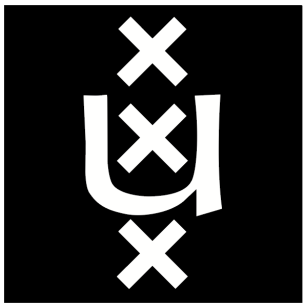
Universiteit van Amsterdam

Research Project I

Protecting against relay attacks forging increased distance reports



Xavier Torrent Gorjón
Xavier.TorrentGorjon@os3.nl

Supervisors:

Jordi van den Breekel
vandenBreekel.Jordi@kpmg.nl

Paul van Iterson
vanIterson.Paul@kpmg.nl

February 8, 2015

Abstract

For a long time, distance-bounding protocols have been an extensive research topic due to their usefulness as a security feature for systems that assume a specific proximity between parties, such as Passive Keyless Entry Systems (PKES) for cars. However, we did not find in the current literature any attempts to use these protocols to prevent relay attacks forging increased distance reports.

This project first proposes a variety of scenarios, in which the involved devices use distance-bounding protocols to perform distance checks between themselves. Relay attacks that attempt to fake increased distance reports between these devices will be studied, and a discussion of the motivation these attacks might have, as well as their consequences, will be provided.

Afterwards, available systems that could be used instead of distance bounding protocols will be reviewed. In particular, the analysis will focus on Global Positioning System (GPS), Inertial Navigation System (INS) and Radio Detecting and Ranging (RADAR) systems. This study will aim to justify developing solutions based on the current distance-bounding protocols, providing an insight on the limitations of these other systems for these purposes.

Various low-cost, easy-to-implement enhancements on the distance-bounding protocols will be proposed, which diminish the success chances of these relay attacks against systems using these protocols.

Keywords — Relay attack, distance-bounding protocol

Glossary

ACS Access Control System: Systems that use authentication mechanisms to validate the access to resources.

GPS Global Positioning System: Navigation system based on satellite communication maintained by the United States government.

INS Inertial Navigation System: Navigation system that keeps track of the route used by an object to have awareness of its location.

LIDAR Light Detection and Ranging: Object-detection system based on laser.

MANET Mobile Ad-Hoc Network: A network of independent devices deployed for a specific purpose.

PKES Passive Keyless Entry Systems: A type of access control, usually used in cars, that features the possibility of automatically opening doors without need of interaction from the user.

RADAR Radio Detection and Ranging: Object-detection system based on radio waves.

RCS Radar Cross Section: Signature of an object on a RADAR system.

ToF Time-of-Flight: Measurement on the time required to receive a signal response from another party after a signal is sent.

Contents

1 Introduction

Communications between machines face many challenges when the transmitted information needs to be protected. Most communications can prove to be valuable attack points for third parties that want to recover, modify, block or otherwise manipulate the original message for personal profit. Part of these attacks can be prevented by using end-to-end encryption and signature of the data. However, relay attacks cannot be prevented just by using cryptographic algorithms.

Relay attacks consist of the mere reception and replay of information. Although at first this might seem harmless, many systems become vulnerable if that relaying of information is not noticed. One scenario that can be used as an example of the threat these attacks represent are Access Control Systems (ACS), in which a device is used to prove that a user is within a certain distance from a validator through a challenge-response protocol. On unprotected implementations of these access control systems, an attacker can relay the challenge from the validator to a valid user who is not in range and relay its answer back to the validator, effectively bypassing distance validation. Practical attacks on this kind of systems have been demonstrated in various studies [6, 7, 11, 17].

This paper, however, will study attacks that are not related to proximity-checking systems. Distance-bounding protocols are already an effective solution for ACS and other systems that validate the proximity of a user before performing operations, and are only limited by the specifications of the systems that need to implement such protocols. Nonetheless, we did not find, in the current literature, attempts to use distance-bounding protocols to prevent forged increased distance reports, although this was an acknowledged issue on the distance-bounding studies. We intend to show that these attacks can be a menace, and propose solutions to prevent them.

This document is structured as follows: in Section 2 we review the literature used in this project. Section 3 presents a detailed explanation on the research questions this project aims to answer. Following in Section 4, an explanation of the methodology used in this study is provided. Section 5 discusses the actual results from our initial investigation, including an explanation on how distance-bounding protocols work and a study of alternative systems that could be used as countermeasures to the discussed relay attacks. Various scenarios in which relay attacks forging increased distance reports could be used are presented in Section 6. Multiple solutions based on the current distance-bounding protocols will be proposed in Section 7, analysing the level of protection they provide, as well as the feasibility and cost of using them. Conclusions are gathered in Section 8, which includes a review and a discussion of the obtained results.

