Extended Abstract

Secrecy and Authenticity in Mobile Ad-Hoc Networks

Master's Thesis

Willard Þór Rafnsson

Distributed Systems and Semantics Unit,
Department of Computer Science,
Aalborg University, Denmark

10th June 2008

Security protocols, such as protocols for secrecy and authenticity, specify how parties can establish mutual privacy and trust, typically by use of encryption. A widely-applied example of such a protocol is the Diffie-Hellman key agreement, used to establish an encryption key for subsequent encrypted communication. Software systems rely heavily on the *guarantees* claimed by security protocols for *correctness*, and this reliance is only increasing. Examples of such systems include software used by banks to wire-transfer funds, practically all internet services requiring user authentication or secure communication channels, and remote-controlled critical systems such as those to control unmanned subway trains remotely. Security in these settings is an issue since information is transferred over an *unsafe medium*, often routed via. untrusted intermediaries.

Because of this, *formal verification* of security protocols is of particular importance, since *flaws* have been found in many published protocols. Flaws are sometimes overlooked during scrutiny due to the imprecise, informal manner in which these protocols are specified, and frequently remain undiscovered for years, even after being accepted by international standard bodies like IEEE and ISO, and applied widely. Much effort has therefore been spent in developing and applying theory for formal verification of security protocols.

While manual proof techniques for rigorously proving (in)correctness of security protocols exist, some flaws may escape even the protocol analyst, as was the case with the Needham-Schroeder public key protocol. *Automated verification* techniques therefore have much appeal, as analysts can rely on the rigorously-proven *soundness* of the claims made by the automated verification.

While formal methods for automated verification of security protocols exist, few of them are applicable to *security protocols for Mobile Ad-hoc Networks* (MANETs). This is typically due to the underlying assumption of an *unchanging point-to-point* network

topology in the *formal language* used to formally specify the protocols prior to analysis, contrasting the *broadcast* message delivery in the *changing* network topology of MANETs. As security protocols for MANETs are fairly new, there is an an inherent *lack of methods and tools for verifying their correctness.* Several such protocols are in the process of standardisation, and two of these protocols, ARAN and SAODV (protocols for secure routing in MANETs), have been proven insecure.

We propose *a framework for automated verification of MANETs* in our thesis, which consists of a *formal language* and a proven sound *verification technique* which can be automated.

The language we develop is the Distributed Applied π Calculus with Broadcast, which, as the name implies, extends the Applied π calculus by Abadi and Fournet with a new Distributed π calculus style *network abstraction layer* by Hennessy and Riely, communication-constraining *connectivity graphs* similar to those of CBS$^\sharp$ by Nanz (to represent the network topology), and with a *broadcast message-passing semantics* over named channels. This lets us model MANETs more accurately, with an arbitrary data language in the form of a *term rewrite system*, in a similar manner as signatures can be instantiated in Applied π. New interesting features we can model in our language include several broadcast mediums, safe and unsafe locations (the former guaranteeing that attackers cannot impersonate a location), and safe and unsafe communication mediums. The increase in the conceptual complexity of the calculus extension is surprisingly small, and involves only a slight change in the inference rules of Applied π. Due to its close relation to Applied π, we inherit many central definitions and results from Aπ to our calculus, like the notion of *frames and static equivalence*, and thus the classic definitions of *secrecy and authenticity.*

Working towards our automated verification technique, we prove a powerful theorem expressing *a syntactic relationship* between Horn clauses generated from initial processes in the calculus of Abadi and Blanchet, and the initial process. Several interesting corollaries follow from this result, including the *soundness of Horn clause deduction* with regards to message-passing in the source process, and that the *Horn clauses overapproximate syntactic secrecy in the active case* (defined by Cortier, Rusinowitch and Zalinescu). We do this by imposing several (harmless) syntactic limitations on our source process, including *canonicalisation* and *enrichment* of the Horn clauses generated by Horn clause generation algorithm. In the process of making the proof, we observe a sometimes-*overlooked assumption* in the Dolev-Yao threat model (the model typically assumed in the field of security protocol verification): that *any* message, including those sent during internal reduction, sent on free names are obtained by the hostile environment. To express this assumption, we devise a *revelation semantics*, which can easily be adapted to, for instance, Applied π, as it assumes only the existence of a labelled transition relation (which only allows sending of identifiers), and the definition of evaluation contexts.

Finally, by proposing how the constraints imposed by network topologies can be encoded into Horn clauses, we derive a proof of *soundness of Horn clause deduction for our calculus* from the proof mentioned previously.

Together, these results pave the way for, with minimal effort, to apply automated Horn clause constraint solvers such as ProVerif and the Succinct Solver Suite to reason soundly about the validity of secure Mobile Ad-hoc Network protocol models.