Security and Privacy in Intermodal Baggage Management With RFID

Ricardo Carapeto
Instituto Superior Técnico
Universidade Técnica de Lisboa
rcarapeto@gmail.com

ABSTRACT
In order to lower the costs associated with the loss and mishandling of luggage, airports and airlines began to consider the adoption of radio frequency identification (RFID) technology in their baggage handling systems. Under this problem, the Safe Luggage project was born with the purpose of enabling the location and tracking of luggage by embedding a passive RFID tag within its structure. This approach would be supported by a completely decentralized management and monitoring system, that would promote the cooperation and sharing of tracking information among all the involved baggage operators.

This thesis addresses the challenges of security and privacy raised by the Safe Luggage management model, with the purpose of constructing an appropriate security model for it. In that sense, this thesis starts out by analyzing the whole universe of RFID attacks, identifying the main threats to this system and producing a list of security requisites for it. Subsequently the proposed security model is presented and its evaluation done resorting to a functional prototype.

This evaluation highlights the capabilities of this security model to scale in a real world implementation of the Safe Luggage system. Moreover, it's stressed the difficulty of providing effective security and privacy with the usage of actual passive RFID tags.

Author Keywords
RFID, Safe Luggage, security, privacy, luggage

1. INTRODUCTION

Despite the improvements over the last two years (2008 and 2009), that managed to decrease by 24% globally the number of lost or mishandled bags, this is a problem that still costs the Air Transport Industry (ATI) around US$2.5 billion[1] every year – A sum that it cannot afford to lose in the current economic climate.
In order to address this issue, the Air Transport Association (IATA) developed a business case to examine the performance of the RFID technology applied in a baggage handling scenario. This study proved that the adoption of the RFID for the sorting and handling of baggage along the global supply chain provides advantages for the three main stockholders: airlines, airports and passengers. This result drove the IATA Baggage Working Group to adopt the Ultra High Frequency (UHF) RFID for the *recommended practice* 1740c [1].

1.1. SAFE LUGGAGE[2] PROJECT

Regarding the complexity of passengers and luggage transportation and the necessity to guarantee their safety along their journey, the Safe Luggage Project proposes a system that enables the tracking and location of luggage through an information system embedded within. In order to achieve this successfully, the system has to be tamper-proof and compliant with international standards, such as those imposed by IATA.
Besides tracking and location, this system provides bag identification by storing its owner personal data in its identifying device. Therefore, this approach enables a fast and adequate response in case of lost or stolen bags, provided an infrastructure compatible with the used identifying device exists.
This vision would be supported by a decentralized management and monitoring system, where all the involved operators could share tracking information with each other regarding the managed bags.
Even though this project considers the usage of several information technologies (RFID, WSN, GPS/Galileo, GSM/3G), each one enabling the tracking and location of bags at different precision and location levels, this thesis only focus on the security and privacy aspects of the RFID approach.

2. PROBLEMS AND OBJECTIVES

This thesis focus on addressing every single potential security and privacy issue that affects the users of the Safe Luggage system, in order to develop a security model that provides enough protection against these threats. Thus, this

[1] SITA Report obtained in http://www.sita.aero/content/baggage-report-2010

[2] Safe Luggage obtained in http://www.mala-segura.com/

thesis includes a detailed analysis of all the existing attacks on RFID, serving as a support for the identification of all threats to the Safe Luggage system that must be addressed in the solution. Once this is done, the security model is presented and its performance measured through the use of a functional prototype.

3. STATE OF THE ART

Due to the RFID industry's desire to trade-off hardware functionality to manufacture passive tags – RFID tags that have no internal power source – at low costs, security and privacy has received less attention. This means that these low-cost tags are vulnerable to a broad range of threats that can be easily exploited to compromise RFID-enabled systems.
The latest EPCglobal Class-1 Generation-2 UHF RFID standard [2], which defines the air interface protocols and the physical and logical requirements of these passive Tags, includes some security improvements over the past versions. However, these are still insufficient to provide meaningful security against several threats. Briefly, this standard provides the following mechanisms:

Kill Command: Tags can be permanently disabled. Killing tags at point-of-sale enables greater data security and personal privacy. This command is protected by a Tag specific 32-bit password, which protects it from malicious disablement. Even though this approach is highly efficient in securing the consumers privacy, it is only applicable in specific business models.

