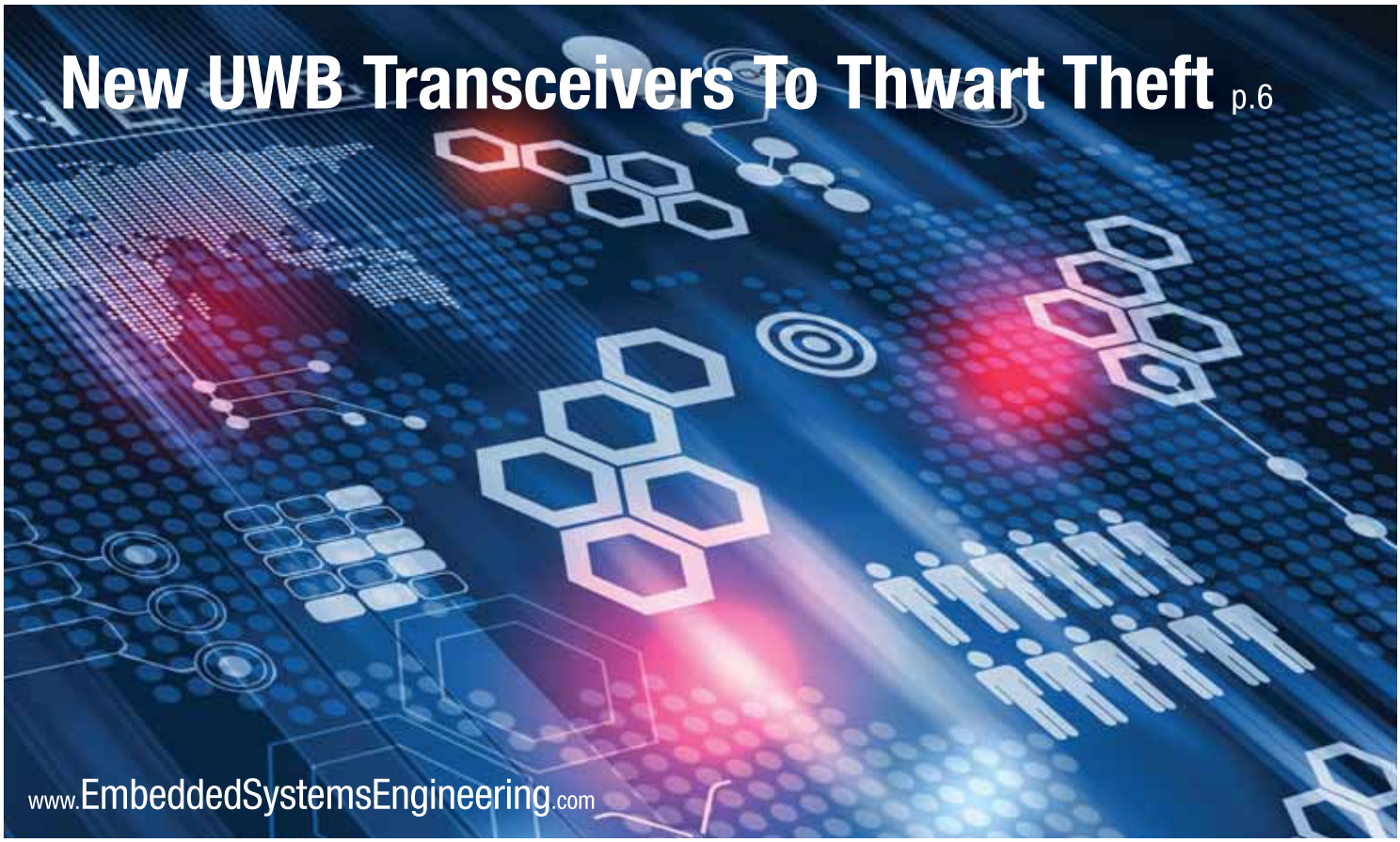
EECatalog

EMBEDDED SYSTEMS ENGINEERING

September/October 2014

Guiding Embedded Designers on Systems and Technologies



Automotive Sponsors

MICROCHIP

ublox

Embedded Linux & Android Sponsor

MontaVista

LTE/4G Sponsor

ublox

Smartphone/Tablet/Wearables Sponsor

MICROCHIP

Automotive Security: Why UWB Measures Up

When IEEE ratified 802.15.4a it opened the way to highly accurate tracking using wireless technology for the automotive and other industries. Now, with a new breed of integrated Ultra Wide Band (UWB) transceivers debuting, a disturbing criminal trend might just be stopped in its tracks.

