Journal of Network and Computer Applications ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Improved security for commercial container transports using an innovative active RFID system

Francesco Rizzo *, Marcello Barboni, Lorenzo Faggion, Graziano Azzalin, Marco Sironi

Joint Research Centre of the European Commission, Institute for the Protection and Security of the Citizen, Via E. Fermi 2749, 21020 Ispra (Va), Italy

ARTICLE INFO

Keywords:
RFID technology
Wireless communications
Secure transport
Secure supply chain
Electronic seals

ABSTRACT

The huge number of containers daily involved in the global transportation system opens important logistic and security issues. The matter of improving the management of goods in the harbor and the serious vulnerability problem of containers are relevant topics in the commercial supply chain. In fact, both can be easily exploited as carriers for illegal and dangerous items.

In this paper, we focus on the security of commercial containers starting with the analysis of the most common technologies presently used in the field.

Then, we concentrate on the research carried out by the Joint Research Centre (JRC) of the European Commission in the field of supply chain security. In particular, we discuss in-depth our innovative active RFID-based sealing systems designed at the JRC, giving a detailed technological description of its working logic and main features. Experimental results of the laboratory tests are presented, in order to show the performance of the system and its capabilities in improving security in commercial transportation systems.

1. Introduction

Security-wise, one of the most critical elements in the transport supply chain is represented by the flow of commercial containers. The design concept of commercial containers has not changed over the last forty years. Commercial containers are, still today, built without having security as a primary goal. Unfortunately, the social conditions have changed very much since the original design of commercial containers and today security is a primary concern. A huge number of such containers, which are used daily in the global supply chain, are extremely vulnerable. Containers are subject daily to potential physical attacks to their integrity.

Technology providers and stakeholders in the world of global shipping propose two main solutions for securing commercial containers. The first one relies on the use of on-board smart systems that control the internal volume of the container by using different device sensors. These systems are able to send an alarm message to remote servers if a non-authorized door opening has been detected (Satish Bukkapatnam et al., 2007; Craddock and Stansfield, 2005; Whiffen and Naylor, 2005). The second solution focuses on maintaining the physical integrity of the closed container doors by means of mechanical seals. Every attempt to trespass on the container should leave behind evidence on the seal. However, the possibility to physically tamper with the seal during the long journey periods in which containers are not controlled, makes this solution highly vulnerable and ineffective. Moreover, even when the tampering attempt is detected, a mechanical seal cannot provide information regarding the time and the place in which the infraction took place.

In order to overcome these problems, a new class of electronic seals based on radio frequency identification device (RFID) technology has been developed (see for example Park et al., 2006; Yoong et al.,). The basic idea is to add new security features with respect to standard. The capabilities of RFID systems: contact-less reading, information storage and remote control.

The European Commission has considered the raising need for safety in supply chains and has started the analysis of the problem through its scientific and technologic reference center, the Joint Research Centre (JRC). The JRC has focused its research work on the development of container sealing systems based on the use of passive and active RFID technologies. The main objectives are to satisfy the increasing need for high security and, at the same time, to be extremely competitive from an economical point of view. In fact, raising the security level and the automation of check operations brings a general improvement in the logistic issues of the supply chain.

In the next sections an innovative electronic sealing system, completely developed at the JRC, will be discussed. The system is based on standard RFID technology. However, while current the electronic sealing systems are based on the use of only one RFID technology (passive or active RFID), our solution exploits the

* Corresponding author. Tel.: +39 3281066199.
E-mail addresses: francesco.rizzo@jrc.ec.europa.eu, fra.rizzo@gmail.com (F. Rizzo), marcello.barboni@jrc.ec.europa.eu (M. Barboni), lorenzo.faggion@jrc.ec.europa.eu (L. Faggion), graziano.azzalin@jrc.ec.europa.eu (G. Azzalin), marco.sironi@jrc.ec.europa.eu (M. Sironi).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.04.006

combined capabilities of both technologies. This choice has been done in order to design a new sealing system able to guarantee a greater security level at relatively low production costs.

2. Sealing systems

A seal, by definition, is a device that can be applied to an object and that must be broken before access to the object can be obtained. The purpose of sealing an object is to guarantee the identity and integrity of the object since the application of the seal. It can be fulfilled checking the authenticity of the seal.