Cover-Coding: This method is used to obscure the information transmitted from the Interrogator (RFID reader) to the Tag. To cover-code data, an Interrogator requests a 16-bit random number from the Tag. The Interrogator then performs a bit-wise EXOR of the data with this number, and transmits the cover-coded (or cipher) string to the Tag. The Tag uncovers the data by performing a bit-wise EXOR of the received cipher with the original number. In case the transmitted data is longer than 16-bits, this process is repeated as necessary. Since the random numbers are 16-bit length, this method is vulnerable to brute force attacks because one attacker can simply generate the 65536 possible combinations and test them to uncover the data. Moreover, an attacker can listen to the communication between Tag and Interrogator, and capture both the random numbers and the cipher, allowing it to disclose the information.

32-bit ACCESS Password: Optionally, a 32-bit ACCESS password can be set in a Tag to provide control both in reading and writing data to it. This password is transmitted to the Tag by cover-coding it, leaving it susceptible to the already mentioned attacks.

These limitations raises two main privacy concerns for users: tracking and inventorying [3].
Since RFID Tags responds to any reader interrogation without informing their owners or bearers, the threat of clandestine scanning of Tags by malicious Interrogators becomes a serious issue. If we also consider the fact that most RFID Tags identify themselves before Interrogators by transmitting a unique identifier, the tracking issue becomes apparent.
In addition to their unique identifiers, certain tags – EPC tags in particular – carry additional information regarding the items they are attached to. Thus, a person carrying EPC tags is vulnerable to inventorying, since a reader can silently harvest the information stored in these tags.

3.1. RFID ATTACKS

RFID systems are vulnerable to a broad range of malicious attacks, ranging from the simple passive eavesdropping to more sophisticated ones such as cryptanalysis. As this technology evolves so does the threats that it is susceptible to. Thus, it is increasingly difficult to capture a global view of this problem.
In order to manage risks efficiently, it's important to define a threat model that identifies and characterizes the most common attacks to RFID systems. In that sense, Mitrokotsa, Rieback and Tanenbaum [4] have proposed a 4-layer model of RFID communication that they use to categorize the RFID attacks, adding one more category for the multilayer attacks

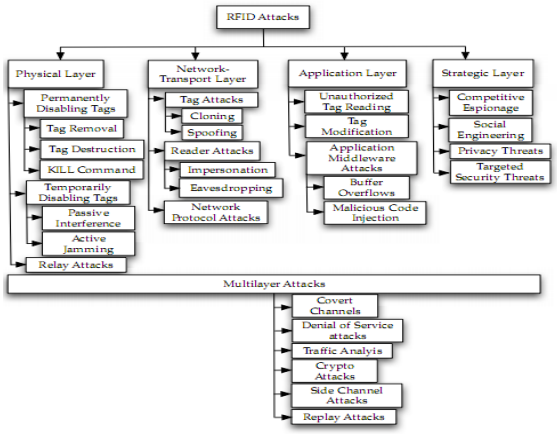

FIG 1 – CLASSIFICATION OF RFID ATTACKS

The physical layer comprises the physical interfaces and the RFID devices. Thus, an attacker in this layer can exploit the wireless nature of the RFID communications to employ attacks that interfere directly with its radiofrequency,

preventing an accurate and efficient communication between the RFID devices (tags and readers). Furthermore, since RFID tags are often attached to items leaving them exposed to direct handling, tag removal or destruction is simple to accomplish.
Even though the KILL command was initially introduced for privacy reasons, it is obvious that it can be exploited by attackers to compromise RFID communications.
In a replay attack an attacker acts as in the traditional man-in-the-middle, exploiting once again the wireless nature of the communication, placing a rogue device that intercepts and modifies the messages from each legitimate device (tag and reader), forwarding it to the original recipient. None of the legitimate devices are aware of this message relaying.

The network - transport layer includes all the attacks that exploit the way that RFID systems communicate and the way that data is transferred between tags and readers. This layer comprises attacks that target the tags, such as cloning and spoofing. These attacks are very similar, since both aims to replicate a legitimate RFID tag. They only differ on the medium used to emulate the original tag. In cloning, it's just created a replica of the original tag, while in spoofing a rogue device is used to emulate the tag behavior.
Because the communication between tags and readers if often unauthenticated, an attacker can easily impersonate a legitimate reader in order access sensitive information in RFID tags. However, regarding reader attacks, the most serious and widely deployed attack is eavesdropping. In eavesdropping, an attacker records the communications between legitimate RFID tags and readers, using it to perform other types of attacks later.
Since RFID systems often comprise the connection between RFID devices and back-end databases, an attacker can target the network protocols used or exploit flaws in the server operating system.

In the application layer, it's included all the attacks that target the information related to applications – called middleware attacks – and attacks that target the binding between users and RFID tags. Buffer overflows and malicious code injections are the main threats to middleware applications. RFID tags can be used as a medium to deploy these types of attacks, storing malicious code in its memory that is used to compromise back-end databases or middleware applications. On the other hand, the unauthorized reading and modification of tags directly affect the binding between RFID tags and its users.

