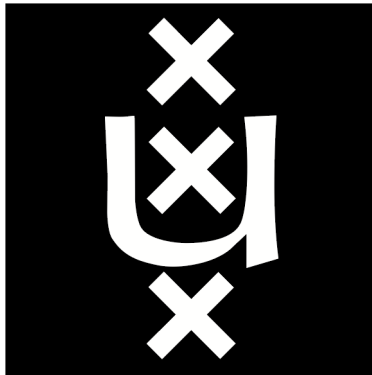UNIVERSITEIT VAN AMSTERDAM

RESEARCH PROJECT I

PROTECTING AGAINST RELAY ATTACKS FORGING INCREASED DISTANCE REPORTS

Xavier Torrent Gorjón
Xavier.TorrentGorjon@os3.nl

January 26, 2015

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed sed diam metus. Quisque velit urna, dictum vel eros eu, congue luctus augue. Nulla sit amet metus nec ipsum pretium vestibulum ut quis sem. Nullam malesuada risus ut rhoncus consequat. Fusce in hendrerit nibh. Morbi a magna nunc. In vel justo tincidunt, porttitor tellus in, porta lacus. Nulla posuere enim arcu, eget aliquet mauris dictum ornare. Morbi iaculis nec elit vitae rutrum. Nam posuere, risus sed semper finibus, augue lorem blandit ex, non tempor nunc tortor vel arcu. Cras non tortor ipsum. Suspendisse vestibulum molestie nibh, lacinia efficitur nunc luctus non. Phasellus sed nibh at est suscipit pulvinar. Cras eleifend ante et volutpat suscipit.

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 sent 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 on 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, 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 on various studies, as in [6, 7, 11, 17].

In this paper, we will first discuss the relay attacks used to forge fake location positions, focusing on the countermeasures against them. We will then focus on attacks forging increased distance reports, the feasibility of these attacks and propose solutions to them. In Section 2 we will discuss the available literature on this topic. In Section 3 we will briefly present results and conclusions from our research in the available literature about distance bounding protocols, GPS, radar detection and Inertial Navigation System. We will present on Section 4 a more detailed explanation on the research questions this project aims to answer. Following on Section 5 we will explain the methodology used in this study. Section 6 will discuss the actual results from our research questions, after which we will provide conclusions about the results gathered in Section 7.

2 Related Work

Relay attacks have been for long, and continue to be, an extensive field of research, as technologies and devices are shifting to a more mobile-focused paradigm. Many old procedures are being enhanced with wireless features, such as credit cards and car keys. However, it is not possible to find in the available literature studies regarding relay attacks used to fake increased distances between two legitimate nodes. It is the goal of this project to prove that these attacks can prove to be a real threat in real world applications, and how current distance bounding protocols can be enhanced to limit their vulnerability against them.

There is much literature available presenting solutions to distance bounding problems, as [1, 21, 18]. All of these studies are used as a base for others in 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 part of these studies as a basis for the solutions against the studied relay attacks.

There are also many practical studies in the field of distance bounding, which aim to test the vulnerabilities on real applications, such as [6, 7, 11, 17, 2]. Although all that research refers to forging decreased distance reports and it is not directly used in our research, it has been deeply as an starting point and inspiration.

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, as [22, 23, 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 location [3] and Inertial Navigation Systems [12] could be arguably used to prevent this attacks. Using these information sources we will explain why these systems are not reliable neither, 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 in 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 insight to our investigation as they are closely related.

3 Background

In this section we will discuss distance bounding protocols, the GPS system and radar detection. All of them are extremely relevant topics to our research. First we will explain the current distance bounding protocols, as we will use them as a starting point for our research. Then we will move onto GPS, and explain why systems shouldn't rely completely on it, hence the need to develop more powerful distance bounding protocols for our study cases. Lastly, we will discuss the possibility of using radar detection and Inertial Navigation System to fight the proposed attack.

