Chapter 7

A Concluding Remark

One of the most important lessons learned while designing SAODV has been the need to keep things clear, so they can be properly analyzed. In a security system there should be a clear distinction of the following items:

- The **scenario** (or scenarios) that is going to protect.
- The **security features** that this scenario requires.
- The **security mechanisms** that will fulfill those security features.

Once the design of the cryptosystem is done, it is time to analyze if it indeed works. And, since the three items listed above are clearly separated in the design, it is much more easier to perform such analysis because it can be splited int the following parts:

- The **analysis of requirements**: Whether the security features are enough for the targeted scenario.
- The **analysis of mechanisms**: Whether the security mechanisms are indeed fulfilling all the security requirements. When doing this, it will be found that there are still some attacks that can be performed against your system. Some of them, typically, are not avoided because a trade off between security and feasibility.

- The **analysis of feasibility**: Whether the security mechanisms have requirements that are not feasible in the targeted scenario.