Cryptology ePrint Archive: Report 2013/014

On formal and automatic security verification of WSN transport protocols

Ta Vinh Thong and Amit Dvir

Abstract: In this paper, we address the problem of formal and automated security verification of WSN transport protocols that may perform cryptographic operations. The verification of this class of protocols is difficult because they typically consist of complex behavioral characteristics, such as real-time, probabilistic, and cryptographic operations. To solve this problem, we propose a probabilistic timed calculus for cryptographic protocols, and demonstrate how to use this formal language for proving security or vulnerability of protocols. The main advantage of the proposed language is that it supports an expressive syntax and semantics, including bisimilarities that supports real-time, probabilistic, and cryptographic issues at the same time. Hence, it can be used to verify the systems that involve these three property in a more convenient way. In addition, we propose an automatic verification method, based on the well-known PAT process analysis toolkit, for this class of protocols. For demonstration purposes, we apply the proposed manual and automatic proof methods for verifying the security of DTSN and SDTP, which are two of the recently proposed WSN tranport protocols.

Category / Keywords: cryptographic protocols / Transport protocols for Wireless Sensor Networks, Security, Cryptographic protocol, Formal verification, Automated verification, Probabilistic Timed Calculus

Publication Info: This work has NOT been published anywhere

Date: received 9 Jan 2013

Contact author: thong at crysys hu

Available formats: PDF | BibTeX Citation

Version: 20130118:123817 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]