A data system for the security and tracking of goods containers

P. J. Munday
Thales Research and Technology, Reading, UK

Abstract

This paper discusses the need for security of goods in shipping containers against the threat of theft, smuggling and contamination. It shows the need to have integrity and tracking sensors within the container, and to regularly report status and location to control centres. This paper describes work done within the PASR2005 SECCONDD activity towards an international interface standard for secure container data. It discusses the types of communications required from the container's sensor system, namely: a) long range reporting over the GSM cellular radio system – to be done periodically or when a significant event occurs, and b) short range reporting over a radio link in the 2.4GHz licence-free band. The paper outlines the types of data that need to be sent in the different cases, and discusses the recommended protocols for encoding, protection and communication of the data. These are based around standard protocols, e.g. Transport Layer Security and IEEE 802.15.4, but adapted where necessary to make transmission of the sensor data efficient, secure and reliable in the shipping container environment. There is a particular issue in a large port where there may be hundreds of shipping containers in radio range of an interrogator device, and where a special radio channel access protocol is required. The paper shows how the system can be implemented in a cost effective, low power device. The paper discusses how the data on location and security status of containers can be used by the relevant trade organisations and law enforcement agencies, e.g. for security risk assessment.

Keywords: containers, security, tracking, authentication, protocol layers, radio channel access, public key infrastructure, risk assessment, tamper protection.

WIT Transactions on Information and Communication Technologies, Vol 40, © 2008 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/DATA080241

1 Introduction

There are over 200 millions of goods container shipments around the world every year. It is estimated that every year, theft from containers runs into over 50 billion US dollars, and a significant amount of smuggling (e.g. of drugs and weapons) takes place using containers. In practice, it is only possible to physically search a small proportion of containers. X ray or radiological scanners are used to electronically search some containers. However, the largest forty foot (13.5m) containers can carry up to about 40 tonnes of material, and it can be hard for scanner operators to detect relatively small amounts of contraband hidden amongst this material.

Another, complementary, approach to container security is to add sensors which can detect things like its location, whether the doors have been opened, any intrusions through the walls, roof or floor, its temperature, and whether it contains radioactive substances. Data can be collected from these sensors and communicated by radio, either "long range" to a container control centre, or "short range" to authorities at a port or border crossing. Analysis of this data would enable suspicious events to be detected, e.g. an unusual route being taken, doors being opened at an unexpected place, or radioactive substances being detected. Also the data can be compared with customs declarations to look for suspicious things, e.g. the origin of the container in the declaration not being consistent with the tracking sensor information.

2 Requirements on the container data system

Containerised goods transport is a highly competitive business and so the container security data system has to be low cost, capable of operation anywhere in the world and for many years without batteries being recharged, and secure against tampering, eavesdropping and data corruption. These requirements in turn lead to the need for the data transmissions to be efficient and for battery power to be conserved as much as possible, e.g. by powering down components when not required. We coined the term "Goods Data Device" (GDD) to cover the unit(s) within the container that would collect, store and transmit the relevant data. (The GDD can also be used in an almost identical way on good vehicles.)

The data interfaces of the GDD need to be standardised so that the data can be read anywhere in the world, and where GDDs and their readers may be produced by different manufacturers. The European Commission, under the Preparatory Action for Security Research (PASR) 2005 programme, supported the SECCONDD (Secure Container Data Device) activity to study and recommend such a standard. The results of the study was a draft standard, for consideration by Comité Européen de Normalisation (CEN) and International Standards Organisation (ISO).

3 Interface standard

The recommended GDD interface standard contains the following protocol layers:

A. An application layer which covers the type of data that would stored, and its encoding for transmission over the radio links.

B. A protection and authentication layer which covers how container data devices and readers are authenticated and their data protected.
C. An "intermediate" layer which provides segmentation, automatic repeat (ARQ) of failed blocks, and channel access.
D. A physical layer which covers transmission of data over a radio frequency bearer, including frequency selection and modulation.

3.1 Application layer

In the application layer, we considered types of data that could be usefully carried in a GDD, both data generated by sensors within the container and other data that could usefully be carried by the GDD, e.g. the unique consignment reference (UCR) of the goods. Different trade organisations may have different needs and so we decided to make many of the data items optional. Items of data from the World Customs Organisation standards [1] have been used where appropriate.

