WHAT CAN RFID DO FOR VANETS?
A Cryptographic Point of View

J. Munilla, A. Ortiz and A. Peinado
Dept. of Ingenieria de Comunicaciones, E.T.S. Ingenieria de Telecomunicacion, Universidad de Malaga, Málaga, Spain

Keywords: RFID security, VANET, Authentication, Traffic safety.

Abstract: Vehicular ad hoc networks (VANETs) are becoming more popular as a way to increase the traffic safety and comfort. The inclusion of RFID technology in the VANETs architecture could enable the development of interesting new services and improve the overall results. However, in addition to the typical problems of RFID systems, new challenges arise in this scenario (RFID-VANETs) that must be solved. This paper analyzes the security aspects of these applications.

1 INTRODUCTION

Nowadays, vehicular ad-hoc networks are presented as a new generation of networks oriented to improve the safety and driving comfort. These networks allow connectivity among mobile hosts. This way, vehicles in a VANET can share information to each other in a short range by using the 802.11p wireless technology. The use of a light infrastructure or a backup network can improve the services offered in a VANET providing the so called vehicle-to-infrastructure communication (V2I) (Hartong, 2007). This infrastructure is not only composed by 802.11p base stations but, there are several approaches proposing the use of a RFID (Radio Frequency Identification) infrastructure (Lee, 2009) for many purposes such as positioning or traffic signals identification. Thus passive RFID tags can be used as information sources at different points such as traffic signs (Ortiz, 2010). The advantage of this option is that they do not require a power source, reducing the maintenance and thus the global cost of the system.

In vehicular applications, RFID is typically used in a scenario where the tag is located on the vehicle and the reader is placed on the road. Tags are usually read statically, since the vehicle will stop over the reader. Bus tracking is a typical application using this scheme (Lee, 2009). Most of these applications belong to the comfort category.

In VANETs there are two different types of information that can be used to improve the traffic safety. The first corresponds to information coming from other vehicles regarding traffic congestion status or accident alerting. The second corresponds to environmental information coming from traffic signs, speed limits, motorway tolls or semaphores.

The use of RFID technology to collect environmental data requires reading tags deployed on the road and the reader to be located on the vehicle. The RFID infrastructure consists of a series of RFID tags located at any signalling point. So, the tags have to contain information regarding the point in which they are located (i.e. a speed limit, a dangerous bend, etc.). Most of these applications belong to safety-related category of VANET applications.

This paper focuses on the security issues related to the use of RFID on vehicular applications. Section 2 shows the state of the art of RFID on vehicular applications. Section 3 depicts future uses. Section 4 analyses the security requirements for RFID in VANETs. Section 5 discusses the Security and feasibility of secure RFID-VANETs architectures and finally Section 6 concludes.

2 PAST AND PRESENT OF RFID FOR TRAFFIC USE

Electronic Toll Collection (ETC) has been until not long ago the main use of RFID for traffic. Since 1992 active RFID tags have been used in vehicles to automate the toll process. These tags, mounted internally (windshield) or externally (near the plate),

Munilla J., Ortiz A. and Peinado A. (2010).
WHAT CAN RFID DO FOR VANETS? - A Cryptographic Point of View.
In *Proceedings of the International Conference on Security and Cryptography*, pages 295-298
DOI: 10.5220/0002929502950298

allow an automated toll process where the vehicles can proceed without stopping to pay at the tollbooths. Theses system consist of three basic parts: the automatic vehicle classification based on sensors that count the number of axles, the automatic vehicle identification which uses RFID tags, and the violation enforcement where cameras are used to identify evaders.

The distance between the overhead antenna in the ETC facility and the tag of the vehicle is around a few meters and, thus the operating frequencies for these applications are usually UHF or microwave (Europe EN 300 440). .

For instance EZ-Pass on the east coast of the United States, Fast-Track on the east coast and SunPass in Florida, use active UHF RFID tags for vehicle identification. As mentioned, the batteries of these active tags need to be replaced after one or two years. Although these active tags are not power constrained and probable secure cryptographic solutions could be implemented, some researches have proved that these tags provide little or not security (Green, 2008).

Other uses of RFID tags in relation to the vehicles but not so much to the traffic is the use of cards to pay in gas stations and as vehicle anti-theft systems (immobilizer). These cards work usually in HF and provides high standard of security. However, there have also been famous cases of attacks; e.g. the security of the DST (Digital Signature Transponder) manufactured by Texas Instrument, with key lengths of only 40 bits, and used by millions of customers was defeated by performing reverse engineering and key cracking (Bono, 2005).