The strategic layer includes attacks that target organizations and business applications, exploiting the poor design of infrastructures and applications. Social engineering and competitive espionage are just a few examples of these attacks. An attacker may use social skills (social engineering) to manipulate his victims in order for them to reveal sensitive information or even to grant him unauthorized access to restrict areas. An attacker can also exploit the ability to track and detect tagged items to gather confidential information in order to sabotage his competitors.

Finally, the multilayer attacks affect several of the previously mentioned layers. This category includes covert channels, denial of service and traffic analysis among others. Covert channel attacks exploit the unused memory of RFID tags in order to securely and covertly transfer data. Denial of service, on the other hand, aims to disrupt the normal functioning of RFID tags by intentionally blocking access to them. In traffic analysis attacks, an attacker analysis the intercepted messages between RFID devices and try to identify communication patterns. Even encrypted communication channels are vulnerable to this type of attack.

This brief analysis of the existing threats to RFID systems serves, in the context of this thesis, as a supporting platform to the identification of all the major threats that a system like the Safe Luggage is vulnerable to. The following section defines the attack model for this system, and the security requisites that should be guaranteed by the security model that's proposed in the solution.

3.2. ATTACK MODELS AND SECURITY REQUISITES

Under the assumption that luggage is constantly moving along its journey, with minor stoppages, we can assume that the location of its RFID tags are constantly changing as well. Moreover, the maximum communication distance between passive tags and RFID readers is limited to 10 meters. These aspects difficult the interaction between an attacker and his victim's RFID tags, restricting his ability to perform certain attacks over his targets.

Considering the fact that the RFID tags are embedded in the baggage structure, one can easily understand that attacks that aim to destroy or remove the tag are immediately prevented. This is one of the key aspects of the Safe Luggage system, since many of the lost or mishandled baggage are due to involuntary tag removal or destruction during the baggage handling process.

Another aspect that must be taken into account is the fact that the majority of the RFID readers are placed in specific locations, to maximize their reading range and to monitor meaningful events.

3.2.1. THREATS IDENTIFICATION

Analyzing the attacks presented in the section 3.1 in the light of what was described in the last section, one can immediately discard a number of threats to this system. Thus, from the attacks to the physical layer, we can ignore the attacks that aim to permanently disable the RFID tags

by removing, destroying or using the KILL command since the usage of this command is not considered in the Safe Luggage system. Furthermore, being the attacks to the strategic layer focused in organizations instead of individuals, these attacks are not considered in this security model. For the same reason, the attacks that aim to subvert the middleware layer are dismissed as well.

For the remaining attacks presented in the section 3.1, the following threats to this system are identified and its associated risk rated using a DREAD[3] model:

Threat Description	An attacker can interfere with the wireless communication channels of RFID devives
Threat target	RFID tags and readers
Risk	Medium
Attack techniques	Use of a *jammer*
Countermeasure	Use of opaque walls to the used wireless frequency

Table 1 – Wireless *Jamming*

Threat Description	Relay of intercepted messages between tags and RFID readers
Threat target	Baggage RFID tags
Risk	Small
Attack techniques	Eavesdropping of communication
Countermeasure	Adoption of authentication protocols between RFID devices

Table 3 – Message relay

Threat Description	An attacker can replicate tags and insert them into another bags
Threat target	Baggage RFID tags
Risk	High
Attack techniques	Reading of tag contents or eavesdropping of communication between RFID devices
Countermeasure	Adoption of effective tracking and monitoring of the tag journey

Table 4 – Cloning of RFID tags

[3] Threat Modeling obtained in http://msdn.microsoft.com/en-us/library/ff648644.aspx

Threat Description	An attacker personifies an authorized RFID reader to scan the tags content
Threat target	Baggage RFID tags
Risk	High
Attack techniques	Reading and writing of the tags content using an RFID reader
Countermeasure	Adoption of authentication protocols between RFID devices

Table 5 – Reading of RFID tags

Threat Description	An attacker personifies an authorized RFID reader to access and modify the tags content
Threat target	Baggage RFID tags
Risk	High
Attack techniques	Writing of the tags content using an RFID reader
Countermeasure	Adoption of authentication protocols between RFID devices

Table 6 – Modification of tags content

Threat Description	An attacker eavesdrops the communication between the RFID devices
Threat target	Baggage RFID tags
Risk	High
Attack techniques	Eavesdropping of communication using an RFID reader
Countermeasure	Adoption of encryption algorithms to protect the transmitted information

Table 7 – Eavesdropping of the communication between tags and readers

3.2.2. OBJECTIVES OF THE ATTACKER

Regarding the identified threats to this system, an attacker can use any of the mentioned attacks to accomplish specific objectives. We refer the following as the main objectives of an attacker towards its victim in a real world scenario of the Safe Luggage system:

- **Incriminate the baggage owner –** An attacker can clone the tag of his victim and insert it into another bag that he then uses to commit a crime.
- **Identify his victims –** Scanning the content of the

victims tag or simply eavesdropping the communication between the tag and the readers, an attacker can learn the name of his victim. In the possession of such information, the attacker can then execute other type of attacks more directed to that particular person.

