Secure Neighbourhood Discovery

Bastian Fredriksson
bastianf@kth.se

November 24, 2016

`Course: Advanced Networked Systems Security, Lecture 2`
`Lecturer: Panos Papadimitratos`

1 Problem definition

Neighbourhood Discovery (ND) is the problem of detecting all neighbours N to a specific device d. $n \in N$ is called a neighbour to d in one of the following two cases

1. Either if n is directly connected to d, e.g through a cable, in which case n is called a communication neighbour...
2. ...or, if n is within distance of the wireless transmitter of d and v.v., in which case n is called a physical neighbour.

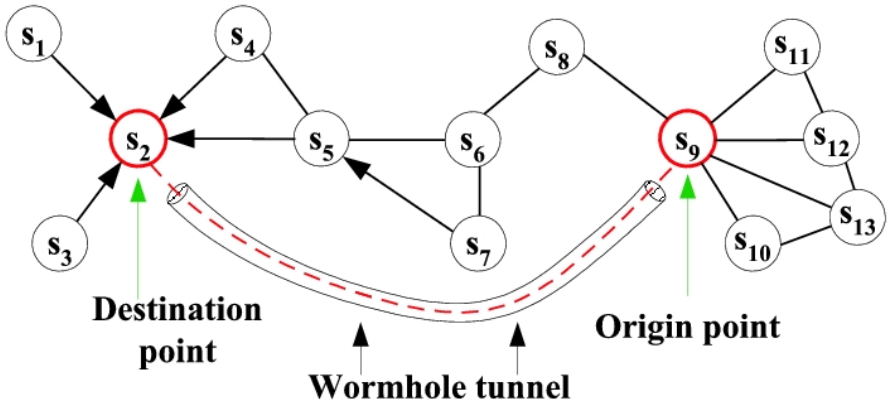
`Important` these two notions are not equal. E.g a device can be a physical neighbour without being a communication neighbour.

Secure Neighbourhood Discovery is the problem of performing ND in presence of an adversary, which might try to jam, relay or modify the communication between two devices to trick them into believing they are neighbours while in fact they are not.

ND is an important building block in many situations, including physical access control, network access control and routing[2].

2 Attacks

Relay attack - Attack where an attacker authenticates by relaying the signal to the victim and replaying his response[5].



Wormhole attack - A "wormhole" controlled by an attacker is set up between two networks. Due to a new shorter route being advertised, the wormhole will attract a considerable amount of traffic, which the attacker can drop, redirect or spy on depending on what he want to achieve[1].

3 Solution

`T-protocols` A T-protocol is a protocol which tries to perform neighbour discovery using a timer which measures RTT. Unfortunately no such protocol can solve the secure neighbour discovery problem, since an adversary is indistinguishable from a correct node[3].

Instead the scheme described in [4] solves the problem. The scheme is divided into three parts. The first part consists of measuring the distance d_{ij} between each pair of nodes (i, j) using ultra-sound. The second step consists of every node sharing a neighbour table containing the triples $(i,\ j,\ d_{ij})$. All messages are encrypted with a shared secret for confidentiality, and authenticated with MAC to detect tampering. The third and last step is called link verification, where three consistency tests are performed. If a node fails a consistency test, it is ignored and discarded.

The consistency tests for a node i are as follows:

1. **Link symmetry test** The distance between i and j must be equal to the distance between j and i.
2. **Maximum range test** The distance to a node must be within the communication range.
3. **Quadrilateral test** For every neighbour j, find two other neighbours u and v such that (i, j, u, v) are all neighbours and the polygon whose corners are the nodes (i, j, u, v) is convex. A convex polygon is a polygon where all interior angles are ≤ 180 degrees.

`Note` The last consistency test requires the location for each of the nodes. We must therefore combine this protocol with a protocol for secure location communication. To be continued...

References

[1] Wireless Attacks Unleashed. http://resources.infosecinstitute.com/wireless-attacks-unleashed/. Accessed: 2016-11-24.

[2] Papadimitratos, P., Poturalski, M., Schaller, P., and D. Basin, P. L., Čapkun, S., and Hubaux, J.-P. Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking. *IEEE Communications Magazine 46*, 2 (February 2008), 132–139.

[3] Poturalski, M., Papadimitratos, P., and Hubaux, J.-P. Formal Analysis of Secure Neighbor Discovery in Wireless Networks. *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)* (2013).

[4] Shokri, R., Poturalski, M., Ravot, G., Papadimitratos, P., and Hubaux, J.-P. A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks. In *Second ACM Conference on Wireless Network Security (WiSec'09)* (Zurich, Switzerland, March 2009).

[5] Thevenon, P., and Savry., O. Implementation of a Countermeasure to Relay Attacks for Contactless HF Systems, Radio Frequency Identification from System to Applications. *InTech, DOI: 10.5772/53393.* (2013).