The Figure below gives an example short range data transmission sequence between an interrogator and a GDD at a port.

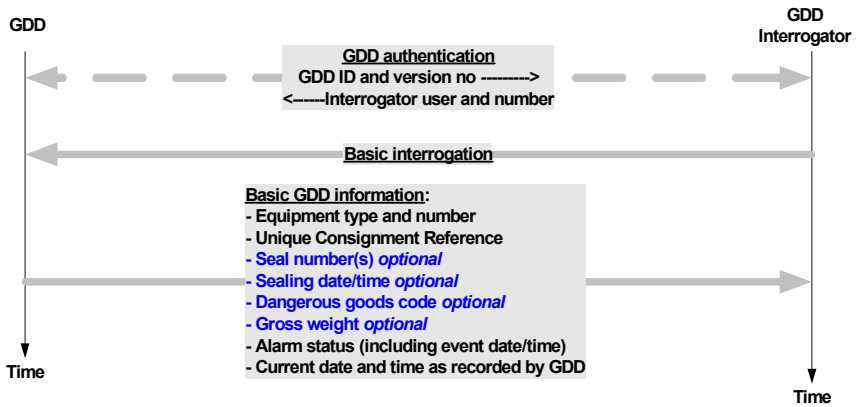

Figure 1: Basic interrogation of a GDD.

Here, after an initial authentication process (carried by a lower layer protocol), the interrogator makes a "basic" interrogation" and is then given "basic GDD information" which includes any alarms generated (e.g. "doors opened when they should not have been") and when they occurred.

There is danger that one trade organisation may use an interrogator to obtain information from a competitor organisation's container. To prevent this, the concept of a "Goods Identity Number" (GIN) for the shipment has been devised. The function of a GIN is analogous to that of a PIN used with a credit card. The GIN is generated when the container is loaded by the "consignor", and is then sent to relevant organisations, e.g. the "consignee", over a secure channel.

An interrogator with the correct GIN for a shipment can obtain extra data (shown in grey text in the Figure below):

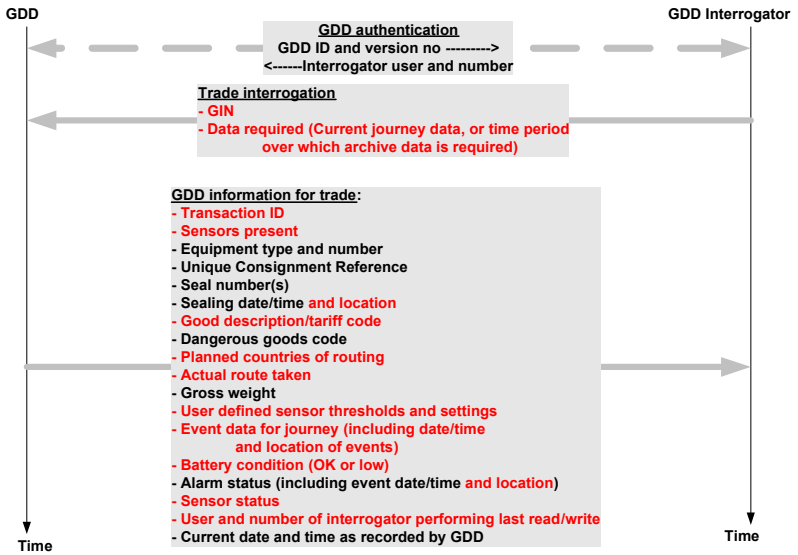

Figure 2: Trade interrogation of a GDD.

Long range radio communications to a control centre are initiated by the GDD, both periodically and when a significant event occurs (e.g. detection of an intrusion into the container). The data exchanged is as shown in Figure 3.

