Security in Intelligent Transportation Telematics

Erich H. Franke

Abstract

More than 10 years ago, the European Telecommunications Standards Institute (ETSI) began to standardize the communication between vehicles and infrastructure in so-called "Intelligent Transportation Systems (ITS)." This communication is supposed to be self-organized, which means, it has to be operated without the assistance from an access network. However, since most of the communication components are deployed in an inhomogeneous manner by vehicle operators "in the wild," the security aspects are—for the lack of a better word—challenging at least. We will examine the security of ITS networks by discussing different modes of possible attacks.

1 The ITS Ecosystem

In August 2008, the European Commission decided the harmonization of the use of the radio spectrum for safety-related applications of Intelligent Transport Systems (ITS). Furthermore, starting around September 2010, the EC published its general view about the communication architecture of ITS systems, as defined in ETSI EN 302 665 V1.1.1 (2010-09). The communication between the different types of ITS stations may use either direct point-to-point communication in single or multiple hops between the source and destination stations, but the access to public and private networks, including the global Internet and even existing infrastructure and satellite broadcast have been considered in the document.

E. H. Franke (✉)
AFUSOFT Kommunikationstechnik GmbH, Königsbach-Stein, Germany
e-mail: erich.franke@afusoft.com

P. Glauner, P. Plugmann (eds.), *Innovative Technologies for Market Leadership*,
Future of Business and Finance, https://doi.org/10.1007/978-3-030-41309-5_3

The participants of the ITS ecosystem can be assigned to four "subsystems," counted in the number of their appearance:

- Vehicular subsystem: i.e., ITS components can be deployed in motor cars, trucks, security vehicles or similar, in motion or parked. Vehicular subsystems are expected to be deployed in high volume, compared to other types of subsystems. Therefore, sometimes Intelligent Transportation Systems (ITS) are—slightly incorrectly—labelled V2X, an acronym, designating communication "vehicle-to-anything." In most of the cases, the ITS components used in vehicles are owned and operated by the owners of the vehicles themselves.

  A common application is the traffic accident warning, which we will discuss later.
- Roadside subsystem: consisting of components, mounted on traffic lights, gantries, poles, etc. In most cases, the deployed ITS components are owned and operated by the authorities or companies responsible for road maintenance.
- Personal subsystem: e.g., hand-held devices for pedestrians or bicyclists. ITS components in this domain are presently not very common. However, as soon as they become part of mobile phones or tablets, their number is expected to increase significantly.
- Central subsystem: traffic control centers, emergency warning centers, adverse weather forecast centers, etc.

In theory, a variety of existing networks may be used to convey ITS messages between subsystems. However, since particularly the mobile components require to communicate with each other, a decentralized, globally available, low-latency and self-organizing communication scheme is required.

To fulfill these requirements, ETSI standardized a communication scheme, based on IEEE 802.11p, which is known in Europe under the label "ETSI-G5." The protocol stack of G5 is similar to standard WIFI; however, its parameters have been modified, to allow connectionless communication even between speeding vehicles and particularly defines the use of the frequency band between 5.85 and 5.925 GHz, which has specifically assigned to ITS safety critical applications. In Europe, this protocol is known as ETSI-G5 and considered as the basis of the Dedicated Short-Range Communication (DSRC) standard.

In this context, it is very important not to confuse the license-free broadcast, WIFI-like, short-range communication protocol ETSI *G5* with the "next-generation mobile communication standard" *5G*.

The latter is a mobile communication scheme, similar to 4G/LTE which requires an operated cellular network and requires, needless to say, communication contracts to be closed between users and network operators and operation fees paid.

Of course any public mobile network can be used to convey V2X messages, technically. The security, integrity, and privacy, however, depend on the security properties of the respective network and its operator.

The underlying network layer structure of public mobile networks, such as 5G, as well as the different data and voice communication capabilities thereof are beyond the scope of this document.

However, two important properties have to be discussed, regardless of the actual network been used: latency and channel capacity. We have to have an eye on them, since these parameters are important for the understanding of operation integrity and of the vulnerability against denial-of-service attacks:

- Latency: Denotes the travelling time of a data packet from the information source to the destination. For highly dynamic traffic information systems, minimizing this latency is desirable.
- Channel capacity: The amount of information, which can be conveyed through any given communications channel.