2 Related Work

There is much literature available presenting solutions to distance bounding problems [1, 19, 22]. All of these studies are part of a constant iteration to improve the protocols. As new attacks emerge against distance bounding protocols, new studies are published to fix the deficiencies of the previous work. This project will use these previously mentioned studies as a basis for the solutions against the studied relay attacks. Even the older documents still prove to be useful, as they can be used as an introduction to the topic and to understand how this field has evolved.

There are also many practical studies in the field of distance bounding, which aim to test the vulnerabilities on real applications [2, 6, 7, 11, 17]. Although all these refer to forging decreased distance reports and they are not directly used in our research, they have been useful as a starting point.

This project will assume certain conditions for the studied attacks. Certain assumptions and justifications will be required on the investigation, based on the characteristics of GPS signals. Many studies focus on the feasibility of intentional attacks against GPS systems [14, 23, 24]. These studies conclude that, even though spoofing is hard with the countermeasures they propose, it is not impossible. With this premise, the goal will be to develop countermeasures against relay attacks without relying on GPS signals.

In a similar way to GPS signals, other systems such as RADAR detection [3] and Inertial Navigation Systems (INS) [12] could arguably be used to prevent relay attacks. Using these information sources [3, 12], we explain why neither of these systems are reliable, reaffirming the need of a modified distance bounding protocol that is not vulnerable to relay attacks.

Finally, this study is closely related to the field of MANETs (Mobile Ad-hoc NETworks), and as such, literature available on this topic is of our interest. In particular, wormhole attacks [10, 13, 16] are a specific type of relay attack that, while being different than the ones we will study in this document, provide valuable insight to our investigation.

3 Research Questions

As seen in Section 2, in the current literature we did not find proposals to fight the subset of relay attacks that attempt to fake increased distance reports between legitimate parties. This project will first study the difficulty of performing these attacks. Therefore, our first research question will be:

Feasibility of forged increased distance report relay attacks

We first present a detailed description of various distance-bounding protocols using different kinds of approaches to check distances between parties, explaining how they work and their limitations.

Following the protocol discussion, we explore a number of real world scenarios that could use these protocols. A number of theoretical attacks on these systems will be proposed, discussing their feasibility and consequences on the studied systems. This analysis is necessary, as the first goal of this project is to prove that these attacks can be dangerous, given the right circumstances. The proposed scenarios are diverse, both in context and properties of the systems involved, implying that the possible solutions for one case might not suit others, especially when considering hardware limitations and economic costs.

After the discussion on the study cases, an evaluation of other systems that could be used to prevent those attacks will follow. This evaluation will include GPS location, INS, as well as RADAR detection. The investigation on GPS and INS systems will focus on their usability as positioning systems, while the study of RADAR will evaluate its usefulness when attempting to physically detect attackers.

If the results from this research determine that these attacks can pose a threat and that the alternative systems are not enough to prevent them, we will consider a second research question:

Preventing relay attacks forging increased distance reports

This second research question will focus on providing solutions to the issues stated on the first. Original distance-bounding protocols used to perform upper-bound distance checking can rely on the speed of light to completely prevent relay attacks faking closer distances between parties. Attacks forging increased distance reports, however, are performed by delaying the original signal, which means that the physical limitation of the speed of light cannot be used to prevent them. From this initial consideration we expect that it will not be possible to provide a solution that completely blocks these attacks. Nevertheless, it may be possible to find countermeasures that greatly reduce the chances of successfully performing these attacks.

4 Methodology

This project will be a theoretical research on the current distance-bounding protocols, and their inability to detect increased distance reports. We intend to expose the limitations of these protocols on specific real world scenarios, and ultimately offer solutions to them.

First, we provide a review of the available literature about distance-bounding protocols, in order to determine which of them is best suited for our research. A discussion of alternative systems that could be used to prevent these attacks will be provided as well.

Following the distance-bounding protocols description, this document will propose systems that could be vulnerable to these attacks, reviewing the difficulty of these attacks and the consequences these attacks might have. In particular, the focus will be on autonomous cars and drones. These scenarios will be the basis for our research.

At the last part of the paper, variations of the distance-bounding protocols will be proposed, aiming to effectively reduce the threat these attacks pose. We discuss the increase in security these solutions achieve, as well as evaluating the feasibility of implementing them on our study cases.

5 Distance-bounding protocols and alternative systems

In this section, we discuss distance-bounding protocols, as well as GPS and INS location systems and RADAR detection. All of them are relevant topics to our research. First, an explanation on the current distance bounding protocols will be provided, as they are used as a starting point for our research. Afterwards, GPS and INS systems will be evaluated, explaining why the studied systems should not rely completely on them, hence the need to develop more powerful distance-bounding protocols. Lastly, we discuss the possibility of using RADAR detection to fight the proposed attacks.