To fulfill the definition of seal:

- Integrity, because it cannot be opened, even temporarily, without leaving behind unconcealable evidence.
- Authenticity, because it is identifiable, and its identity cannot be altered without leaving behind unconcealable evidence.

Sealing is a practice that dates back thousands of years, long before the use of writing became common and widespread. Ancient seals were generally impressions on wax or clay (intaglios) obtained through the use of small bone or stone cylinders carved with geometric designs. Seals were used to secure the fastenings on jars, boxes and bags. If the seal was broken, it suggested that the item had been opened. Evidence of the use of seals in Mesopotamia, ancient Egypt, Japan and China dates as far back as 3200BC (Encarta Encyclopedia,).

As we can see, the definition of a seal has not changed much with time. In the field of container security, a seal is a device that is applied to one or both of the container doors and that has to be broken in order to gain access to the inside of the container. A seal also carries evidence of its own identity, to ensure that the seal itself has not been replaced.

One very common error found in technical literature is the mix-up of the definitions of a seal and a lock. While the function of the latter is to deter the opening of the object to which it is applied through its mechanical strength and robustness, the former is a device that indicates whether the object has been opened or not. The only physical strength that a seal is required to have is one such that it does not break during normal use.

There exists a wide variety of devices that offer both the seal and lock functionalities, all or in part. For the purposes of this document these hybrid devices will be treated as seals.

Seals are designed to be tamper-evident. Normally, to determine if a seal has been tampered with, a visual inspection is required, as the tampering attempt will have altered in an evident way the physical aspect of the seal. With the use of modern technologies, though, a new family of seals has surfaced. These are seals that carry on board some class of electronics, that extends possibilities of seal inspection beyond the normal on-field visual inspection. These seals are normally referred to as eSeals or Smart seals.

In literature today there are many different classifications of seals, based on the type of technology they employ, on physical characteristics, or on the supposed level of security they offer. In this article we offer the following classification:

- *Mechanical seal*: A device that carries out the basic function of a seal as described at the beginning of Section 2, based solely uniquely on its physical characteristics. These seals can be made of different materials, ranging from plastic, to thin aluminum foil, to steel in varying degrees of thickness. All these seals share the same sealing principle, e.g. the fact that they cannot be opened and closed back again without leaving evidence behind. This evidence is detected at inspection time, through manual inspection. The identity of these seals is established through the use of a unique identity number embossed on the body of the seal itself. Alteration of this number should not be possible without leaving evidence behind. If a seal is made of two detachable parts, the identity number should be embossed on both parts, to avoid malicious mixing of parts from different seals.
- *Smart seals*: The definition of this family of seals is very generic, they include any seal that has a form of intelligence built in that extends the functionality of mechanical seals. They are usually able to give more information regarding their status, and allow a number of additional ways of carrying out inspection. For example, a steel seal could be molded with a technique that introduces random imperfections in its internal structure that renders each seal unique, thus giving each seal a unique "signature" (Sironi et al., 2007). This signature can then be verified through the use of ultrasonic inspection. These seals are usually designed to alter their signature in a way known to the authorized inspector when removed. This way they fulfill the definition of seal in that they carry evidence of tampering attempts and a unique identity. Other smart seals include devices that use different technologies to assess their status. These technologies include, but are not limited to, pressure sensors, thermocouples, Speckle signatures (d'Agraives et al., 2001), holograms, radio frequency identification (RFID).
  A particular attention should be paid to *eSeals*. This is a particular category of Smart seal that deserves a special definition due to their unique characteristics and potentialities. For the purposes of this article and the definition of seal given here, eSeals are seals based on active, passive or mixed RFID technology. The presence of one or more RFID device embedded in the seal can be exploited for different purposes. For example, the internal memory of the RFID chips can be used to save a log of events, and it is possible to assess the correct closure of the seal to avoid malicious "fake installations". An eSeal, in fact, features the possibility to certify that it has been closed correctly and can save in the internal memory the time of closure and identity of the operator who performed the installation. Furthermore, with RFID technology a new way of inspecting the seal becomes possible: in fact, in many applications it is the seal itself that performs a self-diagnosis and communicates its state to the inspector. This way the possibility of human error is greatly reduced, and the quality of inspections depend less on the inspector's skills and experience than before. When RFID technology is employed, the seals can be inspected at a distance and on-the-fly (i.e. without physically stopping the cargo). Active seals depend on the presence of an on-board battery for their operation, and this limits the maximum length of a single journey.