- **Follow his victims –** Related to the last threat, an attacker can simply read the tag EPC identifier and use it to follow his victim. This attack is particularly dangerous because any RFID reader can read the EPC identifier from a tag without any kind of authentication between them.

3.3. SECURITY REQUISITES

From the previous assessments, it's clear that there are certain threats that pose a more serious risk to the security and privacy of the Safe Luggage system users. Thus, from the list of threats identified in the section 3.2.1 and considering the objectives of an attacker, we consider the tag cloning and the eavesdropping of communication, as the main threats to the security of the users of this system. This is due to the fact that all of the attacks derive in some way from each of these specific threats.

Regarding the cloning of RFID tags, it has already been mentioned that currently there aren't any effective methods to prevent this threat. RFID tags are available to everyone and they can be obtained at low costs virtually anywhere. Thus, an attacker that is able to scan an RFID tag and replicate its content in another tag can perform this kind of attack. As we can see, the cloning attack can only be executed resorting to the eavesdropping attack or directly accessing tags content. However, if the tag implements an ACCESS password to authenticate any reader that wishes to access to its content, the attacker can only learn this password eavesdropping the communication between these devices.

Regarding the communication jamming threat, even though this kind of attack can easily be performed, we consider that it is of little interest for the attacker, since it doesn't pose a meaningful threat to the security of the users of this system. The same applies to the relay attacks.

We can then conclude that to effectively protect the security and privacy of the users of this system, we must guarantee the following requisites:

- The private data should be protected against unauthorized eavesdropping when transmitted over-the-air.
- Only the authorized entities should be able to read and write the private data contained in the tags.

To achieve these requisites an encryption algorithm should be employed to protect the private data, and the ACCESS password should be used to authenticate the RFID readers. However, as it has already been mentioned, this password provides little security and is only considered in this security model because is the only authentication method available in the EPCglobal Class-1 Generation-2 specification.

3.4. ARCHITECTURE OF THE SECURITY MODEL

One of the main aspects of the decentralized baggage management model envisioned by the Safe Luggage system refers to the ability of the involved parties to communicate and share tracking information of the managed bags. This will be accomplished, in the Safe Luggage system, by a P2P network that will connect all the operators involved in the management of the baggage.

Since every operator will produce and consume information from other operators regarding the managed bags, it makes sense to adopt a federation model for the management of the decentralized network.

To assure the security and correct functioning of the federation the following requisites should be met:

- The entrance of new operators in the federation should be controlled;
- Mechanisms that enable the operators to authenticate between one another should be implemented;
- The access to the private data encryption keys and the ACCESS passwords should be controlled;
- Only operators that belong to the federation and are authorized to access the private data, should be able to access it.

3.4.1. ARCHITECTURE

In order to meet the requisites previously described, we propose the following architecture principles that will serve as the base support for development of the security model in the section relative to the solution:

I. The federation should have a regulatory entity that can determine the authenticity of the operators that wish to join the federation. This entity should be able to issue digital certificates that the members of the federation use to authentication among themselves.

II. Each operator will possess a digital certificate and the associated pair of public and private keys. This certificate is transmitted to each and every other member of the federation when the operator joins

the network. The public keys contained in the certificates will be used to generate access tokens to the private data contained in the baggage tags. This approach allows the development of authentication mechanisms in this security model.

III. The personal data (private data) are encrypted with a symmetric algorithm before being written in the baggage tag. This key is generated by the operator responsible to write the data in the tag.

IV. The generated access tokens are stored in the P2P network by a distributed hash table (DHT) algorithm.

V. If an operator wishes to identify the owner of a bag, it will have to obtain his token specific for that bag from the P2P network. Once he receives this token he'll be able to decipher it using his private key and access the information necessary to read and decipher the private data.

4. SOLUTION DESCRIPTION

Having presented the architectural principles that support the development of the security model that will be proposed for the Safe Luggage system, we will now select which algorithm of DHT will be adopted for the implementation of the P2P network. Then, it'll be chosen which of the currently available encryption algorithms will be used in this security model. Finally, it will be presented each of the protocols that comprise the security model, which are the protocol that manages the entrance of new operators in the federation, the protocol used be the operators to produce the access tokens, and the protocol that is used to search for these tokens in the P2P network.

