Universiteit van Amsterdam

Research Project I

Protecting against relay attacks forging increased distance reports

Xavier Torrent Gorjón
Xavier.TorrentGorjon@os3.nl

Version 3.0

Supervisors:

Jordi van den Breekel
vandenBreekel.Jordi@kpmg.nl

Paul van Iterson
vanIterson.Paul@kpmg.nl

May 7, 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, the solutions proposed in the current literature are limited when it comes to preventing relay attacks forging increased distance reports.

In this document, we first review the available systems that could be used instead of distance bounding protocols. In particular, the analysis will focus on Global Positioning System (GPS) and Inertial Navigation System (INS). This review 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.

We propose a real world scenario, in which a system using a distance-bounding protocol could be vulnerable to these types of relay attacks. We will discuss how the attacks could be performed, and the impact they might have on that system.

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. These solutions will be compared to the previous research done in this field, providing an insight on how they overcome the limitations of these previously developed solutions.

Keywords — Relay attack, distance-bounding protocol

Glossary

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

AM Amplitude modulation: A type of radio transmission based on sending different amplitude signals.

FM Frequency modulation: A type of radio transmission based on sending different frequency signals.

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.

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.

SNR Signal-to-Noise Ratio: Measure on the quality of a radio signal.

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 [4, 5, 7, 20].

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, the solutions available in the current literature for distance enlargement attacks are limited, Verifiable Multilateration and SPINE being the only proposed methods we could find for this purpose [3]. Verifiable Multilateration is a triangulation positioning technique using multiple distance-bounding protocol receivers, whose position is fixed and known, to determine the position of a mobile proving node. Although this solution provides efficient protection against distance enlargement attacks, it requires the whole system to work under a fixed, trusted land infrastructure, which limits its usability. Derived from Verifiable Multilateration there is also another proposed system named SPINE, which is able to resist attacks from a larger number of attacker nodes, but that still has the same limitations as Verifiable Multilateration.

Verifiable Multilateration can be a valid technique to prevent these attacks forging increased distance reports, when the devices work within the boundaries of a certain zone, such as in a warehouse or in a university campus. We propose a study case where the system cannot rely on an auxiliary infrastructure, implying that Verifiable Multilateration cannot be used, therefore justifying the need for different approaches to solve the issue. The crucial difference between our study case and the scenarios discussed in the Verifiable Multilateration (and SPINE, as it is derived from it) is that on our scenario all nodes are equal, and there is no distinction between proving nodes and verifying nodes, given the lack of a fixed infrastructure.

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. A scenario in which relay attacks forging increased distance reports could be used is presented in Section 6, along with an explanation of how these attacks could be performed. 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 an abundance of literature available presenting solutions to distance bounding problems [1, 22, 25]. 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. Specifically, we will discuss the Verifiable Multilateration technique [3] and how does it compare to our solutions.

There are also many practical studies in the field of distance bounding, which aim to test the vulnerabilities on real applications [2, 4, 5, 7, 20]. 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 [18, 26, 27]. 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 Inertial Navigation Systems (INS) [8] could arguably be used to prevent relay attacks. Using these information sources [8], we explain why neither of these systems are fully 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 [6, 17, 19] are a specific type of relay attack that, while being different than the ones we will study in this document, the research on these attacks provide valuable insight for our investigation.

3 Research Questions

We divide the research of this project into three main research questions. The relay attacks discussed, as well as their solutions, refer to the scenario we propose on our second Research Question.

Can other systems, besides distance-bounding protocols, be used to prevent these relay attacks?

The goal of this first research question will be discussing other technologies available that could be used to prevent these relay attacks. Specifically, we will review GPS and INS technologies, exploring their capabilities and limitations for this purpose.

How feasible are relay attacks forging increased distance reports?

In this second research question we discuss the possible implementations of these subset of relay attacks. We provide a small introduction to radio communication to explain how these attacks could be implemented in practice, and their feasibility. In this section we also propose an example of a real world application that could be affected by this kind of attacks.

How can relay attacks forging increased distance reports be prevented?

The last part of our research will focus on what countermeasures can be deployed to limit these subset of relay attacks in our proposed scenario. We propose various solutions, and evaluate how efficiently they protect against forged increased distance reports.

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.

Most of the contents in this document are based on studies done in the telecommunications field. These have been obtained through articles available on Google Scholar [10], with additional support of text books from the library of the Faculty of Science from the University of Amsterdam and various other online resources.

5 Distance-bounding protocols and alternative systems

In this section, we discuss distance-bounding protocols, as well as GPS and INS location systems. 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.

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 [3], 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 [23] proves the usefulness of this location system. Even though attacks on these systems are hard to perform [24], 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 [3].

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 [22] 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 [22], 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 itself and P.