Modern technologies offer the possibility to design reusable seals. A reusable seal is a device that retains the identity and evidence-indicating characteristics of a normal seal, but is designed in a way that allows it to be used more than once. The great advantage of reusing a seal more than once is the improved cost to benefit ratio, although there are several disadvantages that should be kept in mind when evaluating the use of a reusable seal:

- Reusable seals have to be returned to the owner after a journey, and this involves a cost. Sometimes the cost of returning the seal for reuse exceeds the cost of the seal itself.
- They rely on an external database for validation. A supporting information technology infrastructure is needed to track the status of every seal at all times. The complexity of this infrastructure is increased greatly by the geographically distributed nature of container shipping.

Please cite this article as: Rizzo F, et al. Improved security for commercial container transports using an innovative active RFID system. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.04.006

- A common standard will be necessary for a large scale adoption of reusable seals to ensure reader and database compatibility between operators. This infrastructure is dedicated, hence the costs of maintaining and upgrading it will be entirely on the users. This is not the case, for example, when a system relies on an existing infrastructure (such as GSM) for data transfer. In this case maintenance and upgrade costs will be on the owner of the infrastructure, and technological improvements will be driven by market demand. The system will automatically inherit any improvement made to the infrastructure.

3. Electronic active seal

The electronic active seal developed at the JRC is an integrated sealing system designed and realized with the aim of increasing supply chain security. In particular, this seal has been studied to minimize the tampering possibility of a standard container, by sealing both its doors at the same time, as shown in Fig. 1.

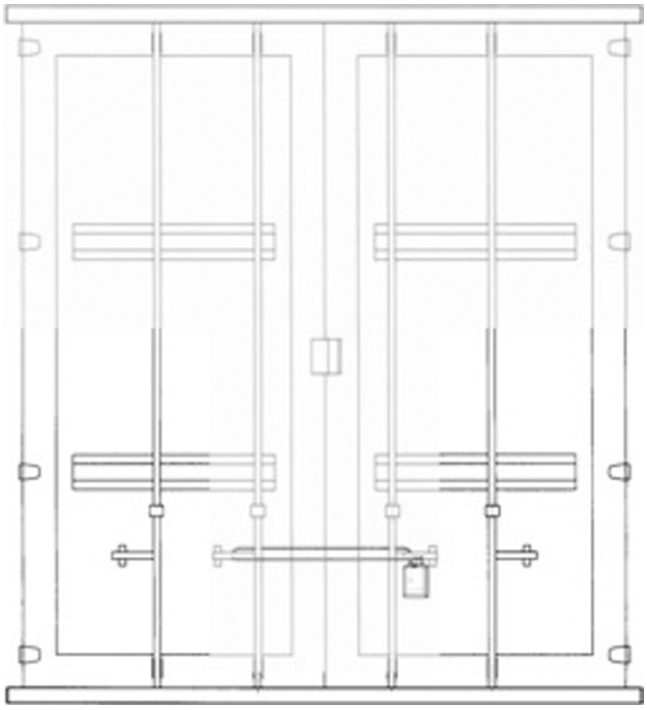

Fig. 1. Schema of a standard container with closed and sealed doors. The electronic seal guarantees the container locking by wrapping both the two bars of the doors.

Fig. 2 shows the external appearance of the electronic seal and its internal structure. The seal is composed by a main plastic body linked to an external cable by two connections. One end of the cable is fixed to the body and cannot be taken out, otherwise the seal would break and the unauthorized opening detected. The other cable end can be inserted in the main body, secured by a ring nut and can be opened.

