On formal and automated security verification of WSN transport protocols

Ta Vinh Thong

WSN transport protocols

The need of WSN transport protocols

- In some applications of Wireless Sensor Networks (WSN), e.g., multimedia sensor networks, the sensors capture and transmit high-rate data with some Quality of Service requirements.
- Transport protocols used in wired networks (e.g., the well-known TCP) are not applicable in WSNs because of its inefficiency.

Design Goals

- reliable delivery and congestion control.
- energy efficiency.

Problem

Most WSN transport protocols do not address security issues at all, hence, they ensure reliability and energy efficiency only in a benign environment.

Attack: Modifying and forging control and data packets

- Modifying data packets could cause honest nodes storing incorrect packets.
- Spoofing, forging, modifying control packets could cause improper deleting of caches or futile retransmissions of packets.
- Degrade the quality of service.

Definition of security to be proven

Prove that the Real and Ideal version are probabilistic timed bisimilar with each other.

Motivation and Goal

- Hard to detect subtle attacks.
- Informal reasoning is error-prone.
- Related works cannot be used to model and reasoning about the systems including (i) real-time, (ii) probabilistic behavior, and (iii) cryptographic operations, all at once.

Goal: 1. Formal and systematic approach
2. Automatic verification method.

Our work

Propose a new probabilistic timed calculus

- Supports syntax and semantics for modelling systems with (i) cryptographic operations, (ii) real-time and (iii) probabilistic behavior at the same time.
- The proposed calculus provides a convenient way for proving the security of WSN transport protocols, as well as their vulnerabilities, using The probabilistic timed bisimilarity.

Real version

Ideal version

In the ideal version: hidden, private channel are defined between honest nodes, for informing each other about the correct messages should be received.

Secure

PAT toolkit

ATTACK TRACE

PAT language
- Transport protocol
- Security property goals

(c) By author, 2013