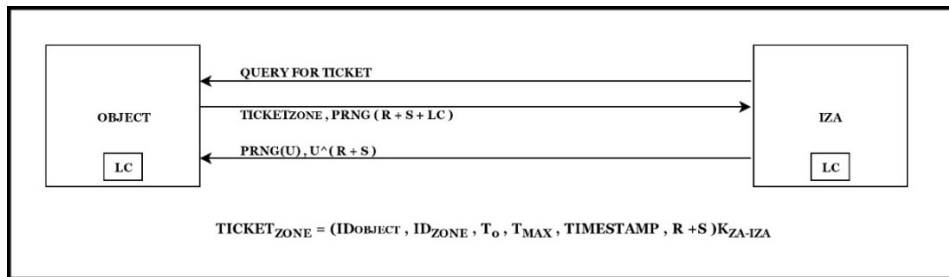


Figure 4. Phase III–mutual authentication phase

XOR and PRNG (Pseudo Random Number Generator) are the main cryptographic operations used in the proposed protocol. Contribution of XOR operation towards securing the proposed authentication scheme has been highlighted in Phase II discussion. $PRNG()$ function generates a random number using a seed. An important property of $PRNG()$ function is that it is a one-way function—the seed cannot be obtained from the random number. It is not possible for an illegal/unauthorised authenticator to obtain the seed (U) and authenticate itself as a legal IZA of the zone. The properties of both XOR and PRNG are exploited to provide a secure authentication protocol that is resilient to eavesdropping attack, Authenticator and object impersonation attack, replay attack and desynchronization attack.

3. Security Analysis and Results

Resiliency of the proposed protocol with respect to different types of attacks is analyzed in this section.

3.1. Eavesdropping Attack

Eavesdropping attack is an unauthorised real-time interception of the communication between an object and an authenticator. An adversary A , may acquire R^S , $PRNG(R+S+LC)$, ticket, $PRNG(U)$ and $(U^{(R+S)})$ from the communication (Phase II and Phase III) between an authenticator and an object. A successful attack can be performed on the RF networked system iff A can perform the following from the intercepted contents:

- a. Decrypt the encrypted system/zonal ticket to obtain its contents
- b. Obtain 16 bit random numbers R, S and U
- c. Obtain LC and compute $R+S+LC$

The proposed protocol is secure against eavesdropping:

- Ticket is encrypted using K_{ZA-IZA} –The eavesdropper cannot gain any valuable information from a ticket without knowing the shared secret key K_{ZA-IZR} .
- It is not possible for an eavesdropper to obtain R or S from $R^{\wedge}S$ or U from $(U^{\wedge}(R+S))$ due to the XOR property in (eqn.1).
- PRNG() function is a one-way function, as a result of this property the eavesdropper cannot obtain the values of $(R+S+LC)$, U from $PRNG(R+S+LC)$ and $PRNG(U)$.

3.2. Authenticator/Object Impersonation Attack

Authenticator-impersonation refers to a process in which an adversary-authenticator A, deceives a registered object to authenticate it as a valid authenticator. Whereas, object-impersonation is the process in which an adversary- object A, deceives a genuine authenticator to authenticate it as a valid object. For authenticator/object- impersonation attacks to be successful, A must perform the following:

- Access memory contents of an object.
- Obtain contents of system/zonal ticket.

The proposed protocol is secure against authenticator/object-impersonation:

- Only the SA and ZA can access the memory contents of the objects as assumed in the protocol. Therefore, an adversary A cannot access the memory contents of the object.
- Tickets in the proposed protocol are encrypted using the secret key (K_{ZA-IZA}) shared between the zonal authenticator and inter-zonal authenticators in a zone. An impersonating authenticator A has to obtain K_{ZA-IZA} , in order to decrypt the ticket and extract the data needed for authentication.