4.1. SELECTION OF THE DHT PROTOCOL

In order to elect the DHT protocol that will support the implementation of the P2P network, we'll compare the following protocols:

- Chord [5];
- Pastry [6];
- Kademlia [7];
- CAN [8];

These protocols were chosen based on their popularity and extensive study.

To compare these protocols and determine which one is more suitable for this system, we'll establish a number of requisites and we'll analyze how well each protocol meets them. Thus, we propose the following requisites:

- Lookup efficiency;
- Ability to scale;
- Performance when peers enter or exit the network;
- Simplicity of the protocol;

The following table presents the lookup performance values of each protocol.

	Chord	Pastry	Kademlia	CAN
Lookup	$O(\log N)$	$O(\log N)$	$O(\log N)$	$O(\mathrm{d}N^{1/N})$

Table 1 – Lookup performance values of the DHT protocols.

From this table it's clear that for the exception of the protocol CAN, all the others present the same lookup performance. Even though this protocol has worse performance than the others, he manages to compensate this fact with its ability to maintain fewer node estates per node. This means that each node of this protocol knows fewer neighbors (other nodes) of the network. This is especially relevant if we consider that these networks tend to scale to hundreds or even thousands of peers. So, regarding the first and the second requisites we consider a tie between all the protocols.

Regarding the third requisite, each protocol treats differently with the join or exit (or fail) of nodes from its network. The protocol Chord is known for dealing especially well under these circumstances as certain **[Jin]** studies show.

Finally, regarding the last requisite, Chord stays again at the top, being the simplest of the protocols considered in this analysis. Cause of these last two aspects, we'll chose Chord as the DHT protocol to support the P2P network.

4.2. SELECTION OF THE ENCRYPTION ALGORITHMS

The process of determining which encryption algorithms are best suited for this security model is a simple one, since cryptography is an extremely studied area. Thus, there are some recommendations and best practices published by respected authorities in this area.

For this work, we have chosen to follow the recommendations made by the National Institute of Standards and Technology – NIST. This agency is responsible to evaluate and produce recommendations regarding the usage of encryption algorithms to protect data for U.S. federal agencies.

Based on these recommendations [9], we've chosen to use RSA as the public key algorithm with a key size of 1024 bits. For the symmetric key, we've adopted the Rijndael algorithm with key size of 256 bits. This protocol with this key size provides the best protection that one can currently obtain with encryption algorithms.

4.3. COMPONENTS OF THE ARCHITECTURE

Some of the components that make part of the architecture of the security model have already been mentioned in the section 3.4.1. However we'll assess each of these components and others that have not already been mentioned in this section. The components are the following:

P2P node – Each of the operators of the federation will control a peer or a group of peers that will communicate with other operator's peers and will allow them to share the necessary information in the network.

Central Authority of Registry (CAR) – As has been already mentioned, this federation will need an authority to control the entrance of operators in the federation and to issue the digital certificates to them. This entity will have responsibilities similar to those of a certification authority.

Personal Information – As was already made clear, this information will correspond to some of the bag's owner personal data that will be stored in the tag embedded within the bag's structure. This information is accessed by the operator to identify the bag when necessary.

ACCESS password – This password was already analyzed and it is used to authenticate the readers controlled by the operators.

Symmetric Key – This corresponds to a Rijndael key with 256 bits of length. It is used to encrypt the personal data.

RSA Key Pair – Each operator generates a RSA key pair with 1024 bits and uses it to encrypt and decrypt access tokens.

Digital Certificate – Each operator will have a digital certificate issued by the CAR. These certificates are used to authenticate operators that want to join in the federation.

EPC identifier – Each tag will have an unique EPC identifier that univocally identifies the tag in the universe of EPC tags. This identifier has 96 bits length.

5. PROTOCOLS OF THE SECURITY MODEL

Understood each of the components that comprise the architecture of the security model, it's now time to describe each of the protocols that govern the entrance of new operators in the federation and the protocols that allow the distribution and search of the generated tokens.

5.1. ENTRANCE OF NEW OPERATORS IN THE FEDERATION

The new operator obtains the CAR certificate from an external certification authority (ex. Verisign). This certificate contains the public key of the CAR.

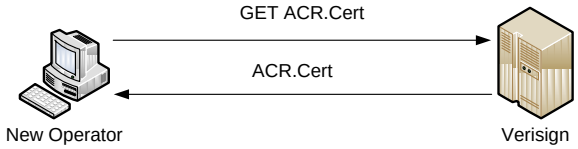

Fig. 2 – New operator obtains the CAR certificate from an external authority.