5.1 Distance-bounding protocols

Distance-bounding protocols were developed as a countermeasure to relay attacks that attempt to fool systems that validate the proximity of a user to a validation point. Common scenarios of these applications are found in ACS, such as smartcards to access buildings or cars using PKES.

These distance-bounding protocols try to use properties of the systems involved in the communications (such as signal intensity or message Time-of-Flight (ToF)) to validate the proximity of users. Based on the previous studies available [4], the available methods to perform distance checks are:

Signal Intensity Signal intensity protocols try to achieve proper distance checking of other nodes by measuring the received signal strength. Previous work available in the public literature [20] proves the usefulness of this location system. Even though attacks on these systems are hard to perform [21], the majority of defences against them rely only on anomaly detection. ToF methods discussed next provide a higher degree of security when comparing both systems working alone, but signal intensity checking can still be used as an additional security feature in combination with the other methods.

Ultrasound ToF Ultrasound ToF uses the round-trip time of messages sent and received from the parties calculating the distance between them. This does not depend on the signal strength for the measurement, although ultrasound-based ToF has the latent vulnerability that other platforms, such as radio communication or optical wires, can surpass the speed of the ultrasound communication, effectively being able to relay information faster than the legitimate infrastructure [4].

Radio ToF Radio-based ToF uses the same idea as ultrasound ToF to perform the distance checking. The key of the success of this method is that the information transmitted travels at speeds close to the speed of light, meaning that it is physically impossible to fake that one node is closer than it really is. Practical studies on this method [19] developed hardware that can perform the operations required under $1ns$. Therefore, the maximum theoretical distance an attacker can shorten its reported distance is under $15cm$, as that is the distance light travels in that amount of time.

In this project we use Radio ToF distance-bounding as a basis for our work, as it is proven to be the most secure and reliable method. In particular, the implementation that will be assumed to be used, will be the one described in [19], as it is the most recent and secure protocol. This distance-bounding protocol is based purely on analog signals, avoiding the time required to convert analog signals into digital signals. A graphical diagram of the communication channels can be found in Figure 1 and, following next, there is a description of the inner workings of the system:

1. First, both validator V and prover P exchange a nonce N. This can be done on-the-fly through a secure channel or before the system starts.
2. When it is necessary to verify the current distance of the two parties, V starts sending challenging bits C_n to P.
3. For every bit C_i received, P sends back a response in the form of $C_i + N_i$. The answer is done by sending the bit C_i through one of the two communication channels for the challenge answers, while the bit N_i is encoded implicitly in the form of which answer channel was selected. For example, if the current nonce bit N_i is 0, the C_i answer would be sent using the first channel, whereas if its value of N_i was 1, the second channel would be used.
4. Step 3 is repeated n times. The chances of an attacker faking one of the response transmissions is $\frac{1}{2}$, but after n times of repeating this operation, the possibility of an attacker faking the whole procedure goes down to $\frac{1}{2^n}$.
5. Finally, V can calculate the mean value of all the received challenge-response ToFs, effectively obtaining the distance between him and P.

However, although this protocol alone can prevent relay attacks attempting to forge decreased distances between the legitimate parties, it is not enough to fight attacks that forge an increase on the real distance [4], and this will be the main focus of our research.

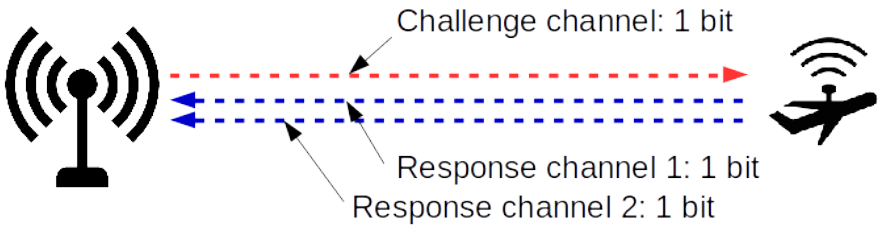


Figure 1: Channels in the distance-bounding Protocol proposed by Rasmussen and Capkun [19].

5.2 GPS location

It could be argued that GPS location could be used to prevent the attacks that we will discuss on the next section. However, GPS signals have their own weaknesses both with and without presence of adversaries.

In settings without adversaries, GPS positioning cannot be reliably used indoors or underground, and sometimes the presence of tall buildings or structures nearby is enough to disrupt its data.