3.3. Replay Attack

Replay attack is performed when an adversary (object or authenticator) A, captures and attempts to reuse the authentication component used in handshake. A captures the authentication component $PRNG(R+S+LC)$ in Phase III, and attempts to replay it (later on) in another authentication session with an authenticator. Logical Clock LC, is an incrementing software counter maintained in each process by which the happened-before ordering can be captured numerically [30]. LC is used in the protocol to resist replay attacks. LC values are updated for each authentication by both the object and IZA. For replay attack to be successful A must has the correct LC value of a particular authentication session. This is not possible as the LC value is updated after every handshake in phase III. In Figure 5(a) LC is updated to LC' by both the object and IZA after handshake in phase III. Figure 5(b) illustrates a replay attack, where A (adversary object) replays the $TICKET_{ZONE}$, $PRNG(R+S+LC)$ captured from the session #n during session #(n+1). Since $LC \neq LC'$, the authentication fails.

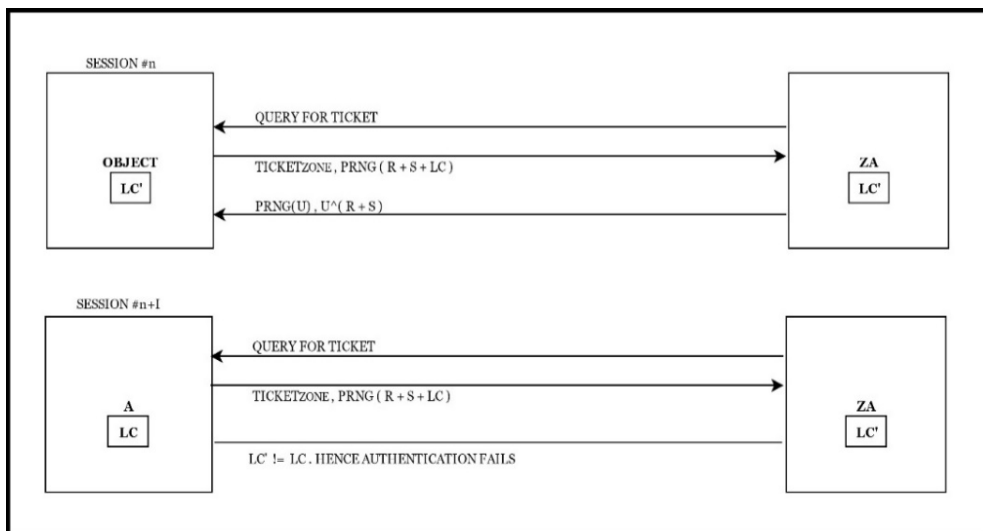


Figure 5. Replay attack

3.4. Desynchronization Attack

An adversary A, performs desynchronization attack with an intent to disrupt the authentication process. A desynchronization attack on the RF system forces the object and authenticator to update their common values to different values. In the proposed protocol, LC is a logical clock that keeps track of the number of times handshakes have been performed for an object in a zone. The LC values are updated by the object and the IZA only after a successful handshake in Phase III. A desynchronization attack can be successful iff the LC updating is desynchronised; LC in the proposed protocol is not updated if the handshake in Phase III is unsuccessful. As a result, the adversary cannot perform a desynchronization attack to disrupt the authentication process of the proposed protocol.