The operator uses the certificate to send a certificate signing request to the CAR. This comprises information regarding the operators activity (credentials) and his public key from the RSA key pair. The CAR receives this information and certificates the new operator, responding with a signed certificate a MembersList, containing the certificates of every other operators of the federation, and the IP and port necessary for the new operator communicate with one of the nodes of the network.

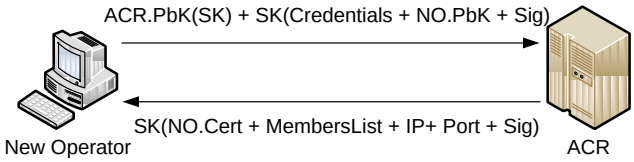

Fig. 3 – Registration of the new operator.

The new operator uses the IP and port and connects to one of the peers of the network. He sends the certificate to the federation peer that promptly determines its validity by checking the CAR signature in it. However, this is not sufficient to admit the new operator in the network. First the new operator must prove that it possesses the corresponding private key of the public key contained in the certificate.

This authentication protocol simply comprises a nonce that is produced and sent to the new operator encrypted with the public key of his certificate. On his turn, the operator receives the encrypted nonce, decrypts it and sends it to the federation peer. If the nonce corresponds to the original one, then the new operator is authorized to join the network.

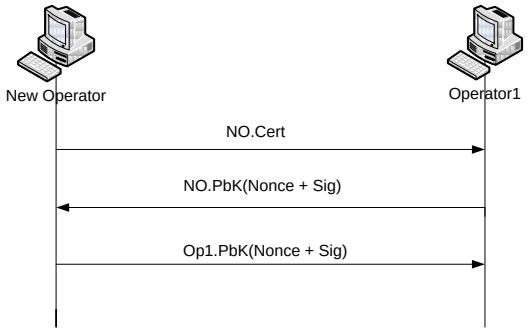

Fig.3 – Authentication of the new operator.

After this process of authentication, the peer transmits the certificate of the new operator to his successor, initiating a sequence of successive transmissions of the certificate, until it returns to its owner (new operator). This process is needed to inform the other members of the federation that a new operator has arrived. The field subject of the certificate corresponds to the unique identifier of the operator in the P2P network.

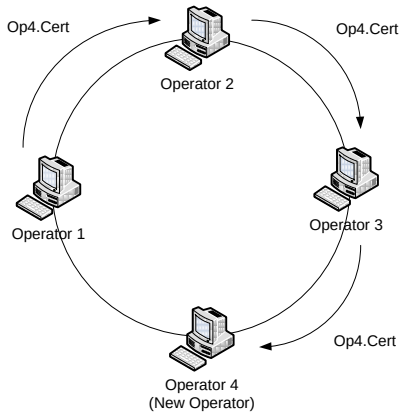

Fig. 4 – Transmission of the certificate in the Chord ring (P2P network).

One of the aspects that have not been mentioned already refers to the fact that the nodes of the P2P network supported by the protocol Chord, are organized in a ring, where each node knows two immediate neighbours: the successor and the predecessor.

In the end of this process, every operator has learned about the new operator.

5.2. PRODUTION AND DISTRIBUTION OF TOKENS IN THE P2P NETWORK

At the moment of writing the private data into the RFID tag that accompanies the bag, the operator has to determine which of the remaining operators of the federation will have access to this data. Since this federation gathers only interested parties in the management of baggage, we can assume that it'll be granted access authorization to every member of this federation. However, with this model of authorization based in tokens, it is possible to institute access levels within this federation by restricting the access of certain operators to the private data.

We'll assume in this protocol, that the tags are empty at the moment of check-in.

This protocol starts at the check-in counter in the airport, with the passenger providing his identification to the operator (clerk).

The clerk receives this data and encrypts it with a Rijndael 256-bits key (ki). The resulting cipher is then written in the RFID tag of the bag

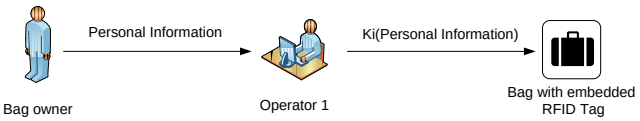

Fig. 5 – Writing of the private data in the tag.

Afterwards, the operator produces N ciphers with the public key (Pbk) of each one of the other operator, with the following format: `Pbk(Ki+ACCESS)` . These ciphers can only be decrypted by the corresponding private keys of the RSA key pair, thus only the owner of the public key will be able to do it.

Each token is associated with an index key that is used by the protocol Chord to assign it to a node in the P2P network. This aspect allows load balancing in the distribution of tokens over the network since every node will be responsible to manage roughly the same number of tokens. This index key is obtained by hashing (with MD5 for instance) the EPC identifier of the tag with the ID of the operator for whom the token is was produced for – `MD5(EPC+ID)` .