Considering scenarios with one or multiple adversaries, even though there are many countermeasures to prevent attacks against GPS positioning [14, 23, 24], they do not provide complete security, similar to the signal intensity ranging protocol.

Due to these problems, the U.S. government actually recommends to always have backup systems for GPS and suggests to not rely on it entirely[1]. Based on these premises we will assume that GPS is not a part of our system, or that we cannot rely on it.

5.3 Inertial Navigation System

Inertial Navigation Systems are devices used to provide machines a sense of self-awareness of their current position, based on their initial position and the chosen routes, by using accelerometers and gyroscopes. These systems could be relevant for this research, as they share the same positioning approach, staying independent from third party sensors.

However, INS hardware cannot realistically provide an accuracy below $5m$ of error after 60 seconds of operation [25]. In an environment with multiple nodes using this system, this means that after 60 seconds, the location detection between two nodes could be as biased as $10m$. This also limits its usability

[1] `http://www.gps.gov/support/faq/#jamming`

as a stand-alone positioning system, as the error will only grow larger as time progresses.

Although INS accuracy is improving over the years, at the moment it is not a viable solution to prevent relay attacks.

5.4 RADAR detection

One way to protect against this kind of relay attacks could be by attempting to physically detect the attacker that is performing the relaying of messages. If an unidentified object is detected between the parties and it is confirmed that it does not belong to the system, security measures could be taken to prevent such relay attacks.

However, Radar Cross Section[2] (RCS), a measurement used to rate the ability to reflect radio waves by an object, can be heavily decreased by employing proper techniques [3], such as the usage of special materials, radiowave-absorbing paint and specific shapes that minimize and disperse radio reflection.

As a real world example, the first operational aircraft designed to employ advanced stealth technology, the Lockheed F-117 Nighthawk from the United States Air Force, with a wingspan and a length of $13.20m$ and $20m$ respectively[3], has a RCS signature of $0.025m^2$, which is similar to that of a bird [3].

In the attack scenarios proposed in Section 6, flying drones would be the most versatile device to perform the attacks. Considering these drones can be considerably smaller than these aircraft (depending on the situation, the used drone could be shorter than $1m$ in length, height and width), it is easy to foresee that they would be almost invisible to radar systems. If the attack scenario does not require the attacker to fly at relative high speeds, its RCS signature could be further decreased by designing an attack drone with a shape specifically made to absorb radar waves.

We therefore conclude that, in the current state of stealth and anti-stealth technologies, RADAR detection would not be a strong countermeasure to prevent against malicious devices attempting to perform relay attacks.

[2] http://www.microwaves101.com/encyclopedia/Navyhandbook/4.11RadarCross-Section(RCS).pdf

[3] http://www.fighter-planes.com/info/f117_nighthawk.htm

6 Feasibility of forged increased distance report relay attacks

The theoretical attack we propose relies on the fact that the discussed protocols regarding distance bounding on the available literature do not prevent relay attacks that report an increased distance between two legitimate parties.

The basics of the attack are easy to understand. Assume two parties are communicating using a transmitter-receiver model, that is, one of them is actively reporting its position to the other, using the distance-bounding protocol [19]. At a specific moment in time, an attacker seizes a position between them and starts disrupting the communication between them, either by attempting to block the communication or by jamming its frequency range. At the same time, he starts recording the information and resending it to the receiver node, adding a brief delay on it. Figure 2 provides a graphical description of the problem. The effectiveness of this attack can be increased by having multiple malicious nodes attempting to block the original signal.

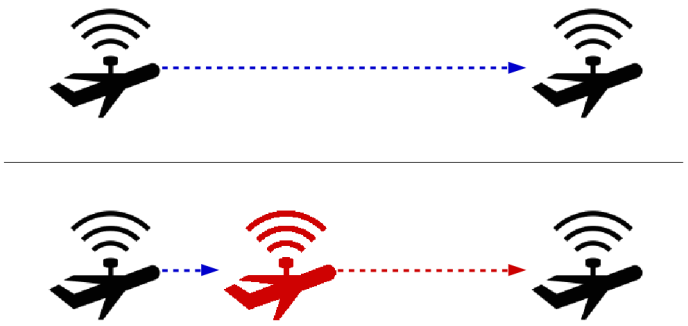


Figure 2: Regular communication versus block and relay attack.

Many systems use these distance reporting protocols for their pathing decisions. This kind of attack could cause unexpected behaviour on the systems, effectively altering their original desired outcome.

Such attacks are difficult to perform in practice, as they require relaying and jamming communications at the same time. Appropriate timing on the relay and a certain degree of knowledge about the system are also required to successfully perform an attack. However, this could be done in theory.