3.5. Performance Analysis

Table 3 illustrates an analysis of the proposed protocol in terms resiliency requirements against eavesdropping, impersonation, replay, and desynchronization. Performance of the proposed protocol is analyzed for the time complexity of the operations (TXOR-time complexity of the XOR operation, TRNG-time complexity of the random number generation operation, TPRNG-time complexity of Pseudo Random number function, TEDC-time complexity of the encryption/decryption cryptosystem) used in mutual authentication. Table 4 projects the total time complexity at an object and an authenticator. The proposed protocol performs 2 XOR operations at the object in Phase II and III, 2 XOR operations at the authenticator in phase II and III. Accounting for a total of 4 XOR operations performed by the object and authenticator at the end of phase II and phase III. The total of 2 PRNG operations is performed by the object in phase III, 2 PRNG operations at the authenticator in phase III. Accounting for a total of 4 PRNG operations performed by the object and authenticator at the end of phase II and phase III. Two Random number generation operations are performed at the authenticator in phase II. Only one encryption/decryption operation is performed at the authenticator in phase II and phase III. Therefore, a successful mutual authentication in a zone requires a time complexity of $2T_{XOR}+2T_{PRNG}$ at the object and $2T_{XOR} + 2T_{PRNG}+1T_{EDC}+2T_{RNG}$ at the authenticator. Object’s data/information may be required to be processed by more than one authenticator in a zone, accounting for multiple authentications. The number of times (x) a object is authenticated in a zone accounts for a total of $x *(4T_{XOR}+4T_{PRNG} +1T_{EDC}+2T_{RNG})$. Performance Analysis of MKT phase (mutual authentication, key update and ticket computation) in [1] is analyzed for the time complexity of the operations (TXOR-time complexity of the XOR operation, TRNG - time complexity of the random number generation operation, TPRNG-time complexity of Pseudo Random number function, TPER-time complexity of permutation operation, T_{MOD} - time complexity of modulus operation) used in mutual authentication.

Table 5 projects the total time complexity at a tag identifying the object and a reader (authenticator). The protocol in [1] performs 75 XOR operations at the tag in MKT phase, 63 XOR operations at the Reader in MKT phase. Accounting for a total of 138 XOR operations performed by the tag and reader at the end of MKT phase. The total of 72 PRNG operations is performed by the tag in MKT phase, 36 PRNG operations at the Reader in MKT phase. Accounting for a total of 36 PRNG operations performed by the tag and reader at the end of MKT phase. 12 permutation operations, 2 Random number generation operations are performed at the reader in mutual authentication phase. 6 modulus operations are performed at the tag in mutual authentication phase. Therefore, a successful mutual authentication requires a time complexity of $75T_{XOR}+36T_{PRNG}+12T_{PER}+6T_{MOD}$ at the tag and $63T_{XOR}+2T_{RNG}+36T_{PRNG}$ at the reader.

Table 3. Comparison of related protocols

Security methods	Eavesdropping	Impersonation	Replay attack	Desynchronization
[1]	Yes	Yes	Yes	Yes
[2]	Yes	No	Yes	No
[31]	Yes	No	Yes	No
[3]	Yes	Yes	No	No
Proposed protocol	Yes	Yes	Yes	Yes

Table 4. The Performance of analysis of the propose protocol

Object	Authenticators(ZA and IZA)
$2T_{XOR}+2T_{PRNG}$	$2T_{XOR}+2T_{PRNG}+1T_{EDC}+2T_{RNG}$

Table 5. The Performance Analysis of mutual authentication, key update and ticket computation in [1]

Object	Reader(Authenticator)
$75T_{XOR}+36T_{PRNG}+12T_{PER}+6T_{MOD}$	$63T_{XOR}+2T_{RNG}+36T_{PRNG}$

Performance analysis in Table 4 and Table 5 infers that the proposed protocol in this paper functions with a lesser time complexity compared to the MKT phase of the protocol proposed in [1].

3.6. Formal Validation of the Proposed Protocol

SPAN is a security protocol animator for HLPSSL and CAS+ specifications that is similar AVISPA (Automated Validation of Internet Security Protocols and Applications). It facilitates analysis of large-scale Internet security-sensitive protocols and applications. SPAN implements an active intruder that allows to interactively find and build attacks over protocols. SPAN automatically build an attack message sequence chart on HLPSSL and CAS+ specification of the protocol using the AVISPA verification tools. CL-Atse is one such AVISPA verification tool. It is an efficient versatile automatic analyser for the security of the cryptographic protocols. State-based security property like secrecy, authentication and fairness can be modelled using the CL-Atse tool and the algebraic properties of operators like XOR or exponentiation are taken into account with much less limitations compared to other tools, thanks to a complete modular unification algorithm. The intruder simulation of the proposed protocol is done using SPAN. The intruder simulation of the proposed protocol is shown in Figure 6. The protocol was found to be safe from intruder attacks. In addition to the intruder simulation, an CL-Atse tool verification for proposed protocol was performed. Figure 7 and Figure 8 displays the CL-Atse tool summary check for the proposed protocol. The proposed protocol was found to be secure against various attacks simulated by the CL-Atse tool.