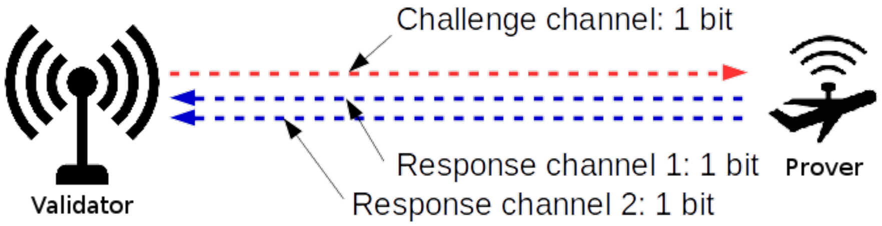

Figure 1: Channels in the distance-bounding Protocol proposed by Rasmussen and Capkun [22].

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, unless additional systems or infrastructures are deployed [3], and this will be the main focus of our research.

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 [18, 26, 27], 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 [28]. 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 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.

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

6 Attack Description

The original distance-bounding protocols were designed to prevent relay attacks forging decreased distance reports. These attacks were set under the assumption [1] that the original valid prover P is outside the range of the validator station V. Distance-bounding protocols were proposed as a viable solution to these kind of attacks, based on the fact that using a challenge-response system, a passive attacker could not relay information between points without adding additional delay. These conditions do not apply on the type of relay attack we study in this project. In this Section we will describe a scenario where this attack could take place, and discuss the possible implementations of the attack.

6.1 Real world example

To illustrate the possibilities of this type of attacks, we propose a specific real world scenario of a system using the distance-bounding protocol that could be vulnerable to these forged increased distance reports.

Drones can be used to perform tasks such as area surveillance or mapping. In certain environments, using one drone is not enough as the area they can effectively cover is limited. This can be solved by using drone MANETs, and keeping track of where the neighbour nodes are to prevent underperformance by checking overlapped areas or leaving areas unexplored. If these systems were to be attacked by relay attack forging increased distance reports between the drones, some areas could be left unexplored. Figures 2 and 3 provide a graphical interpretation of this issue.

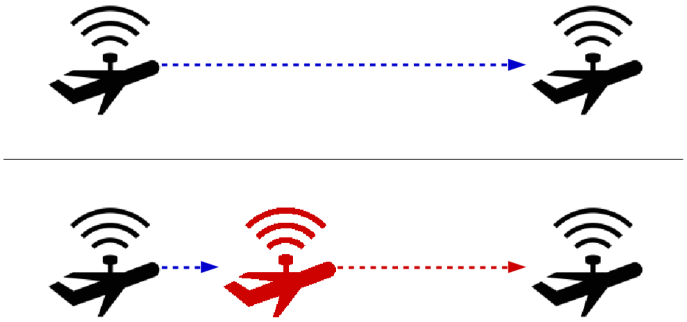

Figure 2: Regular communication versus block and relay attack.

6.2 Performing the attack

There are two main procedures to communicate information via radio signals: Amplitude Modulation (AM) and Frequency Modulation(FM). AM communi-

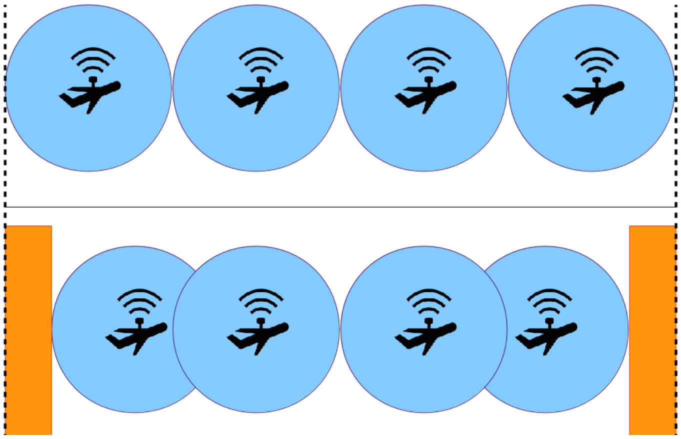

Figure 3: Example of the proposed attack. On the first case, the four drones manage to explore all the expected area (marked with trailing dots). On the second, the marked zones on the sides represent the resulting unchecked area as a consequence of this attack.

cation is based on emitting radio signals of different amplitude, whereas FM communication modifies the frequency of the signal. Figure 4 represents the differences between the two methods.

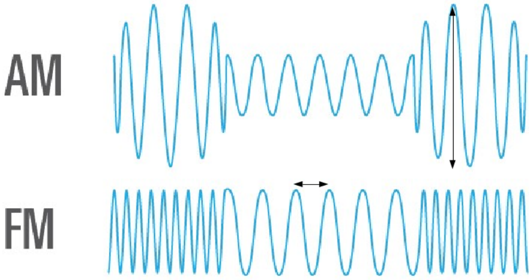

Figure 4: Difference between AM and FM information encoding. The black arrows show the variables in each case. Base image source: ravtrack.com.