The electronic components of the system are embedded into both the main body and the external cable. The active RFID circuit is placed in the seal body, together with a passive low frequency (LF) transponder reader, working at the frequency of 125 kHz. A passive RFID chip is installed in the removable end of the external cable. The passive transponder is used to guarantee the proper closure of the seal: when the end of the external cable is inserted and the seal is closed, the passive system reads the unique identifier (UID) of the passive tag and transmits it to the active transponder. Every active circuit is linked to the UID of a specific passive transponder. Such pairing mechanism is set during the seal production process and ensures that the seal is correctly closed with the right cable (the pairing is signaled through a buzzer at seal closure). Once the seal is closed every attempt of opening it will be detected from the passive RFID system components and signaled to the active circuit logic. The external cable represents another critical component of the system: possible attacks to the system could be done cutting the shielded cable and re-closing it after the container opening. The solution adopted to avoid this problem is the use of a conductive wire inside the external cable. This wire gives an electrical connection to the electronic circuit placed in the main body, which is continuously monitored by the electronics. Any attempt of cutting the cable would result in a loss of electrical continuity for the electronic seal, and thus an alarm would be triggered.

Every tampering attempt will result in a change of the seal state and will be automatically recorded in a memory section of the electronic card. In general, the seal memory will contain information on any possible operation (authorized opening, unauthorized opening or cable cutting) done on the seal during its working time and after its correct closure (i.e. after that the correct pairing between the passive tag and the active seal electronics has been performed). When the seal memory becomes full it is necessary to reset it by using the portable reading system, as explained in the next subsection.

3.1. Interrogation system: activator and receiver

The active seal is essentially based on an active RFID transponder equipped with an internal power source. The power source is used to activate the integrated circuits and to broadcast the response signal

Fig. 2. Left picture: a closed electronic seal with main body, external cable and closure ring nut highlighted. Right picture: internal structure of the electronic seal.

Please cite this article as: Rizzo F, et al. Improved security for commercial container transports using an innovative active RFID system. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.04.006

to the reader. The transponder is in a sleeping communication state until the reception of an appropriate signal sent by an activation unit (data uplink). This unit emits an electromagnetic signal, at microwave frequency (2.45 GHz). Once the active transponder has been awoken, it inquires its memory and sends an appropriate electromagnetic reply at a frequency of 433.92 MHz. A receiving unit collects the transponder reply (its 32-bit ID code, followed by other data—downlink). In RFID applications and, in general, in systems based on wireless communication protocols, a relevant topic is the security related to the data transmission. The active RFID seal can be easily exposed to security attacks such as eavesdropping of the radio communications between the transponder and the reader and cloning attempts (Sklavos and Zhang, 2007). In order to overcome these security risks it is necessary to consider cryptological procedures, in which transmitted data can be encrypted prior to the transmission disallowing a potential external attack. The power consumption of the active seal depends on the operational state. In the transmission mode, the maximum value of the power consumption is $P_{Max} = 75$ mW. However, this value reduces to $P_{Max} = 12$ mW in the receiving state and to $P_{Max} = 4.5\mu$W in the sleeping mode. Therefore, we have evaluated that using as internal power source a standard lithium battery, the average lifetime of the active transponder in standard environmental conditions is greater than one year. The transmission logic is shown in Fig. 3.

There are two different reading systems for our active seal: a fixed reader composed by two different parts (activator and receiver) and a portable reader, which has the activation and receiving units integrated into one. In Fig. 4 are shown both the reading system solutions.

The portable system is a handheld RFID reader in which the activator and reader units are integrated. This device has the possibility to scan and operate on different seals at the same time. Moreover, the fixed readers have a larger operating range than the handheld reader, due to differences in antenna size. For this reason, in order to avoid possible ambiguities when more than one seal falls within the operating range of the fixed reader, only the portable reading system can reset the memory or authorize the seal opening. In addition, after the initial scan of the transponders in the reading region, the handheld device has the possibility of selecting a specific seal and of operating only on its memory. The portable reading system can authorize the opening for a container check. Once the system has sent the authorization signal, the operator has a fixed time window of 40 s in which the seal can be opened without triggering an alarm. This time window is set during the hardware production and cannot be changed. After this time interval, any seal opening will be considered as an illegal tampering operation and recorded in the memory.