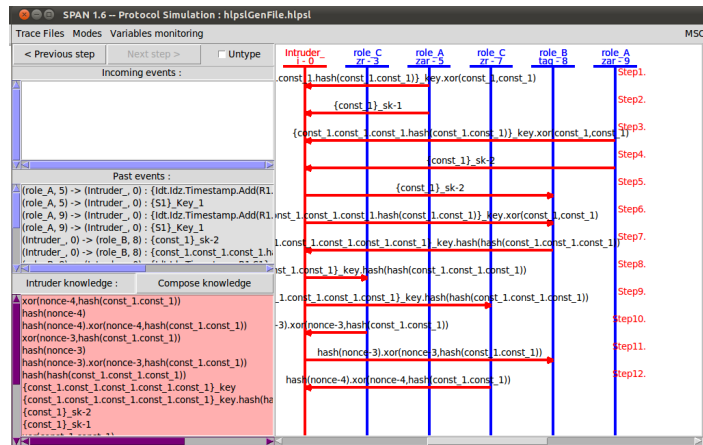


Figure 6. Intruder simulation using SPAN security tool

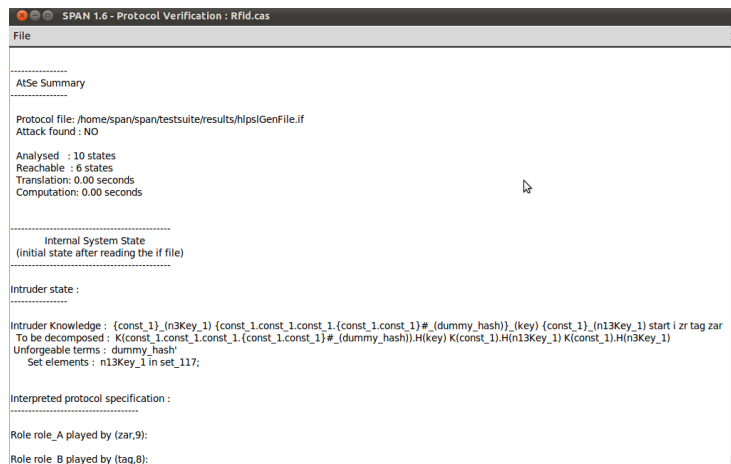
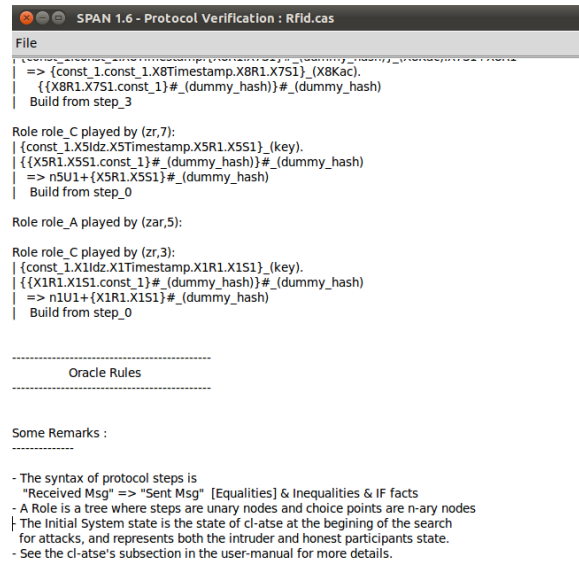