Following, we will discuss a number of real world applications that may be interesting for this research.

6.1 First example of real world attack: Autonomous cars

Autonomous driving is a topic that is receiving a lot of attention by many researchers around the globe in recent years. The variety and quantity of studies on this field [5, 8, 9, 15], prove its relevance as an interesting subject from the point of view of computer vision and location systems.

These autonomous cars use multiple systems to check and validate their position and the layout of the surrounding area. Usually these systems include a subset of GPS location, lasers, radars and computer vision systems [5, 15].

Distance-bounding protocols do not seem to be an active part of these systems, although they could be useful. First of all, the most obvious utility would be to provide an extra security layer to the system, providing additional means to locate other vehicles in normal conditions, or as a backup system in case other devices fail. Secondly, this feature could be used as well to detect pedestrians, if devices such as mobile phones were adapted for this purpose.

Autonomously driving vehicles could also use distance-bounding protocols to perform distance verification of specific targets. The distance-bounding protocols developed in [4, 19] can be used to check the distance with specific targets. This distance checking interesting in this environment as, in a high traffic road, it is difficult to keep track of other specific vehicles through the use of laser location or computer vision system. This functionality could be used, for example, to have a car follow another without knowing the route beforehand.

Although the introduction of these distance bounding protocols on autonomous cars could prove to be useful for these purposes, it would also add a vulnerability in the form of the previously mentioned reported distance increase relay attacks if they are not addressed.

6.2 Second example of real world attack: Drone MANETs

In the recent years there has been a huge increase on the interest towards drones[4], due the emergence of topics such as Amazon Prime delivery drones (Figure 3) or the usage of unmanned aircraft by the US military.

It is safe to foresee that the usage of drones will only grow on the upcoming years due to their ability to decrease costs and improve the performance of systems currently manned by humans. We present two scenarios on which the use of drones can be interesting and how can they be affected by the discussed relay attacks.

[4] `http://www.google.com/trends/explore#q=drone`

Figure 3: Amazon Prime delivery drone carrying a package.

Cooperative working drones Taking as an example the Amazon Prime delivery drones, we can discuss the possibility of having multiple drones working in groups. One interesting scenario is the case of multiple drones carrying a larger package. For a company trying to keep expenses low, it would be sensible to use multiple drones that can work cooperatively in different situations rather than having drones of various sizes for each type of package. In this situation, an attacker could try to attack that system by faking the distance reports from one drone to the others, which may force the drones to change positions and lose equilibrium, eventually crashing.

A relay attack on this platform would be preferred, rather than just attempting to shoot down the drones to achieve the same goal, as it would be extremely difficult to prove that a relay attack took place by checking the logs of the crashed drones. This could lead to a reputation loss for the delivery company, as their system would be seen as unreliable by the customers. Even though this kind of delivery platform has not been deployed yet due to legal constraints, it may start to be available at some point in 2015[5].

Area surveillance drones Another common use of drones is to use MANETs to perform area surveillance. This case has both civilian and military applications. Civilian use cases range from searching missing people to area mapping, while military uses usually imply area reconnaissance, searching for possible threats or targets.

In this particular situation where a group of drones is checking a zone, an attacker could attempt to interfere in the reported distances. This could cause the drones to believe they are farther apart between themselves than

[5] `http://abcnews.go.com/Technology/amazon-prime-air-delivery-drones-arrive-early-2015/story?id=21064960`

what they really are. Under these circumstances, they could decide to get closer together so they do not leave zones unchecked between them, which would inevitably cause a reduction on the covered area. Figure 4 represents an example of this attack.

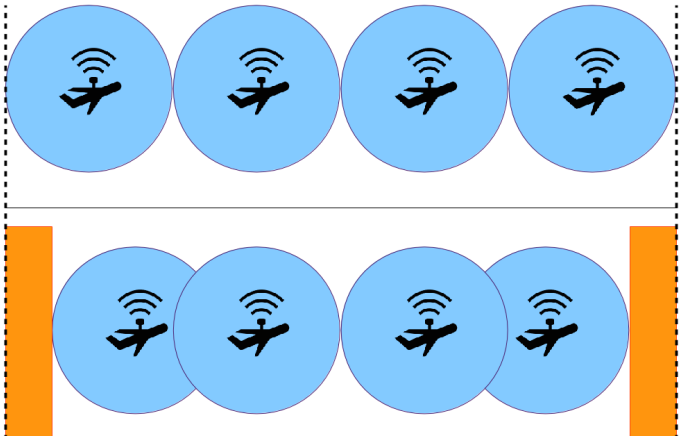


Figure 4: Example of the proposed attack. On the first case, the four drones manage to explore all the expected area (marked with trailing dots). On the second, the marked zones on the sides represent the resulting unchecked area as a consequence of this attack.