An activator and a receiver compose the fixed reading system. Both the components are powered by a 12 V (2A) DC current. In order to visualize the transponder data, the receiving unit has an Ethernet module that permits the connection with a processing unit. Once the network connection has been established, the application program will allow the visualization of the data. The application program automatically connects to the receiver and shows on the screen the memory content of the seals that are in the reading field. In particular, as shown in Fig. 5, the program has two main windows. In the window at the top the seal status is shown. The window at the bottom displays all the details: the seal number, the number of operation read, the number of operations stored in the memory and the operations made on the seal.

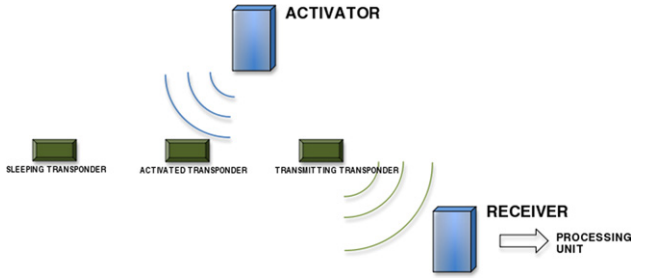

Fig. 3. Schema of the system operation logic. In particular, only transponders that go through the activation field (blue lines) transmit their information status through a 433 MHz electromagnetic radiation (green lines) to the receiver. Finally, the information is sent to a processing unit. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

4. Reading performance: experimental results

In this section we show the main experimental results of the reading capabilities tests carried out on the active RFID sealing

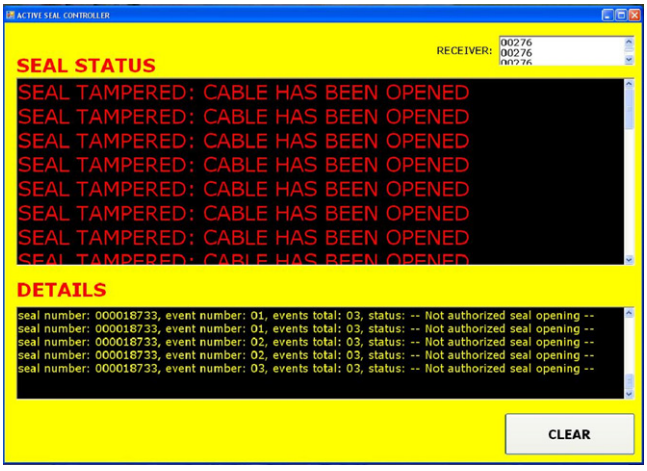

Fig. 5. Screenshot of the application program that manages and shows the operations the status of the electronic seal.

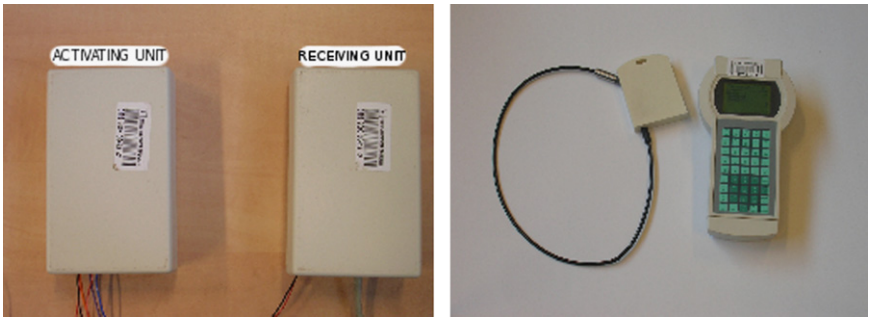

Fig. 4. Left picture: fixed reader solution with separated activator and receiver. Right picture: handheld reader with a closed electronic seal.

Please cite this article as: Rizzo F, et al. Improved security for commercial container transports using an innovative active RFID system. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.04.006

system. We have conducted a series of static readings in different conditions by considering different activation power levels and various reader-seal geometrical configurations.

The aim of static reading tests were to determine the performance of the system by considering fixed positions between the active transponder and the reading system. In particular, we focused on determining the range of the communication between active tag and reader, and the shape of the RF field involved We assumed a set up configuration in which the activator was placed next to the receiver, about two meters above the ground, and the seal in front of the two devices. No obstacles were put between the system components.