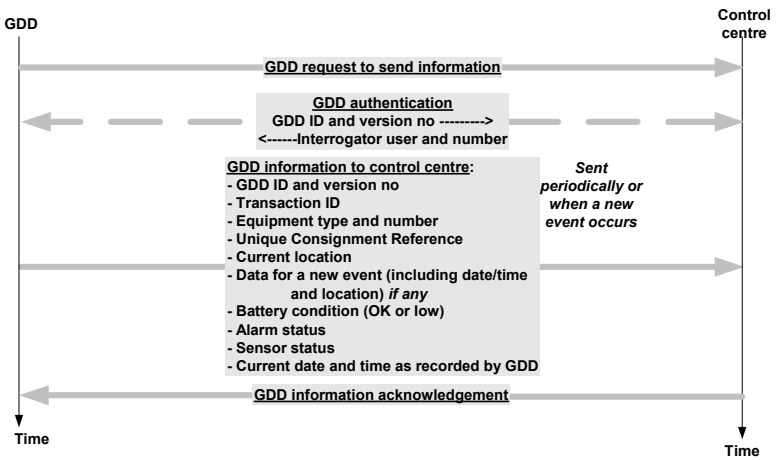

Figure 3: Long range data transmission.

3.2 Protection and authentication layer

The security procedures are based around the Transport Layer Security (TLS) [2]. Validation of GDDs and interrogators and encryption of data is provided by

a Public Key Infrastructure (PKI) approach. GDDs, interrogators and control centres are programmed with secret keys, key certificates and certification authority root certificates as shown in Table 1. There are two types of interrogator, "normal" and "LEA", the latter being those belonging to a law enforcement agency.

Table 1: Keys and certificates in devices.

	GDD	Normal interrogator and control centre	LEA interrogator
Keys	Secret key + certificate	None	Secret key + certificate
Root certificate	For LEA certification authority	For GDD certification authority	

Each interrogator and control centre is able to authenticate the GDD, using the root certificate to validate the GDD's certificate, and hence that the GDD is valid. (This is to prevent use of pseudo GDDs, e.g. which are designed to give misleading information.) The GDD is able to authenticate an LEA interrogator by checking if its certificate is valid, before allowing it access to privileged LEA information.

The data exchanges used in the process of authentication of GDDs to interrogators and of LEA interrogators to GDDs over a short range radio link are illustrated below.

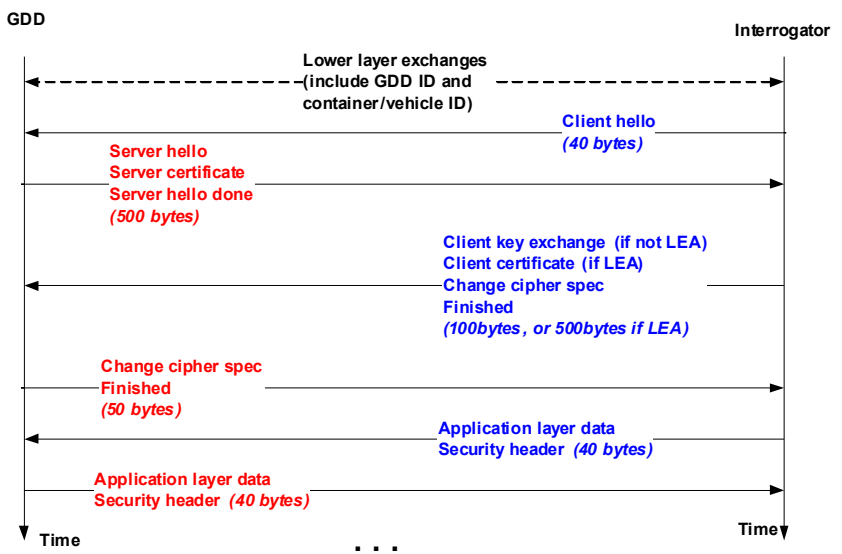

Figure 4: Authentication and protection data exchanges.

The GDD acts as a "TLS server" and the interrogator as a "TLS client". The different security messages required by TLS have been carefully concatenated to minimise the time taken to do authentication, which is important both for battery life reasons and to maximise throughput of containers through a busy port. Key certificates have used formats from the Wireless Access Protocol (WAP) [3] for efficiency reasons.

A similar mechanism takes place for security over the long range radio link between a GDD and a control centre.

The LEA keys can be changed on a regular basis to cover the case of an LEA interrogator being stolen or compromised. New keys and certificates can be sent over, for example, the internet.

Another security measure is to provide tamper protection to GDDs so that they cannot be altered without being permanently damaged and unable to operate, and so that data cannot be extracted from them.