FM communication should not be used for distance-bounding purposes, as it is a vulnerable form of communication due the *capture effect* [11, 14]. The consequence of this phenomenon is that if multiple signals with the same –or similar– frequency are received, only the one with the strongest signal can be demodulated. This implies that to perform the discussed attack, an attacker only needs to overwrite the signal being transmitted with a stronger signal to perform the attack.

Unlike FM communication, AM communication can receive and demodulate more than one signal at a time. This feature hinders the viability of the proposed relay attack, as even though the radio signal can be replayed, the original nodes will still receive the original signal. Because of this, the attacker is required to not only replay the signal with a certain delay, but also to block or otherwise obstruct the reception of the original signal. Although difficult, this obstruction can be theoretically done. We propose two different ways to achieve this: by adding noise or physically delaying the original signal.

6.2.1 Noise addition

Although AM communication is not susceptible to the capture effect, it is much more vulnerable to external noise [11]. Based on this, a node standing between the legitimate parties could add noise to the transmitted signal to decrease its signal-to-noise (SNR) ratio (which compares the desired level of the signal to the level of noise added due to external sources). However, this would also affect the delayed signal. To prevent this, the node performing this noise addition could replay the original signal on a different frequency range, not affected by the noise addition, to another attacker node close to the legitimate receiver, which would replay the original delayed signal on its original frequency with an increased signal strength.

This attack requires multiple attacking parties present in the system, and requires a high degree of coordination to be successfully performed. Albeit difficult, this could be possible with the appropriate equipment, although the details of its implementation fall out of the scope of this study.

6.2.2 Physically delay signals

A different approach to this attack consists on physically hindering the transmission of the original signal, instead of adding noise on the same frequency. This could be done by deploying fabrics of shielding materials [13] between the prover and the validator. Radio frequency shielding materials have two components that help blocking the radio signals:

Reflection Defined by the surface of the material, its reflection rate determines how much of the incident signal strength is reflected back. Besides the material itself, certain types of paint help in the reflection and absorption of radio signals, such as iron ball paint and nanotubes [15].

Absorption From the remaining part of the radio wave, a large fraction of it can also be absorbed by the volume of the shielding material itself.

These shielding fabrics would not entirely block the original signal [13], as part of it would still go through the fabric, and another part would still circumvent the fabric through its edges. However, it could reduce the signal strength to the point where the receiver is not able to reliably detect it, effectively only receiving the duplicated relayed signal.

7 Preventing relay attacks forging increased distance reports

In this section, countermeasures to the studied relay attack are proposed. These different solutions can be implemented at the same time, 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 system discussed in 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 [9].

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.

However, if a node starts suddenly reporting a considerably higher distance from the node performing the validation, this validator could determine that the system is under attack and raise an alarm. This location information should be used only for anomaly detection purposes, and should not be used for any kind of procedure or pathing decisions.

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 Utilizing 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 [12, 16] 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 validating drone detecting inconsistency in the received data.

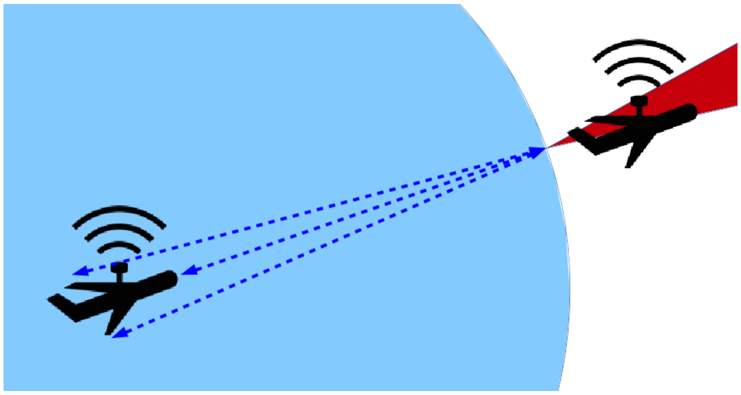

Figure 5: Scenario after the proposed countermeasure.

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 Avoiding 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 itself 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.