3 RFID IN FUTURE VANETS

RFID technology can be easily integrated in vehicular networks as it provides a low cost solution for V2I communications. The RFID applications currently in use employ this type of communication. European Union is working in RFID tracking systems to issue automated tickets for minor traffic violations (Asset, 2010), as an application of the Electronic License Plate. Other proposals describe automatic payment systems of parking-fess, or traffic-light priority systems for easing traffic congestion and reducing road accidents (Lee, 2009), but all of them with the same architecture: tag on vehicles and reader on the road.

Since RFID technology deals with identification and authentication, it represents a further step in the information collection systems. This way, RFID constitutes an alternative mechanism for I2V (infrastructure to vehicle) communication with important advantages.

Low cost of this technology allows the system to disseminate a huge number of tags to complement traditional traffic signalling. The information obtained from RFID tags can be considered as local meaning information due to the reading coverage limitations of this technology. The infrastructure gains a real advantage since a new non-attending signalling system can be deployed. This signalling system will always work under extreme conditions such us VANET loss connection or bad weather conditions (reduced visibility). Safety-related applications, such us collision avoidance, cooperative driving, traffic optimization, lane-changing assistance or road conditions warnings, may be implemented.

RFID signalling may be implemented as a complementary support of the existing technologies. In this way, the information collected from different means can be analysed to obtain trusted and more accurate information. Other I2V applications, such as collision avoiding system in urban intersections or wrong way detection system, may be implemented by means of RFID technology.

Some constraints exist when we try to implement this technology: mainly, the speed of vehicles. Several initiatives including tag on vehicle architectures have been previously published with different objectives in mind (Lee, 2009), (Penttila, 2004), (Chon, 2004). The experimental results state the maximum speed at 100 Km/h, with a high error rate in readings.

Although these results allow the utilisation of this architecture in reduced speed areas, such as urban roads, much more research must be applied. The most important constraint is the reading range and the total reading time which includes activation time and transmission time.

However, none of these proposals have taken in mind security requirements to allow a secure and trusted utilisation of the system. In the next section, we analyse these proposals from a cryptographic point of view.

4 SECURITY REQUIREMENTS

The main problems about security in RFID reside in privacy and authentication (Juels, 2006). Privacy must be applied to avoid physical tracking attacks, where a forge reader can interrogate a legal tag without the knowledge of its owner. Authentication allows readers and tags to verify the real identity of each other. However, depending on the specific application the security requirements may be modified (Avoine, 2005).

Two scenarios are considered: tag on vehicles and reader on vehicles.

Tag-on-vehicle Architecture. In these situations the reader is connected to a backend server or central database while the tags are attached to vehicles. This configuration allows the reader to make hard computations with the help of the server. Thus the limitation of this architecture resides in the tag. Vehicles speed is not a problem for these applications as the vehicles (and hence the tags) interact with the reader at very low speed or when they are completely stopped.

Taking in mind all these features, the security requirements for these applications are practically the same of that for a traditional RFID system, and hence, the protocols proposed for RFID may be applied in most situations.

Reader-on-vehicle Architecture. This architecture corresponds to future or recently proposed applications where the main objective is related to traffic safety. These applications use RFID tags to get information from the road, where the tags are located. It is important to note that this architecture presents severe limitations derived from the simplicity of tags (as any other RFID application) and the connectivity restriction of the readers. The connectivity depends on the VANET instant behaviour and range. Another relevant restriction comes from the high speed of vehicles during the identification process. As a consequence, most of the protocols proposed in the literature are not suitable for this scenario. The security requirements for this architecture are the followings.

Confidentiality. It is not necessary as those applications provide information about road conditions. This is the general criteria applied to safety-related applications (Yousefi, 2006).

Untraceability. Since the tags are located on a fixed place on the road, traceability does not constitute a problem. This fact simplifies notably the identification protocols.

Authentication. It is mandatory. The main risk resides in the possibility that an attacker inserts fake tags on the road producing fake readings. Authentication scheme must be resistant to reply attacks and tag-cloning attacks.

Non-repudiation. This is not a requirement for this kind of application.

Availability. Availability is not the main concern provided that RFID is not the unique mechanism on-board to get road information.

5 OPTIONS AND FEASIBILITY

Security requirements for *tag-on-vehicle* architectures coincide with that of traditional RFID systems. For this reason the only applications currently in use are based in this architecture. In spite of that, many of these applications do not apply security mechanisms or apply very low level security, such us toll collection systems described in section 2.