The requirements for data transfer in ITS communications are different from general data communications, though:

- Point-to-multipoint: most of the ITS data packets are generated in one station, but intended to be received and processed by many recipients, if not for all, in a given range. The transmission from a roadside station, for instance, is subject to be received by all passing vehicles. Emissions from vehicles shall be received by all other vehicles, roadside stations, etc. in the respective range. Point-to-point operation is merely uncommon in ITS.
- Highly dynamic environment: Since the traffic scenario is spatially dynamic, so is the structure of information links for example between speeding cars. In the ITS domain, the term “geo-networking” is commonly been used to describe this kind of scenario. Therefore, ITS communication is practically always connectionless and considered self-managed.
- Information Relaying: Important messages will be relayed by other vehicles in order to extend the information range.

Very well! With ITS, we have to deal with an ecosystem consisting of inhomogeneous entities that dynamically provide each other with relevant traffic-related information. In a perfect world, where all human beings are brothers, everything would be fine so far. In the real world, however, action must be taken to prevent malicious participants from abusing the system. Let us investigate this aspect by examining a typical scenario.

2 Application Scenario Versus Vulnerability

One of the simplest, yet highly important applications derives from the *car crash/traffic jam warning* scenario. Given the—unfortunately inevitable—fact that two vehicles collided on a highway. The airbag sensor will trigger an emergency message, which can be received by all other vehicles in the given range of—

say—200 m. Based on the transmitted geo information, the onboard computer of approaching vehicles—particularly when autonomously driving—may then decide, to perform an evasive maneuver, emergency breaking or such. This measure is more or less automatically controlled ("Direct Control") and intended to prevent another collision by supporting cameras and laser scanners of autonomous vehicles or the eyeballs and/or the brain of a human driver.

The risk level reduces with the actual distance to the crash site. In—say—500 m distance, an approaching vehicle gets a "Collision Risk Warning" (LCRW, ICRW), a bit further upstream, a "Road Hazard Signal" (RHS) is raised for awareness and further away, an information is given, e.g. to be displayed as an "In Vehicle Signage" (IVS). All these steps are considered "Primary Road Safety Applications." Related scenarios include warnings of construction sites or slow-moving maintenance vehicles.

In each case, the "warning" will very likely trigger some automatic actions in the receiving vehicles, from emergency braking, evasive maneuvers, and speed reduction. Since these actions have a severe impact on the traffic flow, the "warning" messages have to be protected adequately.

But there is an even more important scenario: Think about an ambulance, a fire truck, or a police car in a city, which try to drill through the common urban traffic jam during rush hour. Not an easy task and also rather risky! An "electronic lightbar," (e.g., the German "blue light") using ITS communication, as we are currently testing it, could help to warn the other drivers from an approaching rescue vehicle.

But an even better solution is to offer the emergency vehicles free travel at traffic lights by controlling them accordingly. The traffic lights have to be equipped with ITS receivers—so called "roadside units" which examine specific messages denoting the approaching rescue vehicle and identifying their trajectory using the vehicle's geo position and movement vector.

When the trajectory of the rescue vehicle crosses an intersection, the traffic light controller can switch to a special signal phase in order to stop other vehicles and therefore give the rescue vehicle an appropriate right of way.

Both the *car crash/traffic jam warning* and the rescue vehicle right of way scenario can be very helpful. However, since they can have a severe impact on the traffic average flow—on a motorway as well as in a city—any abuse must efficiently be prevented.

3 Signature as the Primary Security Measure

The term "abuse" implies an intentional attack of some kind. This leads our discussion toward the security of such a system: Information Technology Security and Information System Security denotes the protection of the system components "... from intentional theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide ..." as this term is generally defined.

The creators of the ETSI G5 standard decided to cryptographically protect communications, however by *signing* the transmitted messages, rather than *encrypting* them.

The reason for this decision is that each participating station is basically able to receive every message, even if it does not currently have possession of a valid crypto key. In ETSI's opinion, each recipient is responsible for deciding whether or not to use any unsigned or erroneously signed message received.

Of course, a valid message may only be created properly if the sending party has used a valid certificate for signature.

The key distribution system has to take into account, that participants receive their certificates through different channels. This means that in the background, a hierarchical and geographically distributed Public Key Infrastructure (PKI) has to be implemented. Consider, for example, that a French vehicle on a German motorway has to exchange messages with an Italian truck easily, even though all the certificates have been issued in different countries!

The actual certificates, however, have to have a limited validity lifetime. However, the actual certificates must have a limited validity period. Since, for example, a stolen RSU could be used for a hostile attack on the road infrastructure and the vehicles on it, it is important to keep the time window for nay successful abuse as short as possible.