5.3. ACCESS TO THE PRIVATE DATA

After the production and distribution of the generated tokens over the P2P network, each operator is now able to lookup for these tokens, whenever they need to identify a baggage.

To access the private data, an operator must first read the tag EPC identifier, and generate the hash: `MD5(EPC+ID)`, where ID corresponds to his unique identification (Subject of his certificate).

After producing the index key of the token in the P2P network, he communicates with the peer responsible to store the token and retrieves it.

After receiving it, the operator deciphers it using his private

key and retrieves the symmetric Key (Ki) and the ACCESS password.

Finally, the operator accesses the tag using the ACCESS password, reads the encrypted data and deciphers it using Ki, accessing the private data and identifying the baggage.

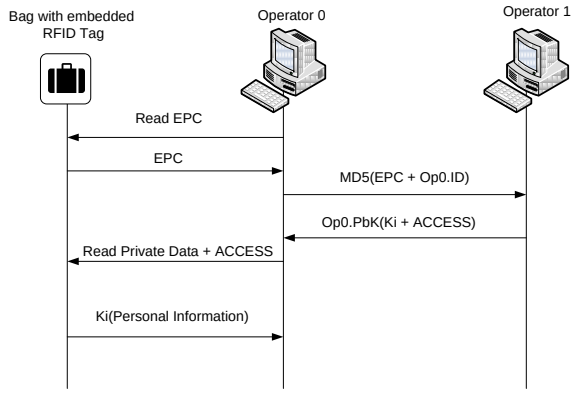

Fig. 6 – Identification of a baggage

It is possible, however, that a baggage gets lost while being handled by an operator that doesn't belong to the federation. In this case, there are two alternatives:

- If the operator doesn't control any RFID reader, he'll be unable to access any content of the tag, so, in this situation he would have to forward the baggage to an operator that belong to the federation and in this case the last protocol would be applied.
- If the operator controls an RFID reader and has internet connection with any of the operators of the federation, he can work as an intermediary between the bag and the authorized operator without any private data being disclosed.

The following picture illustrates this simple protocol:

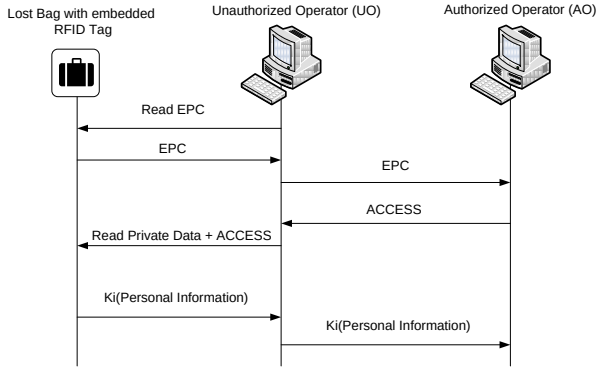

Fig. 7 – Identification of a baggage using an intermediary

This approach raises a problem, regarding the disclosure of the ACCESS password to the unauthorized operator. An evil-minded operator could use this information to access and modify the contents of the tag. Therefore, it is extremely important that the authorized operator has full trust in this unauthorized operator, otherwise problems might arise.

6. EXPERIMENTAL EVALUATION

Since this security model has to respond to the needs of a real world implementation of the Safe Luggage system, it is essential to determine if this solution is indeed scalable and has sufficient performance to cope with the estimated load.

Therefore, to understand the capabilities of this security model, we implemented and tested a functional prototype that simulates de protocols of production and distribution of tokens and the protocol of search for these.

Before testing the performance of this prototype in a stress load scenario, we had to contextualize these tests in a real world scenario. Thus, the first step was to determine the expected load in these kinds of scenarios.

Through analyzes of the annual report of ANA [10] – Aeroportos de Portugal, concerning the statistics for air transportation of 2009, and using the annual report for Transportantion Estatistics in Portugal during 2008 (last available report), produced by INE [11] – Instituto Nacional de Estatística, we came up with the rough estimate of 348 passengers handled per minute in the airports and trains stations of Portugal. We then decided to use this number as an indicator for the performance of this prototype.

For the simulations of this prototype it was considered the use of a maximum of 10 instances to simulate concurrent addition of data in the network, and to analyze the evolution of the performance of the system. Each simulation session comprises two distinct phases. In the first, each peer processes a workload, producing access tokens. In the second phase every peer searches for the tokens that were generated for him.

