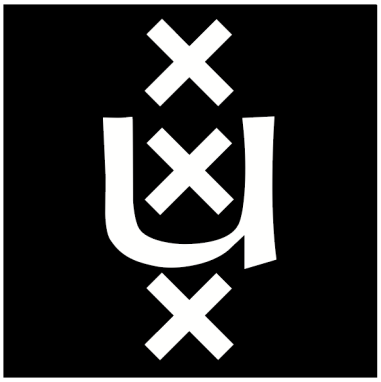
Universiteit van Amsterdam

Research Project I

Protecting against relay attacks forging increased distance reports



Xavier Torrent Gorjón
Xavier.TorrentGorjon@os3.nl

February 6, 2015

Abstract

For a long time, distance-bounding protocols have been an extensive research topic due 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 information on the current literature any attempts to use these protocols to prevent relay attacks forging increased distance reports.

This project first proposes some 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), Radio Detecting and Ranging (RADAR) and Light Detection and Ranging (LIDAR) 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.

Some low-cost, easy-to-implement enhancements on the distance-bounding protocols will be proposed, which greatly 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 **4**

2 Related Work **4**

3 Research Questions **5**

4 Methodology **6**

5 Results **7**
5.1 How feasible are forged increased distance report relay attacks? . 7
5.1.1 First example of real world attack: Autonomous cars . . . 8
5.1.2 Second example of real world attack: Drone MANETs . . 8
5.2 How can forged increased distance report relay attacks be prevented? 10
5.2.1 Introducing behaviour verification 10
5.2.2 Utilize multiple distance-bounding signals 11
5.2.3 Avoid centralized systems: distributed knowledge 12

6 Conclusions **12**

7 Acknowledgements **12**

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 an 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 **??** discusses the actual results from our initial investigation, which includes a proposal of various scenarios in which relay attacks forging increased distance reports could be used and an evaluation on alternative systems that could be used to prevent these attacks. Some solutions based on the current distance-bounding protocols will be proposed on Section **??**, analysing the level of protection they provide, as well as the feasibility and cost of using them. Conclusions are gathered in Section 6, 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, 18]. All of these studies are part of a constant iteration to improve the protocols. As new attacks emerge against distance bounding pro-

tocols, 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 [6, 7, 11, 17, 2]. Although all these refer to forging decreased distance reports and it is not directly used in our research, they have been useful as a starting point.

This project will assume certain conditions for the studied attacks. Some 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 [20, 21, 14]. These studies conclude that, even though spoofing is hard with the solutions 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 (INR) [12] could arguably be used to prevent relay attacks. Using these information sources [3, 12], we explain why these systems are not reliable either, 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 [13, 16, 10] 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 do their work and their limitations.

Following the protocol discussion, we explore some real world scenarios that could use these protocols. Some 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 and LIDAR. The investigation on GPS and INS systems will focus on their usability as positioning systems, while the study of RADAR and LIDAR will evaluate their 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 no enough to prevent them, we will consider a second research question:

Preventing forged increased distance report relay attacks

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

As stated in Sections 1 and 2, there are reasons to see relay attacks that fake increased distance reports as a threat.

Using the information gathered and stated in the Background section, we will first study the conditions under which distance bounding systems could be vulnerable to these attacks. We will present various real life applications of distance bounding protocols whose intended functionality could be altered by performing these attacks.

Afterwards, using the mentioned sources of information, variations to the distance bounding protocols will be proposed, in order to effectively reduce the threat these attacks pose.

Using a theoretical approach, an explanation and evaluation of both the feasibility of these attacks as well as the proposed solutions will be given.

5 Results

5.1 How feasible are 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 Radio ToF distance-bounding protocol[18]. At some point, 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 1 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.

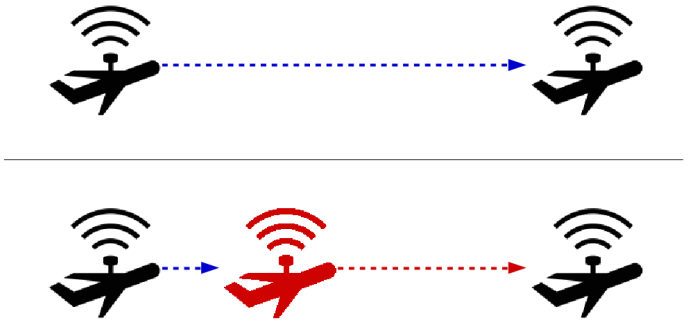


Figure 1: Regular communication versus block and relay attack.

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 some degree of knowledge about the system are also required to successfully perform an attack. However, there is no proving that these attacks cannot be performed with the appropriate technology.

Following next, we will discuss some real world applications that may be interesting for this research.

5.1.1 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 [8, 5, 15, 9], 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 seem to not be an active part of these systems, although they could be useful. First of all, the most obvious utility would be to provide an additional 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. This feature could be used as well to detect pedestrians in a future if devices such as mobile phones were adapted for this purpose.