3.1 Distance bounding

Distance bounding protocols were developed as a response to relay attacks that attempt to fool systems that validate an users proximity to a validation point. Common scenarios of these applications are found in access control systems, such as smartcards to access buildings or cars using remote passive keys.

These attacks try to use properties of the systems used in the communications (such as signal intensity or message time of flight (ToF)) to validate the

proximity of users. Based on the work of Capkun and Hubaux in [4], we will proceed to briefly discuss these methods:

Signal Intensity Signal intensity protocols try to achieve proper location of other nodes by measuring the received signal strength. Previous work available in the public literature, such as the research by Seshadri, Zaruba, and Huber in [19] proves the usefulness of this location system. Even though attacks on this systems are hard to perform [20], the defences against them rely mostly on anomaly detection. The reliability of these systems can be decreased in heavily adverse situations, and the ToF methods discussed next provide a higher degree of security.

Ultrasound ToF Ultrasound ToF measures the round-trip time of messages sent and received from the parties measuring 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 methods such as radio frequency or optical wires attackers can surpass the speed of the ultrasound communication, effectively being able to relay information faster than the legitimate infrastructure.

Radio ToF Radio-based ToF uses the same method as ultrasound ToF to perform the distance check. The key of the success of this method is that the information transmitted travels at speeds near the speed of light, meaning there is no physical way to fake one node is closer than it really is. Practical studies on this method [18] developed hardware that can perform the operations required under 1ns, meaning that the maximum theoretical distance an attacker can shorten its reported distance is under 15cm.

In this project we will be using Radio ToF as a basis for our work, as it is proven to be the most secure and reliable method. However, this method alone is not enough to fight reports that forge an increase on the real distance between parties, and this will be the main focus of our research.

3.2 GPS location

It could be argued that GPS location can 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.

Speaking of scenarios with one or multiple adversaries, even though there are many countermeasures to prevent attacks against GPS positioning [22, 23, 14], there do not provide complete security, similar to the Signal Intensity location protocol.

Due these problems, he U.S. government actually recommends to always have backup systems for GPS and suggests to never rely entirely on it[1]. Based on these premises we will assume that GPS is not a part of our system, or that we cannot rely on it.

3.3 Radar detection

One way to protect against this kind of Man-In-The-Middle attack could be by attempting to physically detect the attacker. 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, recent studies as the one by Cadirci in [3], state that Radar Cross Section,a measurement used to rate the ability to reflect radar waves by an object, can be heavily decreased by employing proper techniques 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[2], has a RCS signature of $0.025m^2$, which is similar to that of a bird[3].

In the attack scenarios proposed on 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 that kind of attacks.

3.4 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 *relative positioning* focus, staying independent from third party sensors.

The work done by Woodman in [24] evaluates the cost and performance of the INS. The conclusion from that work is that available INS hardware cannot realistically provide an accuracy below $5m$ of error after 60 seconds of operation. 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 $10m$.

---

[1] http://www.gps.gov/support/faq/#jamming
[2] http://www.fighter-planes.com/info/f117_nighthawk.htm

This also limits is usability as a stand-alone positioning system, as the error will only grow larger as time goes on.

Although INS accuracy is rapidly improving over the years, right now is not a viable solution or countermeasure to our problem.

4   Research Questions

As seen in the Related Work section, on the current literature there are no proposals to fight the subset of relay attacks that attempt to fake increased distance reports between legitimate parties. This project will prove that these attacks suppose a real threat, and as such, our first research question will be:

How feasible are forged increased distance report relay attacks?

Additionally, after the demonstration of the possibilities of these attacks, a second research question is considered:

How can these attacks be prevented?

4.1   Feasibility of forged increased distance report relay attacks

Minimum distance bounding appeared to have many solutions on the current literature. However, we observed that distance bounding regarding upper limits on reported distances was not a subject of research. In this project, we will present some theoretical attacks that could be used on many real world scenarios, and propose variations on the current distance bounding protocols to solve them.