3.3 Intermediate layer

The "intermediate" layer does the functions normally associated with the Transport, Network and Data Link layers of a communications stack, namely segmentation, framing, frame checking, automatic repeat (ARQ) of failed blocks, addressing and channel access.

Channel access for the short range link required some novel approaches. This is because there can be a large number (a few thousand) of containers at a port, and there may be several different GDD interrogators in use. The intermediate layer needs to ensure that data is communicated reliably and that interference between interrogations of different containers is minimised.

The radio channel access makes use of a "politeness algorithm" to give all GDDs in radio range equal probability of access to the radio channel, so that no interrogations take inordinately long. Other features of the intermediate layer include a "go back N" ARQ protocol, and a channel selection process where an interrogator looks for which of the 4 radio channels has minimum interference, before initiating an interrogation on that channel. The radio circuits in the GDD spend most of their time in a powered down state. They "wake up" every 3 seconds, check all 4 channels for the start of any interrogation, and if none are found power down again.

There are three different modes of interrogation using the short range radio link, illustrated below:

Mode 1): The interrogator sends a broadcast interrogation and each GDD in radio range (up to about 100m) responds. A novel (patented, see [4]) radio channel access protocol is used to minimise "clashing", i.e. GDDs in many containers trying to transmit at the same time. Summary security data is provided by each GDD.

Mode 2): The interrogator is given a container ID to interrogate. It sends a one-to-one interrogation to the GDD of that container. If the GDD is in radio range, it responds and gives information in accordance with the security privileges of the interrogator.

Mode 3): This is as mode 2 except that in addition, the data from the GDD is compared with data from the "cargo declaration" or "import/export declaration" [1] for the container, and anomalies are looked for.

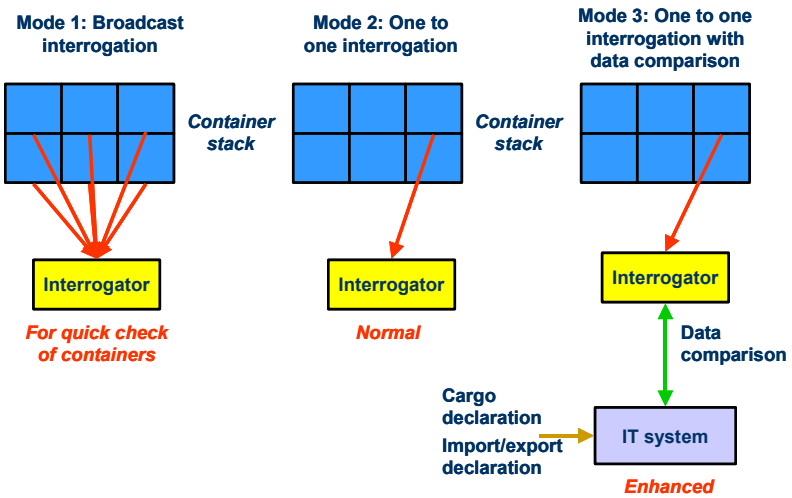

Figure 5: Short range interrogation modes.

The data obtained from the containers can be used to help identify which of them might have been attacked for theft, smuggling or contamination. In risk assessment of containers, the "risk score" for a container would be increased if, for example:

a) The container has no operative GDD.
b) An alarm condition has been raised by the GDD.
c) The container has been in a high risk location or on an unusual route (modes 2 and 3).
d) The GDD data is not consistent with the declarations about it (mode 3).

Based on the risk score from these and other criteria, containers judged to be higher risk may be subject to electronic scanning or physical searching.

3.4 Physical layer

For the short range radio link, a number of factors were taken into account in choosing the physical layer protocol: worldwide availability, license free, low power consumption and readily available components. These factors lead to the choice of the 2.4GHz option of the physical layer of IEEE 802.15.4 [5], which is used with the Zigbee protocol. This provides a data rate of 250kb/s and uses spread spectrum modulation to overcome impairments due to multipath.