In present systems, the certificate used for signing actual messages, is valid 24 h maximum. From a security point of view, although a much shorter interval—e.g., 1 h—would be desirable, this would have a significant impact on the practical usability of the system. Keep in mind that the certificates must be requested online from a PKI, as they cannot be kept in stock for security reasons. This implies that each participant must have more or less permanent online access to the Internet, which may not be a problem for a stationary road unit (RSU), but might have a massive impact on the mobile users, for example, cars and trucks.

The process of requesting the certificates has to be secure—too. Presently, a four-step scheme is implemented. On the top level, every manufacturer of ITS equipment has to be registered with his/her local security agency. Using the "manufacturer's certificate," the provider may request intermediate certificates to create a "trust anchor." All certificates in the chain have different, limited lifetimes, and of course, all requests are cryptographically protected. If all intermediate steps have been processed successfully, the "Authorization Ticket" can be requested, which is then used for signing during the next 24 h period.

4 Security, Safety, Integrity—and Privacy—Issues

Let us now discuss the different implications of the security issue.

Virtually all mobile components of an Intelligent Transportation System, i.e., particularly those mounted in vehicles, are owned and operated by the users themselves. Therefore, the *physical* security, e.g., theft prevention, requires appropriate precautions of the very users. This is particularly important, since the

ITS components contain credentials, e.g., crypto keys. Although these credentials have limited validity, they may still be misused by malicious users. The same consideration applies to road side units. Malevolent users, who succeed in gaining access to a road side unit, might exploit the RSU's transmissions in order to simulate traffic congestion or the like. This kind of misdirection is one of the most likely scenarios for malevolent attacks on ITS.

Another security issue, to be considered, is the classic "Denial of Service" attack. In ITS, this jamming scenario is not always caused by an intentional misbehavior of users or attackers. Since ITS messages are conveyed by radio frequencies, mostly on 5.9 GHz, these can easily be disrupted. This means that any ITS system must be aware that the probability of reception of messages is anything but stable. The conditions are rather like in any Wi-Fi network.

However, malicious attacks are usually in the minority in this scenario.

In general, the reception probability is significantly reduced simply because the vehicular users move relatively quickly on motorways or in an urban area, yielding undefined a nonstationary signal reflection patterns.

Given the fact that ITS uses broadcast transmissions rather than connected ones, the information redundancy is created by repeating the same message with a relatively high information bandwidth.

The latter is important in order to get at least some of the data through the channel. The so-called Cooperative Awareness Message (CAM), which tells all other users of the state of a vehicle, its location, its movement vector and a lot of information more, is repeated with a variable rate between ten times a second down to one per second. The actual transmission rate depends on the speed of the vehicle, if it follows a curve or any state change.

Now consider a scenario on a typical motorway intersection, with several thousand vehicles per hour speeding in different directions. Even if only a few percentage of vehicles are actually equipped with ITS components, there is a lot of radio transmissions on the air.

For information "self-defense," each ITS component uses so-called congestion control functionality, reducing its transmissions if the channel is highly populated.

Therefore, it can be said that traffic flow restrictions are not always the result of an external attack.

The term "safety" denotes "... a state in which ... you are safe and not in danger or at risk..." according to the Cambridge Dictionary.[1] We might discriminate "safety" from "security" in conjunction to unintentional, accidental, and even random risks. In ITS, designers have to take precautions not only against the result of malicious attacks, but also against effects caused by mere system malfunctions. A good example is the GNSS position, which is included in the geo-networking portion of virtually every ITS message. If the satellite navigation signals is jammed, e.g., by multipath reception in an urban environment in one vehicle, the geodetic position may be erroneously distorted. All recipients of this information hence have

[1] https://dictionary.cambridge.org/de/worterbuch/englisch/safety, accessed on December 4, 2019.

to examine the integrity information supplied, in order to be sure, where the sender's vehicle is actually located. This is important, since all moving participants record their recent positions in so-called "traces," posting them over-the-air. All other receivers may exploit these "traces" in order to assure, that their current movement vector is compatible, to provide a form of early warning to a possible collision hazard.

Failing this precaution might lead to unintended behavior, particularly in autonomous vehicles, such as unnecessary lane changes or even braking maneuvers.

In ITS, we have furthermore to assure privacy. The Business Directory defines this term as "...the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational is to be revealed...".[2] Privacy is one of the key factors to assure user acceptance of this technology.