Figure 7. CL-Atse security check output summary



```

File
| {const_1.const_1.X8Timestamp.X8R1.X751}_ (X8Kac).
| {{X8R1.X751.const_1}_#_(dummy_hash)}#_(dummy_hash)
| Build from step_3
|
Role role_C played by (zr,7):
| {const_1.X51dz.X5Timestamp.X5R1.X551}_ (key).
| {{X5R1.X551.const_1}_#_(dummy_hash)}#_(dummy_hash)
| => n5U1+{X5R1.X551}_#_(dummy_hash)
| Build from step_0
|
Role role_A played by (zar,5):
|
Role role_C played by (zr,3):
| {const_1.X11dz.X1Timestamp.X1R1.X151}_ (key).
| {{X1R1.X151.const_1}_#_(dummy_hash)}#_(dummy_hash)
| => n1U1+{X1R1.X151}_#_(dummy_hash)
| Build from step_0
|
-----
Oracle Rules
-----
Some Remarks :
-----
- The syntax of protocol steps is
  "Received Msg" => "Sent Msg" [Equalities] & Inequalities & IF facts
- A Role is a tree where steps are unary nodes and choice points are n-ary nodes
- The initial System state is the state of cl-atse at the beginning of the search
  for attacks, and represents both the intruder and honest participants state.
- See the cl-atse's subsection in the user-manual for more details.

```

Figure 8. CL-Atse security check output summary

4. Conclusion

In this paper, a Light-weight Inter-zonal Authentication Protocol for moving objects in low powered RF systems. This was done by employing the ultra-light-weight the PRNG function and XOR operation. Such use of a simple operation adds a minimal level of computation and energy consumption for low-powered RF systems while, at the same time, supports the cryptographic goals of the protocol. The proposed protocol was verified for security attacks and was formally validated using the SPAN security tool. Analysis of the proposed protocol and comparison with previous works in section 5 and 6 indicate the following: (i) no disclosure of secret information (ii) no dependency on previously used secret data/information (iv) resiliency against niffing/eavesdropping, and replay attacks is guaranteed (iii) the protocol is free from desynchronization issues (v) lower computational complexity (vi) lower time complexity.

References

- [1] Niu, Haifeng, Eyad Taqieddin, Sarangapani Jagannathan. EPC Gen2v2 RFID standard authentication and ownership management protocol. *IEEE Transactions on Mobile Computing*. 2016; 15(1): 137-149.
- [2] Zhang, Changlun, Wenqi Zhang, Haibing Mu. *A mutual authentication security RFID protocol based on time stamp*. Computational Intelligence Theory, Systems and Applications (CCITSA), 2015 First International Conference on. IEEE, 2015.
- [3] Hermans, Jens, Roel Peeters, Bart Preneel. Proper RFID privacy: model and protocols. *IEEE Transactions on Mobile Computing* 2014;13(12): 2888-2902.
- [4] Dharuman, Lavanya, Senthilkumar Mathi. A Time-invariant Scheme for Handover Key Management Using Identity based Encryption in 4G LTE Networks. *Int. J. Contr. Theor. App.* 2015; 8(5): 1823-1830.
- [5] Mathi, Senthil Kumar, M L Valarmathi. An efficacious and secure registration for internet protocol mobility. *Defence Science Journal*. 2013; 63(5): 502-507.
- [6] Mathi, Senthilkumar, Lavanya Dharuman. Prevention of Desynchronization Attack in 4G LTE Networks Using Double Authentication Scheme. *Procedia Computer Science*. 2016; 89: 170-179.
- [7] Rahman, Musfiq, Raghav V. Sampangi, Srinivas Sampalli. *Lightweight protocol for anonymity and mutual authentication in RFID systems*. Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE. IEEE, 2015.
- [8] Pedro Peris-Lopez, et al. *Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol*. International Workshop on Information Security Applications. Springer. 2008.
- [9] D'Arco, Paolo, Alfredo De Santis. On ultralightweight RFID authentication protocols. *IEEE Transactions on Dependable and Secure Computing*. 2011; 8(4): 548-563.
- [10] Tian, Yun, Gongliang Chen, Jianhua Li. A new ultralightweight RFID authentication protocol with permutation." *IEEE Communications Letters*. 2012; 16(5): 702-705.
- [11] Ahmed Eslam Gamal, Eman Shaaban, Mohamed Hashem. Lightweight mutual authentication protocol for low cost RFID tags. *arXiv preprint arXiv:1005.4499* (2010).