The results obtained with this evaluation are presented in the next graphs:

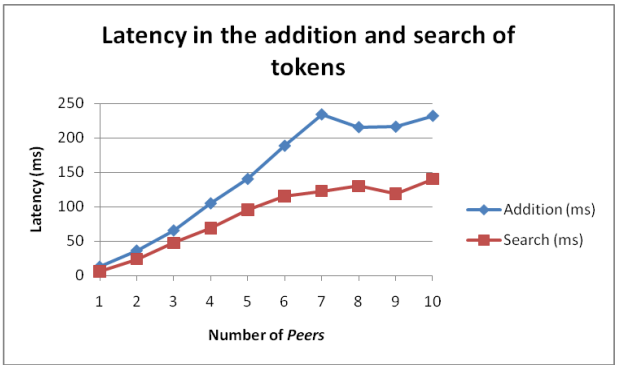

Fig. 8 – Latency in the operations of addition and search of

tokens

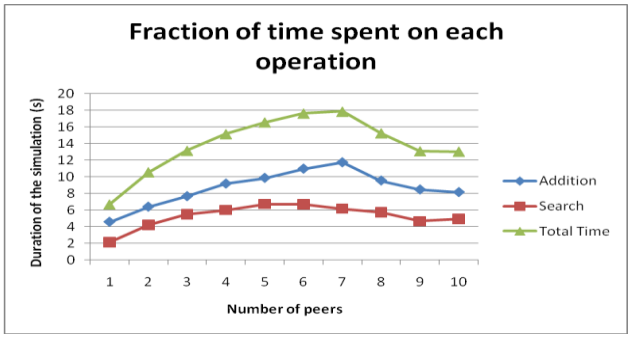

Fig. 9 – Relationship between the time spent on the addition and search of tokens.

Even though the sample of 10 instances used in these tests is small to conclude with higher certainty the behavior of this system, it's important to note that the performance of the searches degrades very slowly comparatively with the addition, because this is the critical operation of the system. The addition of a token to a baggage only occurs once, while the additions will certainty occur much more frequently. The latency with 10 peers allows the system to search in a period of a minute, roughly 4.261 tokens or add 2.574 tokens to the P2P network which largely surpasses the expected 348 queries.

Moreover, we can verify that the performance of the system degrades more than it gains for each peer that enters the network, inverting this situation only when more than 7 peers are connected.

These results are positive, but more testing with larger networks would be necessary to draw better conclusions.

7. FUTURE WORK

Like was just mentioned, it would be interesting to evaluate this system on a larger scale. The replication of data in the network would be interesting to analyze, since it is important to guarantee total availability of the data in situations of peer failures. The management of certificates is discarded as well from this work, being one of the many other points of interest to develop in future works in the context of the presented solution.

8. CONCLUSIONS

During the analysis to the questions of security and privacy that arises in a system with the characteristics of the Safe Luggage, it was clear that the actual limitations of the standard EPCglobal Class-1 Generation-2 prevents the deployment of systems with high security requisites. For these scenarios usage of active tags with cryptographic capabilities are essential. However, the developed security model proves that even with actual limitations, it is possible to provide meaningful security in such scenarios without compromising the performance of the system. One of the key aspects of this model is the possibility of integration with other scenarios of RFID based systems.

9. REFERENCES

[1] IATA. Radio Frequency Identification (RFID) Specifications for Interline Baggage. *Passenger Services Conference Resolutions Manual Part I & Part II.* Montreal-Geneva : IATA, 2008.

[2] EPCglobal Inc. EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.2.0. 11 de Junho de 2008.

[3] Juels, Ari. RFID Security and Privacy: A Research Survey. 28 de Setembro de 2005.

[4] Mitrokotsa, Aikaterini, Rieback, Melanie R. e Tanenbaum, Andrew S. Classification of RFID Attacks. Maio de 2008.

[5] Stoica, Ion, et al. Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications. *Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications.* San Diego, California, United States : ACM, 2001. pp. 149 – 160.

[6] Rowstron, Antony and Druschel, Peter. Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems. *Proceedings of the IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg.* Springer-Verlag, Novembro de 2001. pp. 329 - 350.

[7] Maymounkov, Petar e Mazières, David. Kademlia: A Peer-to-peer Information System Based on the XOR Metric. *Revised Papers from the First International Workshop on Peer-to-Peer Systems.* Springer-Verlag, 2002. pp. 53 - 65.

[8] Ratnasamy, Sylvia, et al. A Scalable Content-Addressable Network. *Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications.* ACM, 2001. pp. 161 - 172.

[9] NIST. NIST Special Publication 800-57. *Recommendation for Key Management – Part 1: General (Revised).* Março de 2007.

[10] ANA - Aeroportos de Portugal. *Relatório Anual de Estatística de Tráfego.* 2009.

[11] Instituto Nacional de Estatística. Estatísticas dos Transportes 2008. Lisboa : INE, 2008.