However, full protection of users' privacy is not an easy task at first. ETSI G5 communication works similarly to other Wi-Fi networks. Each message contains a unique identifier, the MAC address (Media Access). This MAC address is used to ensure that informational messages or replies can be forwarded to the intended recipient.

Since G5 usually operates based on broadcast messages, this MAC address is far less important than in a Wi-Fi network. As a consequence, ETSI defined a scheme to modify the MAC address of each sender frequently during operation in a way, which cannot be reversed. This method, called "pseudonymization," is intended to technically ensure, that it is not possible to identify a mobile user after a short period of time.

5 Why May Someone Want to Attack Any ITS Network?

When we talk about an abnormal, unwanted, or even illegal use of data in an ITS network, we have to keep in mind that the nature of these "nonstandard users" and their intentions can be very different.

We can identify the following groups:

- Road service providers
- Law enforcement agencies
- "Curious persons"
- Malicious attackers

When discussing privacy issues in relation to the first two parties, conflicting aspects must be taken into account.

The transport service providers want to use the data of mobile users to monitor the utilization of the road and the traffic flow. These traffic data are valuable

[2] http://www.businessdictionary.com/definition/privacy.html, accessed on December 4, 2019.

for the actual road users, e.g., in order to derive suggestions for diversions or alternative routes. Of course, these data could also be sold by road service providers, but this would not harm the privacy of a single user. Usually, anonymized or "pseudonymized" data are sufficient to provide this task.

A little bit off are requirements brought in the discussion by law enforcement organizations to use ITS movement data, e.g., for speed violation ticketing or the prosecution of red light violations at traffic lights. Technically, it would be possible to implement these—somewhat strange—ideas with ITS, since all information necessary are already included in cooperative awareness messages (CAM). However, automatic ticketing systems, based on ITS technologies are, not yet considered legal, at least today in western countries. In Saudi Arabia, however, a similar system has already been fielded, as stated by Jan (2014). It is expected that ITS will be used in the future to determine the travel time on motorways, as it is done today by using the Bluetooth emissions of cars, as reported in Spangler et al. (2010).

Pure passive monitoring of ITS activities on highways or in urban environments is easy for any group of curious people to accomplish. A simple WLAN stick capable of receiving IEEE 802.11p emissions along with a simple DIY processor board and a small piece of software is sufficient to perform this task. The specification of the ETSI G5 protocol stack is almost completely in the public domain, and since G5 implements signatures rather than encryption, no certificates are required to exploit an ITS message. However, this is not completely uncritical: Remember that with these rather simple techniques you can monitor ambulances, fire engines, and even police cars. Even without evaluating the MAC address, recognizing these types of vehicles is far from impossible if you exploit the metadata contained in CAM and DENM: vehicle length, width, load, type, speed, acceleration, even the state of the headlights, everything is easy to exploit. Our company has already received requests from law enforcement agencies to "anonymize" at least the speed of its vehicles.

Much more critical than the pure monitoring would be the injection of phony or malicious messages in an ITS network. This could be considered the equivalent of throwing stones from a bridge onto a populated motorway. Attackers can be mere "script kiddies," using openly published malevolent application programs from the Internet. But also criminals or even terrorists could use such devastating techniques, for example, to bind or slow down law enforcement during their illegal activities.

Of course, the ETSI-defined cryptographic signature scheme should protect the network from such malicious user attacks. However, experience tells us that malicious hackers rarely enter the system through the front door. ITS developers therefore have not only to rely on cryptography, but also on sanity checks and data fusion in their software.

6 Conclusions

Intelligent Transportation Systems are currently being created and deployed worldwide in order to orchestrate the various transportation systems in a sustainable and environmentally friendly way. Reasonable operational and communication security, however, are the key elements for the user acceptance and, ultimately, for their success in the real world.

References

ETSI EN 302 665 V1.1.1. (2010-09). Intelligent transport systems (ITS); Communications architecture. *European Standard (Telecommunications series)*.

Jan, Y. (2014). *Drivers' perception of Saher traffic monitoring system in Jeddah, Saudi Arabia*. Masters theses and specialist projects paper 1438. Retrieved March 12, 2019, from http://digitalcommons.wku.edu/theses/1438

Spangler, M., Leonhardt, A., Busch, F., Carstensen, C., & Zeh, T. (2010). *Deriving travel times in road networks using Bluetooth-based vehicle re-identification: Experiences from Northern Bavaria*. Conference paper: FOVUS - Networks for Mobility. Stuttgart, Germany. Retrieved March 12, 2019, from https://www.researchgate.net/publication/266064514