The planar antenna of the activator generates a microwave carrier radiation with a circular conic lobe. The cone has a planar opening angle of about 90°. In Fig. 6 we plot the experimental shape of the communication region, defined as the region in which the seal is activated by the transmitter and the resulting reply is received by the reading unit. We show the evolution of the communication region as a function of the attenuation $Att_i = 10\log(W_i/W_{MAX})$, where W_i is the radiation power of the activating unit and W_{MAX} is the maximum possible power emitted by the unit. The figure points out that the communication region has the conic shape similar to the activation region only near the reader.

As the distance between the seal and the reader increases, the size of cone progressively reduces and, at large distances, secondary lobes appear. These lobes are more marked in correspondence to low activating powers.

Another important parameter is the system reading distance d, defined as the maximum communicating distance between electronic seal and reader along the cone axis. In Fig. 7 we show the behavior of d as a function of the attenuation Att_i for one of our active seals.

Fig. 7 points out the linear behavior of the reading distance d as a function of the module of the attenuation $|Att_i|$ in a semi-logarithmic scale. This means that the parameter d exponentially decreases with the attenuation of the radiating power. Assuming the linear behavior $\ln y_i = mx_i + q$, we have interpolated these data by using the standard method of linear least squares in order to calculate the parameters m and q. The result is

$$m = -0.27 \tag{1}$$

$$q = 3.13 \tag{2}$$

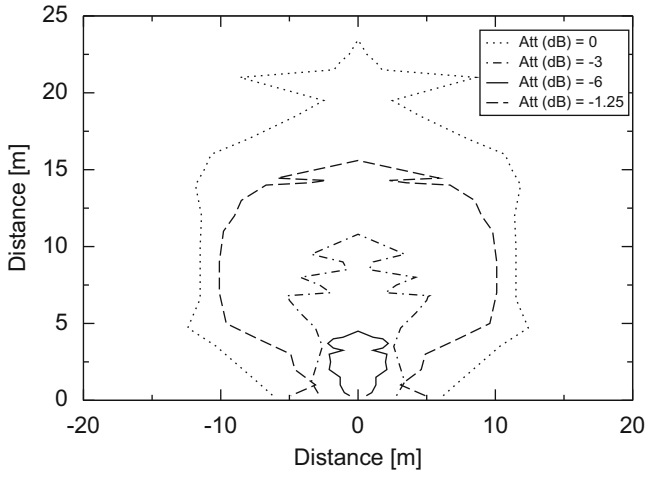

Fig. 6. Shape of the communication region for the system reader-seal. Different curves refer to different values of the activating power W_i.

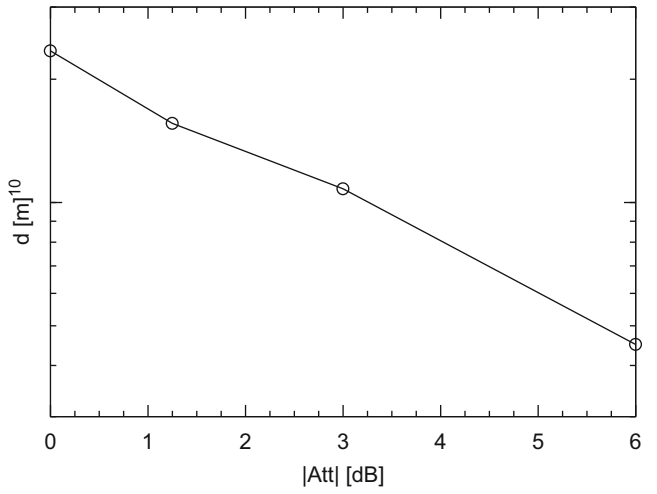

Fig. 7. Behavior of the reading distance as a function of the module of the attenuation Att_i.

Table 1
Main results of the static reading tests.