The proposed scenarios are diverse in both context and properties of the systems involved in the communications. We will focus the study from the point of view of systems involving communication between drones, although we will provide solutions that can be extrapolated to other systems as well, such as automatically driven cars.

In this research question, we ultimately aim to explain why these attacks can be dangerous and an interesting topic of research.

4.2   Preventing forged increased distance reports

The second research question will focus on providing solutions to the issues stated on the first. Unlike minimum distance bounding protocols, we won't be able to use the speed of light as a fact to develop responses that cannot be faked, which implies that we might not be able to develop a system that completely protects against these increased distance reports. However, we do expect to provide solutions that suppose a meaningful security increase against these attacks.

5 Methodology

As stated in the Introduction and the Related Work sections, 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 many 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 suppose.

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

6 Results

On this section we will present the results of our research, structured in the form of two research questions.

6.1 Feasibility of forged increased distance report 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. 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 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.

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.
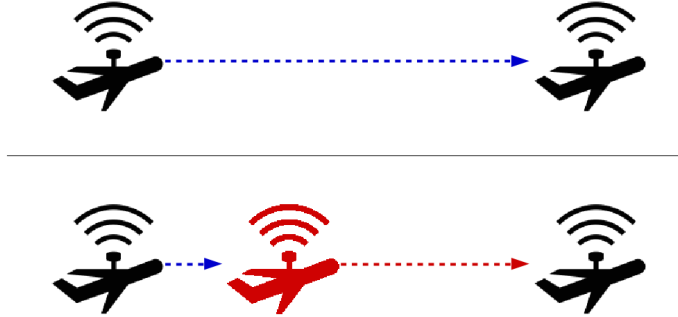
Figure 1: Regular communication versus block and relay attack.

6.1.1 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, such as [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[3] 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.

---

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

6.1.2 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 or the usage of unmanned aircraft by the US military.

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

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 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.

---

[4]http://www.google.com/trends/explore#q=drone
[5]http://abcnews.go.com/Technology/amazon-prime-air-delivery-drones-arrive-early-2015/story?id=21064960

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. Figure 3 represents an example of this attack.
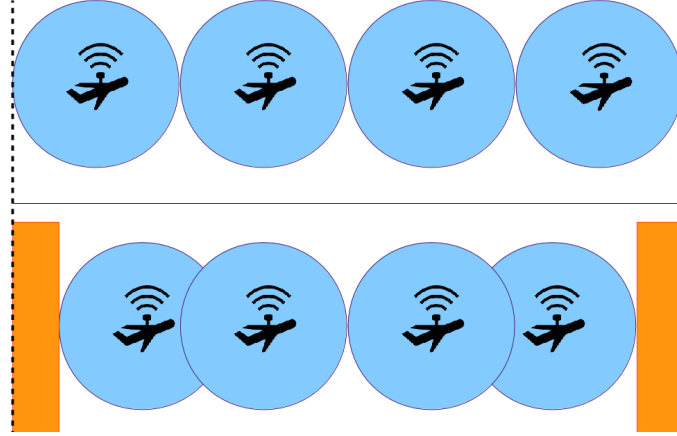

Figure 3: On the first case, the four drones manage to explore all the expected area (marked with trailing dots). On the second, the first and fourth drones are under a relay attack that makes them believe they're leaving area unexplored between them and the neighbour drones, which makes them decide to get closer to the other drones. The orange zone represents 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.

6.2 Fighting forged increased distance reports

Present the solutions

Multiple antenas and shared knowledge [Various paragraphs (5+), this is the first solution]

7 Conclusions

Consider the theoretical assumptions of the project [1 paragraph]

Given the proposed solutions, introduce and explain the implications [2 or more paragraphs]

8 Future Work

Briefly talk about the need of a more practical study with real hardware [1 paragraph]

...?

9 Acknowledgements

[2 paragraphs max]

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: *INFO-COM 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] 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.

[20] 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.

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

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

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

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