- [12] Grimaila Michael. RFID security concerns. *ISSA Journal*. 2007: 30-35.
- [13] Ari Juels. RFID security and privacy: A research survey. *IEEE journal on selected areas in communications*. 2006; 24(2): 381-394.
- [14] Avery Williamson, et al. Solutions for RFID smart tagged card security vulnerabilities. *AASRI Procedia* 2013; 4: 282-287.
- [15] Amit Grover, Hal Berghel. A survey of RFID deployment and security issues. *Journal of Information Processing Systems*. 2011; 7(4): 561-580.
- [16] Shih, Dong-Her, Chin-Yi Lin, Binshan Lin. RFID tags: privacy and security aspects. *International Journal of Mobile Communications*. 2005; 3(3): 214-230.
- [17] Burmester, Mike, Breno De Medeiros. *RFID security: attacks, countermeasures and challenges*. The 5th RFID Academic Convocation, the RFID Journal Conference. 2007.
- [18] Osaka, Kyosuke, et al. An efficient and secure RFID security method with ownership transfer. *RFID security*. Springer US, pp. 147-176, 2008.
- [19] Litian, Duan, Duan Fu, Wang John Zizhong. *A Mixed and Batching Authentication Protocol for Grouped Tags in Mobile RFID System*. Data Science and Data Intensive Systems (DSDIS), 2015 IEEE International Conference on. IEEE, 2015.
- [20] Chien, Hung-Yu, Che-Hao Chen. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Computer Standards & Interfaces*. 2007; 29(2): 254-259.
- [21] David, Mathieu, Neeli R Prasad. Providing strong security and high privacy in low-cost RFID networks. *Security and privacy in mobile information and communication systems*, 2009: 172-179.
- [22] Jiang, Yi, Wei Cheng, Xiaojiang Du. Group-based key array authentication protocol in radio frequency identification systems. *IET Information Security* 2014; 8(6): 290-296.
- [23] Lu, Li, et al. *Dynamic key-updating: Privacy-preserving authentication for RFID systems*. Pervasive Computing and Communications, 2007. PerCom'07. Fifth Annual IEEE International Conference on. IEEE. 2007: 13-22.
- [24] Kapoor, Gaurav, Selwyn Piramuthu. Single RFID tag ownership transfer protocols. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 2012; 42(2): 164-173.
- [25] Chen, Hsing-Bai, et al. *Enhancement of the RFID security method with ownership transfer*. Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication. ACM, 2009.
- [26] Juels, Ari, Stephen A Weis. Authenticating pervasive devices with human protocols. *Crypto*. 2005; 3621.
- [27] Lu, Li, et al. *Dynamic key-updating: Privacy-preserving authentication for RFID systems*. Pervasive Computing and Communications, 2007. PerCom'07. Fifth Annual IEEE International Conference on. IEEE. 2007: 13-22.
- [28] Kaps, Jens-Peter. Chai-Tea, Cryptographic Hardware Implementations of xTEA. *INDOCRYPT*. 2008.
- [29] Wheeler, D, R Needham. TEA extensions (October 1997), Also Correction to XTEA (October 1998). Available via: www.ftp.cl.cam.ac.uk/ftp/users/djw3.
- [30] Lamport, Leslie. Time, clocks, and the ordering of events in a distributed system. *Communications of the ACM*. 1978; 21(7): 558-565.
- [31] Gui, Yi-Qi, Jie Zhang, Hwang Kyu Choi. *An improved RFID security method with ownership transfer*. ICT Convergence (ICTC), 2011 International Conference on. IEEE. 2011: 594-596.