This attack might prove considerably difficult to perform, but can have catastrophic consequences if successful. Unlike the attack on cooperative drones, distance is less of a restriction here, but in this case the attack requires a much deeper knowledge of the attacked system.

7 Preventing relay attacks forging increased distance reports

In this section, countermeasures to the studied relay attacks are proposed. These solutions can stack with one another and, in fact, it is recommended to do so, as each one of them provides an additional layer of security.

These solutions do not need new protocols or hardware, and instead rely on information replication and addition of redundancy to provide protection against the fake increased distance reports. This means that the systems discussed on Section 6 could implement these with minimal modifications.

7.1 Introducing behaviour verification

Nowadays storage is hardly a limitation for systems, as the price, size and weight of these components have decreased to the point where multiple gigabytes of information can be stored in inexpensive memories that can have a size of a few millimeters.

Therefore, storing information on the device about the recent location of one or multiple parties is feasible. Uncoordinated attacks would be prevented with this feature, although it does little to protect against carefully planned ones. All location systems must allow a certain degree of variation on the measurements, as there may be many reasons for a slight delay in a communication. By successfully using that error margin, an attacker could still attempt to fake distance reports increasingly over a period of time.

A major limitation of this countermeasure is that it requires that the devices involved maintain the distance-bounding protocol active. Specific systems could use the distance-bounding protocol intermittently to save energy or because the requirements of the platform are fulfilled without a constant distance checking. In such environments, an attacker could wait until a distance-check ends and start the attack as soon as the next one begins. If the pause between distance checks was large enough, the system could not distinguish a node that legitimately moved away from a relay attack reporting this increase in distance.

7.2 Utilize multiple distance-bounding signals

Historically, distance-bounding protocols are used to validate an upper-bound distance between a prover and a validating station. As such, the exact location of a prover is not required, only its distance to the validating station matters (that is, check if the prover is within a certain radius of the prover in a 2D scenario, or a sphere in a 3D scenario).

If the nodes using distance-bounding protocols are large enough, multiple distance-bounding antennas can be used so that not only the distance from another node is known, but also its approximate location on the 3D space.

By using this triangulation system, attackers need to temper the communication between several antennas at the same time. Coupled with the behaviour verification solution, it becomes easier to detect relay attacks. For an attacker it is still easy to produce fake distance reporting positions on the same vector of the legitimate prover, but it becomes increasingly difficult to fake positions that diverge from that line.

Figure 5 provides a graphical explanation of this defence mechanism. An attacker cannot make the left drone believe that the legitimate drone is inside the circle area, due the original distance-bounding protocol features. With this method an attacker can still fake a position in the darker area with relative ease, but faking a position outside from it becomes increasingly difficult as multiple distance reports have to be taken into account, and a deviation on any of them could end with the checking drone detecting inconsistency in the received data.

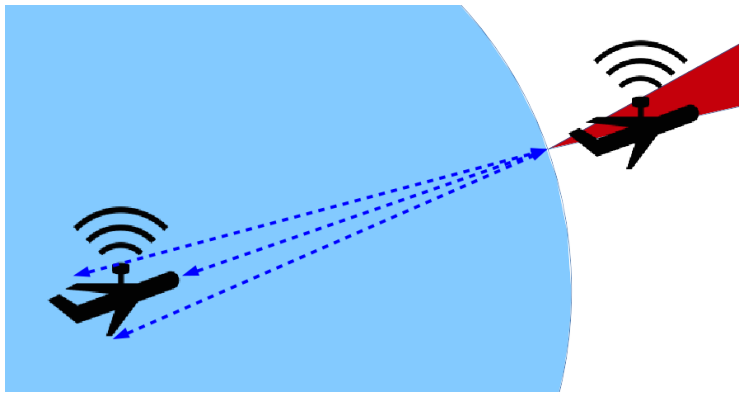


Figure 5: Scenario after the proposed countermeasure.

This protection method has two major downsides. The first is that devices should carry more antennas, increasing their cost and weight. Additionally, the device using this system needs to have a minimum size for it to be reliable, as the antennas need to be at a certain distance from one another to perform a correct triangulation (otherwise the error margins would outweigh the correctness of the obtained distance values).

7.3 Avoid centralized systems: distributed knowledge

When the first attack definition was proposed in Figure 2, only one of the nodes was reporting its location to the other. Although this configuration may simplify the operation and decision-making of these nodes (by having only one node in the system taking decisions for the others), it also makes the system more vulnerable to relay attacks.