For the long range radio link, similar factors were taken into account. No system was fully useable worldwide but the best option was found to be GSM/GPRS. GSM covers most of the important land areas in which container transport takes place. It does not cover oceans (except coastal areas). The GDD

sends long range information when GSM is available. When GSM is not available, the information is stored until GSM again becomes available. It is also possible for a radio on the platform carrying the container, e.g. SATCOM on a ship or lorry, to relay the long range information between GDD and control centre. Analysis indicates that security risks are much greater on the land journey compared to the sea journey, and so delays in reporting security information when a container is at sea is not seen as a significant problem.

When a periodic report is due over the long range link, or an event occurs which requires reporting, the process illustrated below takes place. The GDD processor, GPS unit and GSM/GPRS unit are all powered up at the same time. While a position fix is being taken, the processor starts up and the GPRS unit makes a connection to the GPRS network. The required information is then sent to the control centre in a set of GPRS packets, with protection and authentication taking place as required. The algorithms have been carefully chosen to minimise power consumption, for example the protection and authentication calculations can take place in a total of about 240ms on a low power processor.

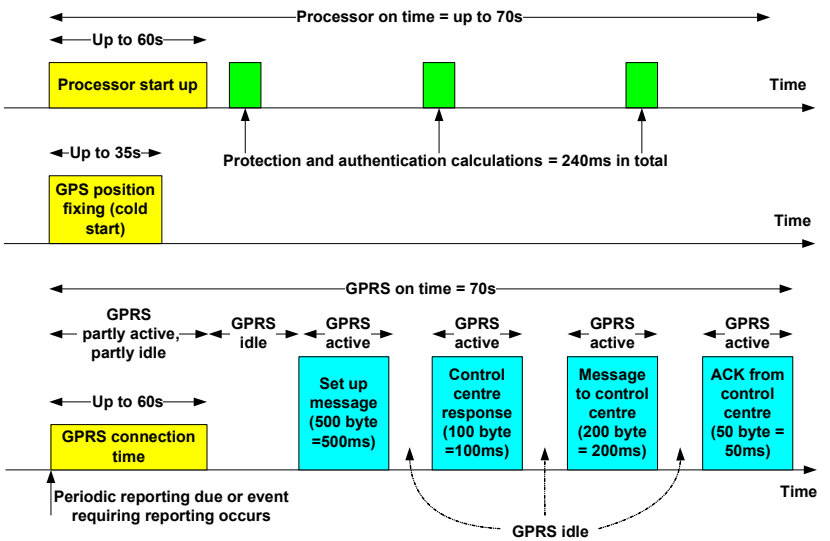

Figure 6: Processes involved in long range data transmissions.

4 Conclusion

The data standard developed within the SECCONDD activity provides a reliable and secure method of interfacing security and tracking sensors in a goods container to readers and control centres. The required equipment is capable of being low cost and having a battery life of several years. Use of such equipment can provide a marked improvement in the security of goods containers by:

a) Providing information for risk assessment, e.g. at a port or border crossing.

b) Providing information for forensic analysis of container crime.
c) Providing real time or near real time alerts at a control centre in the event of security attacks, e.g. for theft, smuggling or contamination.

The GDD information can also be used non security reasons, e.g. to enable the trade to locate containers and know when they are likely to arrive, and to know what happened to a container on its journey and which party might be responsible for any damage inflicted on the container.

Acknowledgements

The author would like to express his appreciation to colleagues who worked with him on the SECCONDD project, from Thales Research and Technology (UK), Her Majesty's Revenue and Customs (UK), Cotecna Inspections, Selex Communications (Italy) and Comité Européen de Normalisation (Belgium). He would also like to thank the European Commission for supporting the SECCONDD activity, and the directors of Thales Research and Technology (UK) for permission to publish this paper.

References

[1] World Customs Organisation (WCO) Framework of Standards to Secure and Facilitate Global Trade, June 2005.
[2] IETF Network Working Group, The TLS Protocol Version 1.0, RFC 2246, January 1999.
[3] Wireless Application Protocol Forum, WAP Certificate and CRL Profiles, WAP-211-WAPCert, 22 May 2001.
[4] UK Patent Application: GBP96472, "Wireless Communications Apparatus", Filing number: 0708428.8, Filing date: 1 May 2007.
[5] IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) IEEE Std 802.15.4TM – 2006.
[6] SECCONDD, Final Report Annex 1, Recommended Standard, available at www.thalesresearch.com.