Information and Computation 226 (2013) 37–56

Contents lists available at SciVerse ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Signal-flow-based analysis of wireless security protocols

Çağatay Çapar [a], Dennis Goeckel [a], Kenneth G. Paterson [b,*], Elizabeth A. Quaglia [b], Don Towsley [a], Murtaza Zafer [c]

[a] University of Massachusetts, United States
[b] Royal Holloway, University of London, United Kingdom
[c] IBM T.J. Watson Research, United States

ARTICLE INFO

Article history:
Available online 7 March 2013

Keywords:
Security protocols
Wireless
Cost
Linear System
Physical layer
Key exchange

ABSTRACT

Security protocols operating over wireless channels can incur significant communication costs (e.g., energy, delay), especially under adversarial attacks unique to the wireless environment such as signal jamming, fake signal transmission, etc. Since wireless devices are resource constrained, it is important to optimize security protocols for wireless environments by taking into account their communication costs. Towards this goal, we first present a novel application of a signal-flow-based approach to analyze the communication costs of security protocols in the presence of adversaries. Our approach models a protocol run as a dynamic probabilistic system and then utilizes Linear System theory to evaluate the moment generating function of the end-to-end cost. Applying this technique to the problem of secret key exchange over a wireless channel, we quantify the efficiency of existing families of key exchange cryptographic protocols, showing, for example, that an ID-based approach can offer an almost 10-fold improvement in energy consumption when compared to a traditional PKI-based protocol. We then present a new key exchange protocol that combines traditional cryptographic methods with physical-layer techniques, including the use of "ephemeral" spreading codes, cooperative jamming, and role-switching. Utilizing signal flow analysis, we demonstrate that this new protocol offers performance advantages over traditional designs.

1. Introduction

With the wide proliferation of wireless devices, securing information sent over wireless channels is imperative and has rightfully received significant research attention. However, the focus of the design and evaluation of security protocols for wireless environments has been on traditional metrics of security, such as resilience against various attacks, key-sizes, computational complexity tradeoffs, etc. While these are important metrics, it is also equally important to consider the communication cost (energy, delay) of a security protocol, especially since wireless devices generally operate under strict resource constraints such as limited battery energy.

Inherently, communications over wireless channels is probabilistic in nature due to random errors caused by signal fading, shadowing, and noise, and due to potential adversarial attacks such as signal jamming, fake signal transmission, etc. Therefore, evaluating the end-to-end performance of a security protocol becomes especially difficult when considering

* Corresponding author.
E-mail addresses: ccapar@ecs.umass.edu (Ç. Çapar), goeckel@ecs.umass.edu (D. Goeckel), kenny.paterson@rhul.ac.uk (K.G. Paterson), Elizabeth.Quaglia.2008@live.rhul.ac.uk (E.A. Quaglia), towsley@cs.umass.edu (D. Towsley), mzafer@us.ibm.com (M. Zafer).

0890-5401/$ – see front matter
http://dx.doi.org/10.1016/j.ic.2013.03.004

a wireless setting. For example, suppose that a security protocol requires the exchange of certain messages over an open wireless channel that is subject to adversarial jamming. Since a message transmission can fail or the message can be corrupted, the protocol would in reality undergo multiple re-trials to deliver each message and/or require re-starts from different points. As the logical protocol flow is probabilistic, evaluating the end-to-end cost is non-trivial. Furthermore, depending on the protocol design, an attacker may be able to exploit the need for such multiple trials and re-starts and force a significant communication cost. Thus, though a cryptographic protocol may provide strong security guarantees, it may also be very inefficient in terms of average resource consumption when communication costs are accounted for. We therefore argue that an *important tradeoff for wireless security protocols is their efficiency measured in terms of the communication cost incurred versus the level of security achieved*.

In this paper, we utilize Linear System theory to develop a signal-flow-based approach to analyze wireless security protocols. The main idea here is to transform a protocol flow chart into a signal flow graph (by assigning probabilities and costs on individual branches) and then utilize reduction techniques to deduce the end-to-end transfer function, from which the end-to-end costs of the protocol can be computed. To concretely present this approach, we consider as a running example the fundamental problem of *secret key exchange over an open wireless channel in the presence of an active adversary*. This will provide an underlying context throughout the paper. We describe this problem next.

1.1. Wireless key establishment

Bootstrapping security over a wireless channel requires first establishing a jam-resilient communication channel, since otherwise open air transmissions are highly susceptible to disruption attacks such as signal jamming. An approach generally employed in this setting is to use spread-spectrum communications (e.g. Frequency-Hopping Spread Spectrum (FHSS)), which limits an attacker's ability to jam the communication signals without expending large amounts of energy [1]. However, establishing a spread-spectrum channel requires the participating parties to either already pre-share or securely establish a cryptographic key, enabling them to select a 'private' spread spectrum channel that is unknown to the attacker. In turn, this requires any pair of network nodes that might wish to establish jam-resilient wireless communication either to have available a pre-established key, or to run a key establishment protocol over an 'open' wireless channel prior to switching to a spread spectrum channel determined by the agreed key.

Consider first the case of using pre-established keys. If we consider the setting where we have a large number of network nodes that may wish to establish secure communications and where node compromise is a realistic threat – for example in a military environment or an emergency scenario – then having a single, system-wide pre-established key is not a viable solution, since compromise of a single node then compromises the whole network. On the other hand, having a unique pre-shared key per possible pair of communicating parties is not a good solution either, since it does not scale well and is inflexible once deployed. Intermediate solutions, such as those proposed in [2,3], scale better, but may still require substantial key storage at the nodes. Instead, establishing shared secret keys on-demand by utilizing cryptographic protocols over the open air is a more flexible approach and may, in fact, be necessary in many emergency and military scenarios.

There is a large body of research on cryptographic protocols for key exchange from public messages [4], but when employed over wireless channels the messages exchanged during key establishment are subject to active adversarial attacks. Because of adversarial attacks (as well as the inherently noisy communications environment), the protocol participants may be forced to repeat steps, or even re-start the protocol from scratch, many times before a session key is successfully established. This implies that establishing a private spread spectrum communications channel may incur significant energy costs, quickly draining battery energy for example. At the outset, it is not clear which protocols minimize energy consumption, or indeed what tradeoffs between security and costs are possible. Nor is it clear whether current classes of protocols for key exchange, designed mostly with wired networks in mind, are efficient for wireless networks, or whether alternative protocols optimized for the wireless environment are needed. Quantifying these costs is essential in selecting the best candidate protocol for a wireless environment.

1.2. Our contributions

1.2.1. Analysis method

Our first contribution is the introduction of an analysis method to study the cost of applying security protocols over wireless channels, which are typically subject to random packet losses. This method basically transforms the protocol flow chart into a signal flow graph (SFG) to enable systematic analysis. We refer to this method as the "SFG method" throughout the text. The SFG method has the following advantages: 1) The method is easy to use since it relies on simple widely-known techniques from Markov processes, and linear systems, yet it is general enough so that any security protocol that runs through random retransmissions (due to bad connectivity, hostile environment, etc.) can be analyzed with the SFG method. 2) The method is flexible enough to accommodate changes such as changing strategy of system nodes, fine tuning of costs, etc., by adding more nodes and branches to the SFG. 3) The method completely characterizes the distribution of the overall cost, so it can provide any statistics of interest (expected cost, variance, tail probability), and most importantly, it enables a transparent view of how the underlying security protocol affects the overall cost which provides valuable insight as described next.