If all nodes on the system can share information of the position of neighbour nodes between themselves, an attack on the system becomes considerably more difficult to perform. It is not required that one node checks the distance between him and another one with all the other nodes on the system, although every additional node verifying the information makes it harder to perform an attack on the system.

Figure 6 shows a graphic description of what this triangulation achieves. An attacker would need to disrupt and replay many reports at the same time, which could be extremely difficult in an environment where the devices are moving in an unpredictable way.

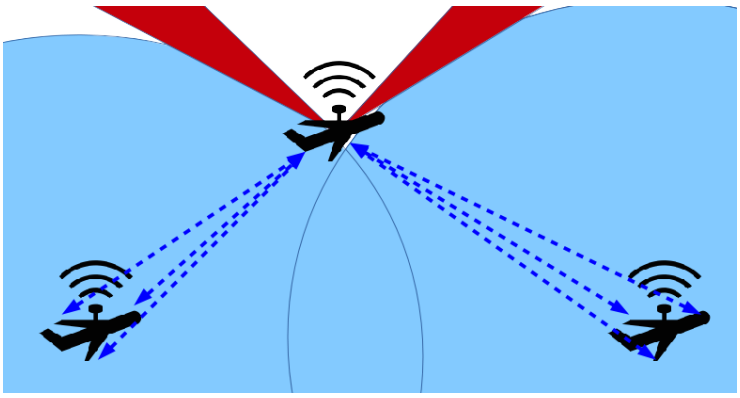


Figure 6: Using the information of multiple drones to check distances hinders the task of a possible attacker, as multiple signals have to be relayed properly.

Besides the added load in the communication this countermeasure produces, a major restriction is to properly handle the location reports other devices sent, as the communication between drones is not instantaneous. A node N_0 attempting to validate the distance of a node N_1 should perform the following steps:

1. N_0 starts the distance-bounding protocol with N_1.
2. N_0 requests other nodes M_n their information on the location of N_1 through an encrypted channel. We note the ToF of these requests as

T_{1n}. We assume N_0 knows the location of the other M_n nodes, or that it also performs the distance-bounding protocol with them.

3. The nodes M_n answer the request from N_0. This answer should include the current location of N_1, as well as its current speed and the vector of its current direction. M_n nodes can be aware of the speed and direction of N_1, if the system is using the behaviour verification proposed before in this Section. There will be a certain delay before the nodes M_n can answer, as they have to decrypt the received message and process the answer, and then encrypt the answer again before it is sent. All this time T_{2n} is not negligible in this high-accuracy environment, and they should measure it and sent it along with their answers. We note the ToF of the response of these messages as T_{3n}.

4. N_0 receives the n answers. Then, for each answer n, it can calculate the approximate position N_1 had $\frac{T_{1n}+T_{3n}}{2} + T_{2n}$ seconds ago according to each node M_n, and using the location of each one of them, it can triangulate the data to obtain the position of N_1 relative to its own. Using the information about its speed and direction, it can also obtain an approximation of its current location. Then, it can compare that information to the obtained by using the distance-bounding protocol on Step 1, and determine if all the data is correct.

8 Conclusions

From the results in Section 6 we can conclude that, even though the explored scenarios are only a subject of investigation right now, and have no commercial use at the moment of writing this document, both autonomous cars and drones will surely be amongst the most important developments in the upcoming years. This makes the vulnerabilities on distance-bounding protocols a latent problem.

All the proposed study cases have vulnerabilities that attackers could attempt to exploit for different purposes, ranging from attacks that attempt to change the expected outcome without the system noticing, as in the drones performing area surveillance study case, to outright make part of the devices involved crash with others, as discussed with the autonomous cars and drone delivery study cases.

As systems like the drone delivery and automated cars are not yet available to the open public, is it difficult to foresee what systems and protocols these platforms will use. However, in this document the usefulness of including distance-bounding protocols on them has been explained, focusing on the consequences distance-amplification attacks might have on them.

Multiple solutions to these distance-amplification attacks have been proposed and discussed. Even though upper-distance bound cannot be solved as lower-distance bound by using limitations on the information travelling speed, the proposed solutions noticeably decrease the chances of a malicious party successfully attacking the protocol.

9 Future Work

There are a number of interesting proposals to continue the work performed in this project.

First, a proof of concept of the discussed attacks would be useful to evaluate the costs and requirements of performing them. As both autonomous cars and drone delivery services are systems that are currently still under development, such proof of concept could be used to prove that those systems do need the additional countermeasures proposed in this document.