Attenuation (dB)	Seal number	Reading distance (m)
0	1	23.45
	2	17.30
	3	21.10
	4	14.55
	5	21.70
	6	21.60
	7	18.40
	8	18.90
	9	21.20
	10	19.30

Therefore, we have evaluated that the exponential behavior of the reading distance as a function of the power attenuation is

$$d \sim 22.87 \times \exp(-0.27|Att_i|) \tag{3}$$

In addition, we have evaluated the parameter d considering the mean value for a sample of seals. In fact, due to unavoidable manufacturing differences, every seal has characteristic activating and transmitting thresholds. Table 1 summarizes the measures for different seals, conducted at the maximum power emitted by the reader. In particular, we have found the following mean value $\overline{d} = (21.9 \pm 3.6)$ m. $\overline{d}$ and its error σ_d were evaluated through the standard statistical analysis:

$$\overline{d} = \frac{\sum_{i=1}^{N} x_i}{N} \tag{4}$$

$$\sigma_d = \sqrt{\frac{\sum_{i=1}^{N} (x_i - \overline{x})^2}{N-1}} \tag{5}$$

It is interesting to observe that the reading performances of some seals are deeply lower than the medium value $\overline{d}$. This behavior should be carefully considered in the design of a real system.

5. Field test

An operative field test was organized in order to verify the actual capabilities and security features of our active RFID sealing system. In the framework of a collaboration agreement with the Italian custom authority *Agenzia delle Dogane*, a field demonstration of the RFID sealing systems was set up in the commercial

Please cite this article as: Rizzo F, et al. Improved security for commercial container transports using an innovative active RFID system. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.04.006

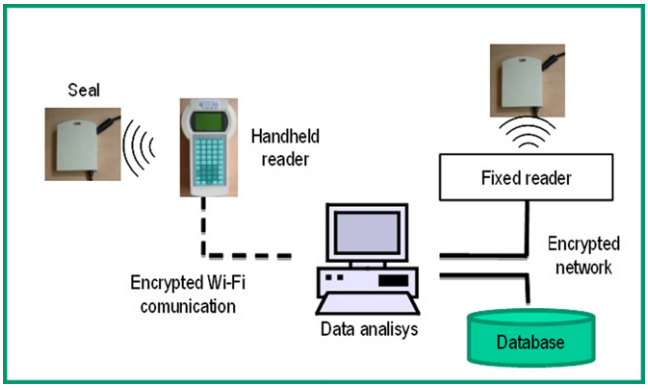

Fig. 8. Schematic representation of the information transmission logic used in the field test.

harbor of Livorno, in Italy, and in the correspondent hub located at 100 km of distance at Prato. Two identical infrastructures have been installed in the chosen locations: each system consisted of two fixed readers, one placed on the entrance lane and the other one on the exit lane, a handheld reader, a wireless and wired encrypted data network infrastructure and a server for the realtime data storage and visualization (Fig. 8).

In addition to the normal customs procedures, an electronic seal was installed on a selected commercial container unloaded from a cargo ship. During the installation procedure, the seal was initialized and associated to the container and to the truck numbers by a custom official using the handheld reader. The corresponding data were stored in the seal memory and sent by the handheld reader to the central database, through the encrypted Wi–Fi network. When the truck with the sealed container arrived to the harbor exit gate, the seal memory had been read by the fixed reader, and a cross check with the container number and truck number plate had been carried out. At this stage three different scenarios had been simulated:

- A wrong association between the container number and the truck number. In this case container was not authorized to leave the harbor.
- A seal tampering attempt during the harbor procedures. Also in this case, permission to leave the harbor was denied.
- All the checks at the fixed reading position were correctly passed and the delivery was authorized.

When the container received the authorization to leave the Livorno harbor, all the data stored in the seal memory were transmitted using an encrypted network, in order to prepare the container reception in the Prato hub.

During the transfer from Livorno to Prato an intermediate en-route check was performed using a handheld reader. The data acquired during this procedure were immediately shown on the handheld reader display and then uploaded to the central database, after arrival at the Prato hub. While approaching the entrance gate at the Prato hub, the seal was read by a fixed reader. The data stored in the seal memory were automatically compared to the ones acquired in the Livorno harbor and, once the seal status had been verified, the automated gate was opened.

The demonstration was compliant with the security requests and the expectations of the *Agenzia delle Dogane* and was deemed as successful. The possibility to transfer commercial containers from the Livorno harbor to the hub in Prato with higher security standards has been demonstrated. In particular, the real-time tampering revelation feature greatly increases the security of the whole supply chain.