Autonomous driven vehicles could also use distance bounding protocols to perform distance verification of specific targets. The distance bounding protocols developed in [18, 4] can be used to check the distance with specific targets. This is interesting in this environment as in a high traffic road it is difficult to keep track of other specific vehicles through the use of lidar[1] or computer vision system.

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.

5.1.2 Second example of real world attack: Drone MANETs

In the recent years there has been a huge increase on the interest towards drones[2], due the emergence of topics such as Amazon Prime delivery drones or the usage of unmanned aircraft by the US military.

It is safe to foresee that that the usage of drones will only grow on the upcoming years due 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.

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 huge package. For a company trying to keep expenses low, it would make sense to use multiple drones that can work cooperatively in different situations rather than having drones of various sizes for each type

[1] Lidar is a laser-based detecting system: `https://lta.cr.usgs.gov/LIDAR`

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

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

Figure 2: Amazon Prime delivery drone carrying a package. Because of legal constraints this delivery system is not being used yet, although it may start to be available at some point in 2015.[5]

of package. In this situation, an attacker could try to attack that system by faking some drone's distance reports to the others, which may force the drones to change positions and loose equilibrium, eventually crashing.

A relay attack on this platform could make more sense than just attempting to shut 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.

Area surveillance drones Another common usage of drone MANETs is to perform area surveillance. This case has both civilian and military applications. Civilian uses 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 further apart between themselves than 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 3 represents an example 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.

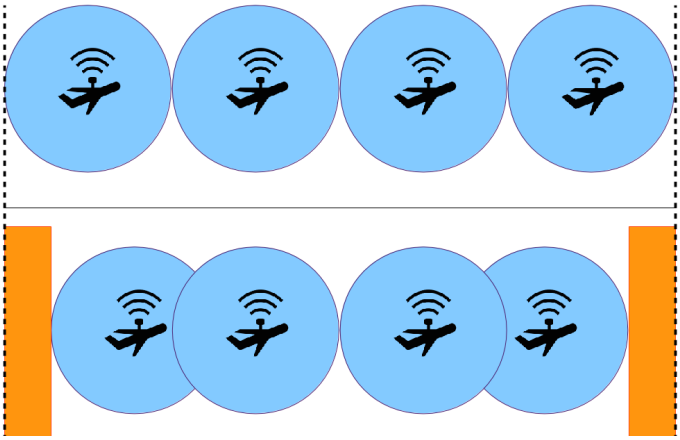


Figure 3: Example of the proposed attack. On the first case, the four drones manage to explore all the expected area (marked with trailing dots). On the second, the marked zones on the sides represent the resulting unchecked area as a consequence of this attack.

5.2 How can forged increased distance report relay attacks be prevented?

In this section some 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 the replication and addition of redundancy to provide protection against the fake increased distance reports. This means that the systems discussed on the first research question could implement these with minimal modifications.

5.2.1 Introducing behaviour verification

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

Therefore, storing information on the recent location history 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 some 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.

5.2.2 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 circle 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 no 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 4 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.

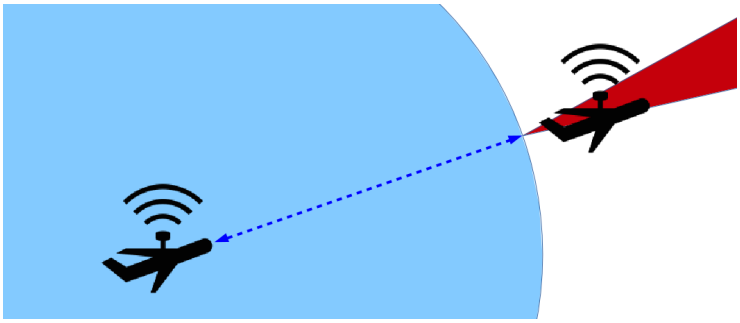


Figure 4: Scenario after the proposed countermeasure.

This protection method has two major downsides. The first is that devices should carry more antennas, increasing their cost. 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 obtain a correct triangulation (otherwise the error margins would outweigh the correctness of the obtained distance values)

5.2.3 Avoid centralized systems: distributed knowledge

When the first attack definition was proposed on Figure 1, only one of the nodes was reporting its location to the other. Although this setup 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. In essence, this solution is similar to the previous one, but on a larger scope. 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.

This trade-off between communication load and security is the only restriction on this solution. Different applications will have different needs, and the delay between messages has to be considered as well (a node A can report to B the position of a third node C on a given time, but B must consider the delay of the transmission with A when checking the received data).

6 Conclusions

From the results on the first research question 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, they will surely be amongst the most important developments in the upcoming years. This makes the vulnerabilities on distance-bounding protocols a latent problem.

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.

7 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 duration 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". In: (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". In: (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". In: ().

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

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

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

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