By Mickael Viot, DecaWave

Developments in vehicle security over recent years have made it increasingly difficult for thieves to steal vehicles by conventional means. Statistics show that on a global scale the number of vehicle thefts has been steadily declining over the past 10 years. However, in developed countries the latest data shows that they are starting to rise again.

Surprisingly, the main reason is linked to… the car key.

Keyless passive entry systems to be exact.

CURRENT PASSIVE ENTRY AND START SYSTEMS…

More and more modern cars are equipped with a passive entry and start system. Introduced on high-end cars in the late 90's, this technology is democratizing and will soon equip more than 50% of cars.

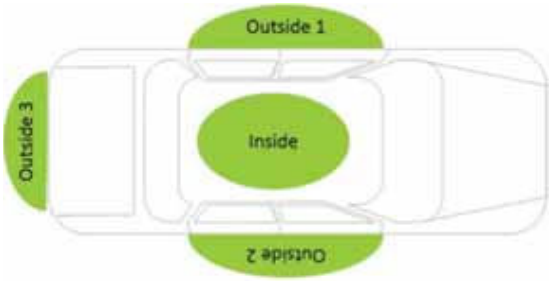


Figure 1. LF transmitter zones coverage

Figure 1 shows a car equipped with LF (125 kHz to 130 kHz) transmitters. Three to 10 transmitters cover specific zones inside and outside the car. These LF transmitters send beacons. If the key is within range, that is, within one to two meters, the "sleeping" key picks up the LF signal, which wakes the key and triggers the processing of the received message. The key then replies to the car using a separate RF channel (433 MHz to 2.4 GHz).

The message contained in the beacon varies based on each transmitter zone. For example, the message could vary based on whether the zone was inside or outside the vehicle, or, even whether the zone is on the driver's side, passenger side, or trunk. This capability allows the key to send specific answers that will trigger specific actions such as opening the passenger door or starting the engine if the key is inside the car.

AND THEIR WEAKNESSES

Despite incorporating encryption and other secure mechanisms, keyless entry systems have some serious weaknesses. Here are some ways those weaknesses can affect you, the vehicle user.

First, the RF channel can be jammed. When thieves jam the RF channel, you, like most other drivers, will clamber out of the car counting on the vehicle to lock itself. Thanks to the jamming though, your car can't receive the "lock" command.

While jamming the RF channel does not disable the passive start system and thieves will not be able to take your car, your valuables become easy pickins.

Second, more enterprising criminals can launch a relay attack, which is both more complex to execute and more lucrative.

As described in Figure 2, the relay attack consists of relaying the messages exchanged between the car and the key over long distances, up to 1000 m. Thieves begin the attack by relaying the beacon from the LF transmitter in the car to the key.

Where once these bad actors may have carried a Slim Jim, now their bag of tricks includes an antenna close to the door lock and an amplifier to convert the signal to a longer range RF signal to transmit it over long distances. A thief places himself within a few meters from the car owner with equipment that will convert the RF signal back to an LF signal and, thanks to an amplifier, will reach the LF receiver embedded in the

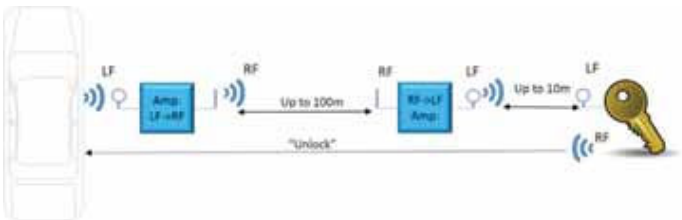


Figure 2. Passive key entry makes a car theft method known as the relay attack possible.

key. Once the key gets the beacon message, it will answer as usual with an "unlock" command. This command will be picked and relayed as described above to travel back to the car.

