On automating the verification of secure ad-hoc network routing protocols:

RELATED WORKS (until my publication)

Ta Vinh Thong
thong@crysys.hu

Budapest University of Technology and Economics,
Department of Telecommunications,
Laboratory of Cryptography and Systems Security

2011

Figure 1 shows the position of our contribution compared to previous works in the literature. In the figure, we classify the most important related works into three categories, each of which is represented by a circle. The circle on the left includes automatic model-checking tools, the uppermost circle contains the works that are concerned with formal analysis of ad-hoc and sensor networks, and finally, the formal methods proposed for reasoning about secured protocols can be found in the circle on the right.

SAL model checker, SPIN [8], and UPPAAL [2] are general purpose model-checking tools. The main drawback of them is that they lack semantics and syntax for modelling secure routing protocols, and for reasoning about attackers specific to ad-hoc networks. CSP [11], CPAL-ES [9], and ProVerif [3] are automatic verification tools developed for verifying security protocols, but they lack semantics and syntax for modelling routing protocols and ad-hoc networks. The tool in [12] is proposed for detecting loops in ad-hoc networks, however, it lacks semantics and syntax for modelling cryptographic primitives and operations, and does not consider attacker nodes.

A calculus for sensor networks [10], a calculus for ad-hoc networks [7], a work based on the simulation paradigm [5], and the ω-calculus [12] are proposed for analysing pure and secure routing protocols. However, the main drawback of
these methods is that they are not automated. The well-known \textit{spi-calculus} [1] and applied \textit{π-calculus} [6] are proposed for modelling security protocols. They are not automated and cannot be used to model routing protocols.

To best of our knowledge, our method is the first that supports all the three issues at the same time. The works that are the most closely related to the work presented in this paper are [4] and [3]. As we have mentioned before, this paper can be considered as an improved and extended version of [4]. The main new contributions in this paper include the handling of arbitrary network topologies and reducing the verification complexity by backward reachability analysis. Our proposed technique was inspired by the verification method used in the well-known Proverif automatic verification tool proposed for verifying security protocols [3]. However, as opposed to [3], our method is designed for verifying routing protocols, it includes numerous novelties such as the modelling of broadcast communications, neighborhood, transmission range, and it uses an attacker model specific to wireless ad hoc networks.

\section*{References}