Security requirements for *reader-on-vehicle* architectures apparently simplify the RFID identification schemes as only authentication is mandatory and anti-collision is not necessary. However, the existing protocols can not be applied due to constraints imposed by vehicle speed, reading range and reader connectivity lack. Furthermore, although transmission time is short, it is important to note that any attacker can interrogate a tag for undefined time because the tags are located on the road with no physical access restriction.

Cryptographic tags may be divided into two categories: symmetric-key tags and asymmetric-key tags. Symmetric-key tags are not suitable because the key management is too complex. The number of tags to authenticate is too high, and the readers on vehicles must know all the secret keys. Remember that the reader have no permanent connection with the backend server.

A special type of asymmetric-key cryptosystems is the identity-based encryption and signature, particularly designed to reduce the global complexity using the own identification data (such as the email address) instead of digital certificates as a public key for encryption and signature verification (Baek, 2004). In (Liang, 2008), it is proposed an implementation of identity-based encryption and signature in RFID systems. The implementation of these schemes requires the existence of a central trusted server (PKG). PKG first generates its master (private) and public key pair. Then the PKG generates the private key of every user associated with his identity. In the case of RFID systems, this key may be loaded in each tag and reader prior to the system deployment. The main advantage of these schemes resides in the mechanism to obtain the public key of another user. In traditional asymmetric schemes, public keys must be retrieved from a public repository. In identity-based encryption, every user can generate the public key of another user employing the identifying information of the receiver (for encryption) or the signer (for signature) and the public key of the PKG. Hence, no connection has to be established to verify the signatures sent by the tags. Thus, identity-based encryption and signature seem to be the most suitable schemes to this architecture, although more research has still to be applied because identity-based cryptography is based on asymmetric-key cryptosystems, and its computational complexity must be taken in mind

6 CONCLUSIONS

The feasibility of RFID applications in VANETs has been analysed from a cryptographic point of view. In addition to the typical problems of RFID systems, new challenges arise in this scenario (RFID-VANETs) that must be solved. A classification of RFID-VANET applications is presented based on the reader-tag architecture, resulting in two categories: tag on vehicles architectures, similar to traditional RFID systems, and reader on vehicles architectures, with new challenges to solve. Most relevant guidelines to secure this kind of systems have been presented, since currently, most RFID systems can be characterized by an important security lack.

ACKNOWLEDGEMENTS

This work has been partly supported by the Spanish Ministry of Science and Innovation and the European FEDER funds under project TIN 2008-02236/TSI.

REFERENCES

Hartong, M., Goel, R., Farkas, C., Wijesekera, D., 2007, "PTC-VANET Interactions to Prevent Rail Intersection Crossing Accidents" in VTC 2007.

Lee, Y. M. Yoo, C. G. Park, M. Kim, M. Gerla, 2009, "Installation and Evaluation of RFID readers on Moving Vehicles", in Proc. of VANET'09

Ortiz, A., Peinado, A., Munilla, J., 2009, "A Scaled Test Bench for Vanets using RFID Signalling". in *Comp. Intelligence in Security for Information Systems*.

Green, M., 2008, Attacking and Defending RFID Systems.

Bono, S. C., Green, M., Stubblefield, A., Juels, A., Rubin, A. D., Szydlo, M., 2005. "Security analysis of a cryptographically-enabled RFID device", in *Proc. of the 14th conference on USENIX Security Symposium*.

Asset-road Project, 2010, http://www.project-asset.com

Penttilä, K., Sydänheimo, L., Kivikoski, M., 2004, "Performance development of a high-speed automatic object identification using passive RFID technology", in *Proc. Of the 2004 IEEE International Conference on Robotics & Automation*.

Chon, H. D., Jun, S., Jung, H., An, S. W., 2004, "Using RFID for Accurate Positioning", in *Proc. of 2004 International Symposium on* GNSS/GPS.

Juels, A., 2006, "RFID Security and Privacy: A Research Survey", Selected Areas in Communications, *IEEE Journal*.

Avoine, G., 2005, Cryptography in radio frequency identification and fair exchange protocols, Ph.D. Thesis.

Yousefi, S., Mousavi, M., Fathy, M., 2006, "Vehicular ad hoc networks (VANETs): challenges and perspectives" in *6th International Conference on ITS Telecommunications*.

Baek, J., Newmarch, J., Safavi-Naini, R., Susilo, W., 2004 "A survey of identity-based cryptography", in Proc. of the *10th Annual Conference for Australian Unix User's Group*.

Lian, Y., Rong, C., 2008, "RFID system security using identity-based cryptography", LNCS 5061, 2008, Springer-Verlag Berlin Heidelberg.