University of Amsterdam

Research Project I proposal

Protecting against relay attacks forging increased distance reports

Xavier Torrent Gorjón
Xavier.TorrentGorjon@os3.nl

January 9, 2015

1 Introduction

Most communication systems can be secured by using encryption protocols when there is a need to secure user data. This prevents attackers from gaining any information (provided the protocols are correctly implemented and the algorithms have no weaknesses) about the data being transmitted.

However, attackers can still make use of attacks based on relaying information to achieve goals such as system malfunction or even unauthorized access. There are many publications providing practical and real world examples about this problem, such as [2, 3, 4]. These publications show that this is a general problem not bound to specific implementations of hardware or software, and depending on the constrains of the used systems (power requirement, size, environment conditions) they can be quite challenging to solve.

There have been many studies providing solutions to these problems, using distance-bounding protocols such as the proposed in [1] and [5]. These protocols prevent verifying terminals from getting relayed messages reporting legitimate users to be closer than they really are.

However, we could not find in the available literature solutions for the opposite problem: malicious users relaying attacks to claim that a legitimate user is further away than he really is. Possible interesting study cases regarding this issue might surveillance drones or automated cars.

Imagine a situation where a squadron of flying drones were used to explore an area. To make sure all the area is being checked, these devices must rely on some kind of protocol to exchange information about their positions so that the whole squadron can reassign positions or change formation as obstacles appear. GPS signals can be used to avoid relay attacks forging distance reports, but it is not a system that can be trusted (drones working inside a warehouse, or being on a hostile environment where GPS signals are blocked), so the whole system should be independent from external positioning information. If the drones' system to report relative position to other drones is tempered somehow, it could lead to an attacker successfully preventing an area from being explored or even forcing two or more drones to crash together by making them believe they are further away than they really are.

It is easier to find an exploitable situation on automated car systems, as usually they loose their GPS signals without being in an obviously hostile environment, due *natural* causes such driving inside a tunnel, being on a neighbourhood with tall buildings or stopping at an underground parking.

These study cases are topical issues nowadays, and we find them an interesting subject to work with. They both fall under the category of MANETs (Mobile Ad Hoc Networks) and, treating them as such, the goal of this project will be to provide solutions to the stated problems.

2 Related Work

All the papers we found researching on this subject were focused on preventing attacks aimed to fake a closer position, usually related to access systems such as PKES (Passive Keyless Entry and Start Systems) [2] and proximity cards [3].

Although the proposed solutions for these problems ([1, 5]) are not suitable for our research, they will surely serve as an inspiration.

3 Research Questions

In this project we will attempt to answer two main questions:

How feasible it is to perform relay attacks on MANETs which forge reports stating increased distances than the real ones?

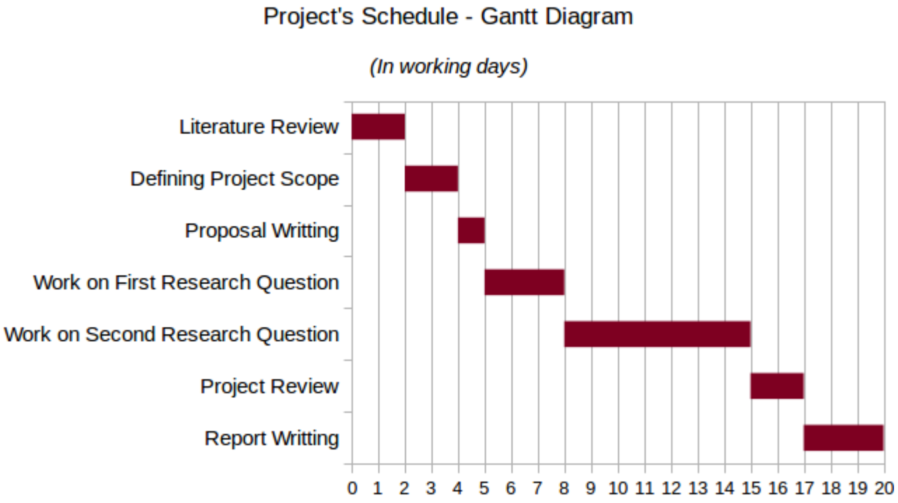
To what extent can we detect, prevent, or provide countermeasures against those attacks?

Answering the first question is a pre-requisite to narrow down the scope of the project and make decisions on how to proceed with the investigation. It is important to study which conditions and attack paths could be available in order to provide a complete picture of the problem.

The second question will be a theoretical research on how can these networks be protected against that kind of relay attacks. It is possible that more than one solution is found, and in that case, a comparison between them will be given, as different solutions will most likely have different advantages and disadvantages over the others.

4 Planning

The assigned time for this project are four weeks, from January 5th to January 30th. The presentation and defence of the project will be done on the first week of February. The project development will proceed as follows on the next diagram:



5 Expected results

By the end of this project we expect to provide one or more theoretical solutions and countermeasures to protect MANET from relay attacks on their communication systems that lead to nodes believing they are further apart than where they really are.

6 Ethical considerations

The project will be a theoretical study that will not be using any kind of user data, and solutions provide will be based upon theoretical models. We can safely assume that we won't be running on ethical issues regarding user privacy.

At this moment we cannot foresee any direct implications regarding ethical issues, as this project will focus on developing new protocols to protect against a certain type of relay attacks, not on trying to find weaknesses on any theoretical or real application.

References

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

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

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

[4] 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.

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