A second interesting future research would be to investigate the possibility of using channel hopping [18] as a countermeasure for the discussed attacks, having distance-bounding protocols use multiple channels and not only the three that have been discussed.

Acknowledgements

We would like to thank Jordi van den Breekel and Paul van Iterson, supervisors of this project at KPMG, for their support over the course of this project. In a similar way, we would also like to thank Jaap van Ginkel and Arno Bakker, staff at the System and Network Engineering MSc, for their insight and guidance.

References

[1] Stefan Brands and David Chaum. "Distance-bounding protocols". In: *Advances in CryptologyEUROCRYPT93*. Springer. 1994, pp. 344–359.

[2] Jordi van den Breekel. *A Security Evaluation and Proof-of-Concept Relay Attack on Dutch EMV Contactless Transactions*. 2014.

[3] Serdar Cadirci. *Rf stealth (or low observable) and counter-rf stealth technologies: Implications of counter-rf stealth solutions for turkish air force*. Tech. rep. DTIC Document, 2009.

[4] Srdjan Capkun and Jean-Pierre Hubaux. "Secure positioning in wireless networks". In: *IEEE Journal on Selected Areas in Communications* 24.2 (2006), pp. 221–232.

[5] AG Continental. *Autonomous Driving in Urban Environments: Boss and the Urban Challenge*. 2008.

[6] Aurélien Francillon et al. "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars." In: *NDSS*. 2011.

[7] Lishoy Francis et al. "Practical NFC peer-to-peer relay attack using mobile phones". In: *Radio Frequency Identification: Security and Privacy Issues*. Springer, 2010, pp. 35–49.

[8] U Franke et al. "Autonomous Driving approaches Downtown". In: *IEEE Intelligent Systems* 13.6 (1999).

[9] Andreas Geiger, Philip Lenz, and Raquel Urtasun. "Are we ready for autonomous driving? The KITTI vision benchmark suite". In: *Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on*. IEEE. 2012, pp. 3354–3361.

[10] Priyanka Goyal, Sahil Batra, and Ajit Singh. *A literature review of security attack in mobile ad-hoc networks*.

[11] Gerhard P Hancke. "A practical relay attack on ISO 14443 proximity cards". In: *Technical report, University of Cambridge Computer Laboratory* (2005), pp. 1–13.

[12] Eddy Hose. "Inertial navigation system". Pat. 4085440. 1978. URL: `http://www.freepatentsonline.com/4085440.html`.

[13] Yih-Chun Hu, Adrian Perrig, and David B Johnson. "Wormhole attacks in wireless networks". In: *Selected Areas in Communications, IEEE Journal on* 24.2 (2006), pp. 370–380.

[14] Ali Jafarnia-Jahromi et al. "GPS vulnerability to spoofing threats and a review of antispoofing techniques". In: *International Journal of Navigation and Observation* 2012 (2012).

[15] Jesse Levinson et al. *Towards Fully Autonomous Driving: Systems and Algorithms*. 2011.

[16] Ritesh Maheshwari, Jie Gao, and Samir R Das. "Detecting wormhole attacks in wireless networks using connectivity information". In: *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE. 2007, pp. 107–115.

[17] Konstantinos Markantonakis. "Practical relay attack on contactless transactions by using nfc mobile phones". In: *Radio Frequency Identification System Security: RFIDsec* 12 (2012), p. 21.

[18] Vishnu Navda et al. "Using channel hopping to increase 802.11 resilience to jamming attacks". In: *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE. 2007, pp. 2526–2530.

[19] Kasper Bonne Rasmussen and Srdjan Capkun. "Realization of RF Distance Bounding." In: *USENIX Security Symposium*. 2010, pp. 389–402.

[20] Vinay Seshadri, Gergely V Zaruba, and Manfred Huber. "A bayesian sampling approach to in-door localization of wireless devices using received signal strength indication". In: *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*. IEEE. 2005, pp. 75–84.

[21] Yong Sheng et al. "Detecting 802.11 MAC layer spoofing using received signal strength". In: *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE. 2008.

[22] Yu-Ju Tu and Selwyn Piramuthu. "RFID distance bounding protocols". In: *First International EURASIP Workshop on RFID Technology*. 2007, pp. 67–68.

[23] Jon S Warner and Roger G Johnston. "GPS spoofing countermeasures". In: *Homeland Security Journal* (2003).

[24] Hengqing Wen et al. "Countermeasures for GPS signal spoofing". In: *ION GNSS*. 2005, pp. 13–16.

[25] Oliver J Woodman. "An introduction to inertial navigation". In: *University of Cambridge, Computer Laboratory, Tech. Rep. UCAMCL-TR-696* 14 (2007), p. 15.