6. Conclusions and future work

The goal of this work has been to investigate and design a new sealing system for commercial containers, able to significantly increase the security of the supply chain. A fundamental role in the realization of this new electronic sealing device has been played by RFID technology. In particular, the possibility of information recording, remote control and contactless reading, typical of active RFIDs, has given the possibility to develop a new device with a higher security level than standard mechanical seals.

The main security features studied for the sealing system are:

- Possibility to check the proper seal closure by using an internal passive RFID system, and to save operator identity and time of closure in the internal memory.
- Possibility to record every authorized and unauthorized operation made on the seal, along with time and date.
- Possibility to check the seal status, by remote interrogation of the electronic card memory (2.4 GHz–433 MHz active RFID communication protocol).

Experimental tests were conducted in order to determine the performance of the system. The results have emphasized that at full power the communication between the system components becomes active and efficient at a mean distance of $\overline{d} = 21.9$ m. We have also experimentally found that the shape of the communication region is a cone in proximity of the activator, which narrows as the seal-to-reader distance increases.

Dynamic reading trials, necessary to define the effective operating distance between the seals and the reading system when transponders are moving with respect to the reader, were not yet performed and will be further investigated. In fact, in this configuration we should consider some additional parameters affecting system performance. In particular, the reading capacity of the system will depend on the relative speed between the seal and the reader, and there will be a critical speed indicating the working limit of the system. Another important issue in the system performance is the possible interference in the communication range due to the presence of undesired medium, such as water or metallic materials. Also this relevant problem will be further investigated and the main results will be the object of a future work.

In the future developments of the sealing system, all the information concerning the container contents, which are currently written on the shipping note, will be saved on the memory seal reducing costs and possible human errors and increasing the overall security and automatization of the shipping process.

Finally, the low production cost of the seal (a rough estimate for industrial production is less than 50 euros) makes it highly suitable for large scale use on commercial containers. This cost is primarily determined by the electronics (the active RFID transponder coupled with the passive one) and then by the mechanical assembly of the device. The system is patent pending.

References

Craddock RJ, Stansfield EV. Sensor fusion for smart containers. In: The IEE seminar on signal processing solutions for homeland security, 2005. p. 5.

d'Agraives BC, Chiaramello M, Mascetti E, Tebaldi P. Identification by speckle interferometry. In: Proceedings of the 29th ESARDA annual meeting, symposium on safeguards and nuclear material management, Bruges, 8–10 May 2001. p. 606–9.

Encarta Encyclopedia. Online version: 〈http://encarta.msn.com/encyclopedia_761564981/Seal_(art).html〉.

Please cite this article as: Rizzo F, et al. Improved security for commercial container transports using an innovative active RFID system. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.04.006

Park T-S, Oh S, Cheong T, Lee Y. Freight container yard management system with electronic seal technology. In: Proceedings of the IEEE international conference on industrial informatics, 16–18 August 2006. p. 67–72.

Satish Bukkapatnam TS, Moore E, Komanduri R. Container integrity and condition monitoring using RF vibration sensor tags. In: Proceedings of the third annual IEEE conference on automation science and engineering, 2007. p. 585–90.

Sironi M, Poucet A, Littmann F, Chiaramello M, Heppleston M, Weeks G. New ultrasonic sealing systems for CANDU spent fuel bundles. In: Proceedings of the 29th ESARDA annual meeting, symposium on safeguards and nuclear material management, Aix en Provence, 22–24 May 2007.

Sklavos N, Zhang X. Wireless security and cryptography: specifications and implementations. CRC-Press, A Taylor and Francis Group, 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, Fl 33487-2742; ISBN: 084938771X, 2007.

Whiffen J, Naylor M. Acoustic signal processing techniques for container security. In: IEE seminar on signal processing solutions for homeland security, 2005. p. 7.

Yoong W-j, Chung S-H, Kim H-P, Lee S-J. Implementation of a 433 MHz active RFID system for U-port. In: Proceedings of the ninth international conference on advanced communication technology 2007;1:106-9.

Please cite this article as: Rizzo F, et al. Improved security for commercial container transports using an innovative active RFID system. J Network Comput Appl (2010), doi:10.1016/j.jnca.2010.04.006