Secure Neighbor Discovery in Wireless Networks

IK2200 Communication System Design, HT 2023

TA: Ahmed Hussain, **Email**: ahmhus@kth.se
and Panos Papadimitratos
Networked Systems Security Lab
www.eecs.kth.se/nss

1 Introduction

Wireless networks are becoming more and more of an integral part of our daily lives, providing connectivity and enabling communication across various devices. Neighbor Discovery (ND), as depicted in Fig. 1, is a fundamental process in wireless networks that allows devices to find and communicate with nearby devices. However, this process can be exposed to various security threats, such as spoofing, eavesdropping, and denial-of-service. Hence, the need for having a mechanism to ensure Secure Neighbor Discovery (SND) is essential.

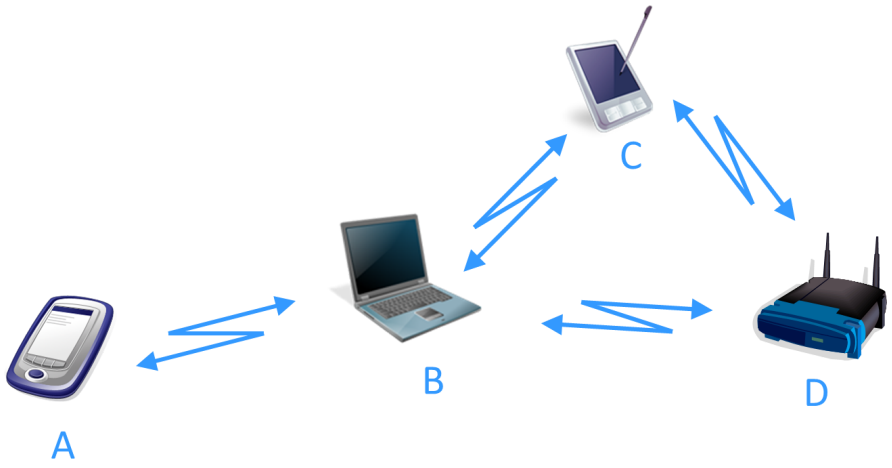

Figure 1: Neghibor Discovery in Wireless Settings

In this project, you are expected to do the following:

- Investigate existing methods to implement SND with wireless-based systems
- Implement SND based on time, time-location, and other various methods found in the literature [1, 2]
- Implement different scenario settings and perform different attacks (MiTM, Wormhole,...etc) to examine the implemented protocol robustness
- Compare the efficacy and effectiveness of the different methods used to achieve SND

2 System Overview

Secure Neighbor Discovery ensures that devices can identify and communicate with legitimate neighbors while ensuring they communicate directly with them. As illustrated in Fig.2, we have two devices (**A** and **B**) that perform ND. **A** and **B** communicate directly or equivalently; they are neighbors, or as it is usually said, are within range of each other. When **A** and **B** are not neighbors, as in Fig.3, an adversary ($\mathcal{E}$) relays their messages. Without SND, A and B can be misled that they are neighbors while they are not. An example of a solution includes **A** transmitting an SND message that includes its location coordinates, a timestamp, and a digital signature, where **B** can verify (using **A's** public key) that it is communicating with a legitimate neighbor, and assess whether it communicates directly with A.

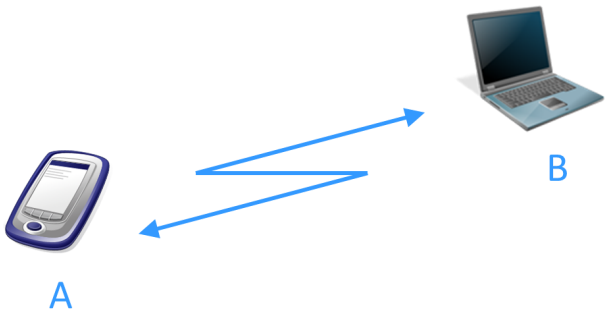

Figure 2: Two devices **A** and **B** trying to discover one another given that they are in range.

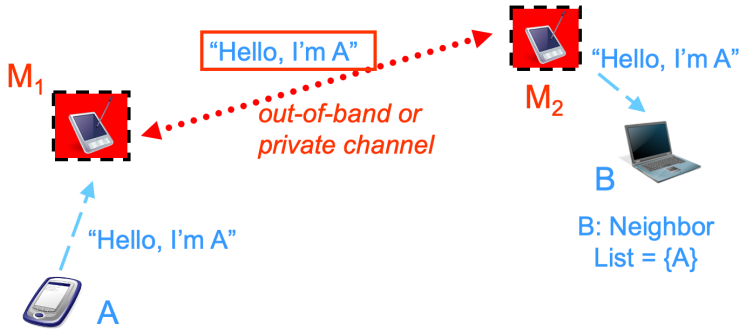

Figure 3: **A** and **B** are not in range and $\mathcal{E}$ (M_1 and M_2) is misleading them to believe that they are in range by relaying their messages.

3 Project Description

3.1 Literature Review (15%)

You are anticipated to familiarize yourself with foundational concepts in computer security, encompassing fundamental security-oriented topics such as hash functions, symmetric key cryptography, and public key cryptography. Additionally, a literature review is needed on SND [2, 1, 3]. This review will enable you to explore and understand how existing protocols for SND work.

3.2 Implementation (50%)

The implementation phase will involve implementing and building the Secure Neighbor Discovery on actual devices. This implementation encompasses the following:

1. Implementing a basic ping-pong protocol (exchanging simple messages) between two devices as an initial phase to have a plain ND (15%)

2. Improve ND into authenticated ND (10%)

3. Extend the previous implementation into time-based, location-based, and time-location-based SND [1] (30%)

4. Performance evaluation, where you experiment with different device distances and channel conditions, then observe the protocol robustness and correctness (15%)

5. Introduce 1 or 2 attack scenarios and perform them (30%)

3.3 Experimental Evaluation (20%)

During the evaluation phase, you are tasked with assessing the performance of the implementation, encompassing both the baseline scheme (the plain ND), the authenticated, and the variants of the SND protocols. The experiments should illustrate the effects of processing delays, communication distance, channel conditions, and resilience to different types of attacks while considering varying the parameters.

3.4 Final Report and Deliverable (15%)

In the final phase, it is imperative to have a comprehensive report that includes and discusses each stage's intricacies. Moreover, you should document your code and use version control (e.g., GitHub). Finally, you are expected to prepare an oral presentation and present a working demo illustrating your implementation.

4 Passing Requirements

To obtain a passing grade for the course, the following is required:

1. Successful implementation of the none-secure ND protocol and the authenticated ND

2. Successful implementation of at least one of the methods (e.g., time-based, time-location-based...etc. Including basic crypto as well) to Secure the ND protocol

3. Implementing at least one attack scenario

4. Providing at least two performance evaluation metrics of your implementation

References

[1] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Formal analysis of secure neighbor discovery in wireless networks," *IEEE transactions on dependable and secure computing*, vol. 10, no. 6, pp. 355–367, 2013.

[2] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux, "Secure neighborhood discovery: a fundamental element for mobile ad hoc networking," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132–139, 2008.

[3] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.-P. Hubaux, "A practical secure neighbor verification protocol for wireless sensor networks," in *Proceedings of the second ACM conference on Wireless network security*, pp. 193–200, 2009.