

# PhD Subject in Computer Science: Formal analysis of mobility in wireless communication

Verimag\*

October 23, 2007

**Supervisor:** P. Lafourcade<sup>1</sup>  
**Contact:** Pascal.Lafourcade@imag.fr  
**Also a master degree subject**

## 1 Context

Sensors, cell phones, cars and many modern applications use wireless communication. This allows more freedom and flexibility to users. Many designers have proposed protocols to guarantee the security of such communications. Most of these protocols use timestamps and cryptographic primitives. In this area, new properties appear, such as the concept of neighborhood. Neighborhood is the property to communicate directly with one of your actual neighbors (it means without replay). In wireless communications one well-known attack is the worm-hole attack. It consists in an intruder catching a signal emitted by a player A and forwarding it to some instance B which is not his neighbor. By this way, the intruder misleads the instance B receiving the forwarded signal, making it believe that he is the player A. One concrete application of this attack is that an intruder can enter into a building faking a control access RFID reader. Many new protocols try different ways to avoid this kind of attack [6, 5, 9, 8, 12, 7]

In the last few years, formal analysis of cryptographic protocols has become classical. Many formal methods exist or are still being designed for automatic verification of properties like secrecy or authentication [10, 3, 1, 11, 4, 2]. This area of research is very active and it aims at eventually prove security of concrete protocols used in modern communications. The aim of this work is to analyze, using a formal approach, different properties of wireless networks.

## 2 Goals

The first goal of this work is to list and understand what are new properties that wireless communications have to guarantee. We also want to analyze what are the intruder capabilities in this context, and propose a formalization, which

---

\*<http://www-verimag.imag.fr>

<sup>1</sup><http://www-verimag.imag.fr/~plafourc>

try to catch the mobility of the agents. For this purpose, we can try to extend our first draft of model of neighborhood property.

After this analysis and formalization, the last task would be to perform an automatic formal analysis for the selected properties.

### 3 Bibliography

#### References

- [1] R. Amadio, D. Lugiez, and V. Vanackère. On the symbolic reduction of processes with cryptographic functions. *Theoretical Computer Science*, 290(1):695–740, 2002.
- [2] David Basin, Sebastian Mödersheim, and Luca Viganò. Ofmc: A symbolic model checker for security protocols. *International Journal of Information Security*, 4(3):181–208, June 2005. Published online December 2004.
- [3] B. Blanchet and A. Podelski. Verification of cryptographic protocols: Tagging enforces termination. In *Proc. 6th International Conference on Foundations of Software Science and Computation Structures (FOSSACS'03)*, volume 2620 of *Lecture Notes in Computer Science*, pages 136–152, Warsaw, Poland, 2003. Springer-Verlag.
- [4] Liana Bozga, Yassine Lakhnech, and Michael Perin. HERMES: An Automatic Tool for Verification of Secrecy in Security Protocols. In *Computer Aided Verification*, 2003.
- [5] Levente Buttyán, László Dóra, and István Vajda. Statistical wormhole detection in sensor networks. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, *ESAS*, volume 3813 of *Lecture Notes in Computer Science*, pages 128–141. Springer, 2005.
- [6] J. Eriksson, S. V. Krishnamurthya, and M. Faloutsos. Truelink: A practical countermeasure to the wormhole attack in wireless networks. In *ICNP'06*, 2006.
- [7] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In *IEEE Conference on Computer Communications INFOCOM*, 2003.
- [8] Ritesh Maheshwari, Jie Gao, and Samir R. Das. Detecting wormhole attacks in wireless networks using connectivity information. In *IEEE Conference on Computer Communications INFOCOM*, 2007.
- [9] Radha Poovendran and Loukas Lazos. A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wireless Networks*, 13(1):27–59, 2007.
- [10] M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions is NP-complete. In *Proc. 14th Computer Security Foundations Workshop (CSFW'01)*, pages 174–190, Cape Breton, Canada, 2001. IEEE Comp. Soc. Press.

- [11] Mathieu Turuani. The cl-atse protocol analyser. In *Proceedings of the 17th International Conference on Rewriting Techniques and Applications (RTA '06)*, Lecture Notes in Computer Science, Seattle, USA, August 2006. Springer-Verlag. To appear.
- [12] Weichao Wang and Bharat Bhargava. Visualization of wormholes in sensor networks. In *WiSe '04: Proceedings of the 2004 ACM workshop on Wireless security*, pages 51–60, New York, NY, USA, 2004. ACM Press.