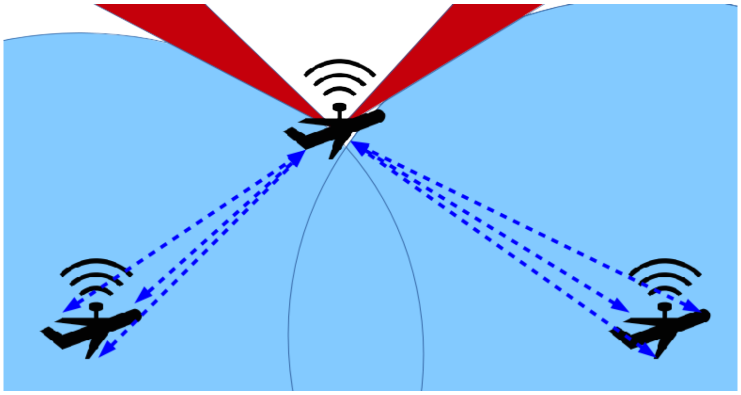

Figure 6: Using the information of multiple drones to check distances hinders the task of a possible attacker, as multiple signals have to be relayed properly.

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 of the investigation on the first research question, *Can other systems, besides distance-bounding protocols, be used to prevent these relay attacks?*, we conclude that GPS and INS can be solutions under certain conditions, or be used as an additional layer of security. However, systems should not rely solely on them, as they have certain limitations that cannot be circumvented. GPS relies on the information provided by an external source which could not be available, and INS accuracy is limited, especially have to be used over long periods of time.

The second research question stated was *How feasible are relay attacks forging increased distance reports?*. We discussed a particular study case, and two different ways on how these attacks could be performed. The attacks proposed have a high degree of complexity, and are difficult to do in practice. However, none of the difficulty of these attacks comes from the distance-bounding itself, but from the physical implementation of radio communication. These attacks could be feasible with the technology available, but it could be argued that in the next years, these could only become easier to perform, hence the need to develop a distance-bounding protocol that does not rely on external implementation features to remain secure.

To solve these issues, we proposed our third research question, *How can relay attacks forging increased distance reports be prevented?*. We propose three different solutions to the issue. These solutions can be implemented separately or on top of each other, which allows to select a subset of them depending on the limitations of each specific system.

Our first solution, utilizing behaviour verification, offers an increase in security at the cost of requiring additional memory space. It does not require a noticeable increase of computing power, and does not alter the original idea of the distance-bounding protocols. It is, therefore, the easiest and cheapest solution to implement, meaning it could be applied to most systems.

We propose using a triangulation system based on the distance-bounding protocols in our second solution. This solution offers a higher degree of resilience than the first solution, but comes at the cost of having an additional expense due the need for more hardware. However, the solution is still relatively simple to implement.

The last proposed solution features a design in which nodes can share the knowledge of the position of other nodes relatively to their own position. Compared to the other solutions this one is more difficult to implement, as it requires nodes to keep up multiple communication channels and process the information received from them. This generates a processing need that is not negligible, and that not all systems may be able to afford.

The three solutions proposed offer higher degrees of resistance against the discussed relay attacks. However, unlike the Verifiable Multilateration and SPINE solutions, our solutions cannot achieve total protection from distance enlargement, as our proposed system on the discussed scenario cannot rely on a stable, fixed and trusted land infrastructure to perform the distance checks. However, the proposed solutions hinder considerably the success chance of these relay attacks.

When deploying a new system that requires protection against such distance enlargement attacks, it should be considered whether it is possible or not to use a fixed infrastructure as the one used in the Verifiable Multilateration and SPINE techniques. If that was the case, these solutions already offer a highly resilient solution against these relay attacks. However, as these techniques cannot be used without that type of infrastructure, our solutions could be applied on all the other scenarios that do not meet that requirement.

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. We left out of the scope the practical details of how these attacks could be performed, as it is a topic large enough to be a separate project.

A second interesting future research would be to investigate the possibility of using channel hopping [21] as a countermeasure for the discussed attacks, having distance-bounding protocols use multiple channels, and not only the fixed three that are necessary to use distance-bounding protocols.

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] 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.

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

[5] 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.

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

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

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

[9] http://ns1758.ca/winch/winchest.html. *Nova Scotia's Electric Gleaner webpage - Cost of Hard Drive Storage Space.*

[10] http://scholar.google.nl/. *Google Scholar website.*

[11] https://www.windows2universe.org. *RICE University Windows to the Universe wepage.*

[12] http://www.britannica.com/EBchecked/topic/604642/triangulation. *Enciclopaedia Britannica page on triangulation.*

[13] http://www.emiguru.com/. *Kimmel Gerke Associates web blog.*

[14] http://www.its.bldrdoc.gov/. *Institute for Telecommunication Services wepage.*

[15] http://www.technologyreview.com/news/426276/nano-paint-could-make-airplanes-invisible-to-radar/. *MIT Technology Review.*

[16] http://www.trimble.com/gps_tutorial/howgps-triangulating.aspx. *Trimble page on triangulation.*

[17] 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.

[18] 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).

[19] 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.

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

[21] 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.

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

[23] 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.

[24] 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.

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

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

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

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