Now that the thieves are in the car, they don't have to settle just for stealing what's inside. They simply position the antenna close to the transmitter in charge of the "inside" zone, triggering the activation of the passive start system. Your car is gone.

REPELLING RELAY ATTACKS

Nowadays key fobs all use advanced security techniques like encryption to secure the communication between the key and the car. But if someone manages to relay the communication, all this security is useless.

One option to avoid relay attack is to measure the real physical distance between the car and the key. If the car detects that the key is not physically close, it will simply ignore the commands received.

Measuring RF signal strength is one way to obtain a distance measurement. But doing so relies on the assumption that the signal strength and distance have a deterministic relationship, according to the Friis equation. Unfortunately, the Friis equation is only applicable in free space. In an environment with multi-path, interference and lack of sight, the range estimate will have an accuracy of tens of meters.

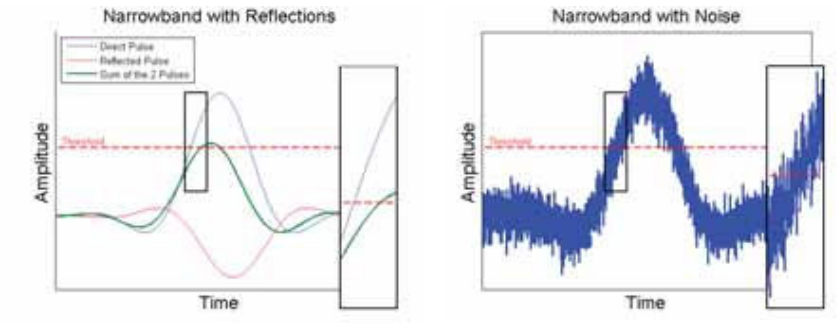


Figure 3. Narrowband signal in presence of multi-path and noise

A second technique consists of measuring the Time of Flight of the RF signal to estimate the distance between the transmitter and the receiver. There have been attempts to build time of flight systems using standard narrowband RF like Bluetooth or other 2.4 GHz signals.

The problem here is that due to the narrow bandwidth, the rising edge of the signal is slow, and it is difficult to determine the exact time of arrival in multi-path and low-signal-to-noise-ratio environments (see Figure 3), resulting in an accuracy of several meters, with reliability still very dependent on the environment.

UWB TAKES ON MEASUREMENT TO STOP PASSIVE-AGGRESSIVE BEHAVIOR

Ultra Wideband (UWB) may finally offer the performance needed for accurate and reliable distance measurement. The UWB signal consists of narrow pulses, typically no more than 2 ns wide. This makes it highly immune to multi-path and interference (see Figure 4). Being Ultra Wide Band, with a bandwidth between 500 MHz and 1.2 GHz, this technology is also much more difficult to jam.

OPERATION ONLY WITHIN A GIVEN DISTANCE FROM THE VEHICLE

UWB technology allows Line-of-Sight ranges of greater than 200 m. However, the in-vehicle unit can be configured to only take action when the measured distance is less than a certain vehicle manufacturer defined value.

Because UWB is capable of achieving 10 cm accuracy with 100% reliability, manufacturers could define very accurate zones, triggering the lock release mechanism only when the driver is within close proximity to the vehicle.

DETECTING ON WHICH SIDE OF THE VEHICLE THE FOB IS LOCATED

As we've seen earlier, the latest generation cars using traditional LF and RF technologies are capable of knowing from which side of the car the driver is approaching, triggering specific actions like opening a specific door or the trunk.

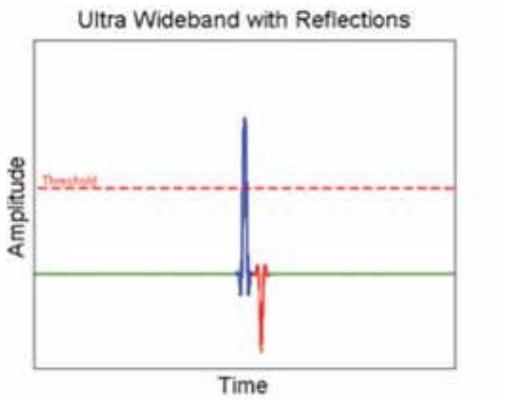


Figure 4. UWB offers high immunity to multi-path and noise.

But using UWB, how does the car know which car door or trunk to release?

A single two-way ranging exchange between one in-vehicle unit and a fob is sufficient to measure how far away the fob is from the vehicle. However, having only one piece of information—a single distance—available is not enough to determine on which side of the vehicle the fob is located.

Knowing on which side of the vehicle the fob is located takes two pieces of information. These two pieces of information could be, for example, two distances from two in-vehicle units, provided of course that these in-

vehicle units are positioned in an appropriate way. If the two units are mounted across the vehicle, then it becomes possible to uniquely identify the side of the vehicle on which the fob is located.

And if you add a third unit in the car, trilateration becomes possible, resulting in very accurate positioning of the fob in or around the car, thereby enabling the release of the locking mechanism of the trunk, the left rear door, or wherever... based on fob location.

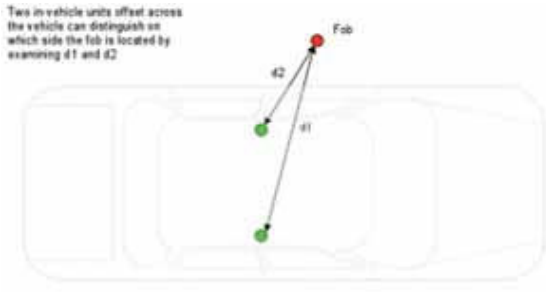


Figure 5. Making trilateration possible results in highly accurate positioning of the key fob.

FROM THEORY TO REALITY

UWB has been around for years, but until recently the implementations were bulky, power hungry, proprietary and very expensive. Not really what the automotive industry was looking for.

This was until the IEEE ratified a new standard, the 802.15.4a, now part of 802.15.4-2011. This new standard, specifically targeting highly accurate positioning, opened the door to many new potential applications:

- Asset tracking in environments including hospitals, factories or warehouses
- Tracking individuals such as fire fighters in a burning building or newborns in a maternity ward
- Indoor navigation down to the level of an object

This new potential attracted the interest of the semiconductor industry and after several years of R&D, the first integrated UWB transceivers are now reaching the market. As you can expect from integrated circuits, they are small (a few square millimeters), low power (coin cell operated) and cheap—characteristics that make them ideal for fitting in a key fob.

Car manufacturers did not take long to understand the potential of this new technology. Many are having a close look at it now... and some pioneers have already decided to integrate it in the generation of vehicles that will reach the market in 2016.

THEFT DETERRENCE AND MORE

UWB technology is solving one of the current important issues for car manufacturers thanks to its capability to accurately measure the physical location of the key fob, thus ensuring a high level of security to their passive entry systems.

Figure 6. DecaWave UWB transceiver.

But could it offer more to the automotive industry?

After years working on the security of car passengers, car manufacturers are now investigating ways to make the car safer in an environment that includes pedestrians or cyclists. The current radars that equip cars are capable of detecting large objects but do not "see" smaller ones like humans. Fully autonomous cars are getting pretty close to it but their cost and complexity will keep them out of reach to most of the population for one or two decades.

If cyclists and pedestrians were equipped with a UWB tag, cars could detect them in advance—remember UWB can reach more than 200 m—and avoid a collision.

And car manufacturers have many similar scenarios in mind!

Mickael Viot is the Marketing Manager at Decawave, a pioneer company in the field of UWB chips. In this role, he is responsible for defining the product and business strategies related to indoor location and Wireless Sensor Networks.