Computer Networks 84 (2015) 46–63

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

ESC: An efficient, scalable, and crypto-less solution to secure wireless networks

Roberto Di Pietro [a], Gabriele Oligeri [b,*]

[a] Bell Labs, Paris, France University of Padua, Maths Department, Padova, Italy
[b] Department of Mathematics and Physics Università di Roma Tre, Roma, Italy

ARTICLE INFO

Article history:
Received 13 February 2014
Revised 24 March 2015
Accepted 1 April 2015
Available online 18 April 2015

Keywords:
Communication system security
Cryptoless protocols
Wireless communications
Key establishment
Anonymous channels

ABSTRACT

In this paper we present ESC: an efficient, scalable, and crypto-less solution for the establishment of a secure wireless network (that is, a network where, for any pair of nodes, there exists a path composed of encrypted links).

ESC guarantees the security of the 90% of the network scenario in the presence of 4 global eavesdropper adversaries with about 370 local peer-to-peer communications avoiding both pre-shared secrets and cryptographic functions.

The founding block of our proposal is inspired by COKE [1], where the bits of the secret key associated to a link are generated via a multi-round protocol that, at each round, leverages just channel anonymity.

Starting from this founding block, we further provide several relevant contributions: we devise a theoretical model and prove a lower bound for the probability to establish a safe-link in the presence of a global eavesdropper adversary. Further, we study the emergent property of network security achieved via the local property of safe-link establishment. To characterize this feature, we introduce two intuitive and useful metrics: *network safety* and *largest safe component*, both aimed at capturing the security features provided by ESC.

The thorough theoretical analysis of our proposal, the security proof (under the Canetti–Krawczyk model) supporting our key establishment protocol, as well as our extensive simulations showing the effectiveness and efficiency of our protocol for a wide range of network configuration parameters, make our proposal a viable solution to enforce the security of real networks, other than paving the way for further research in this field.

1. Introduction

Securing communications of wireless devices is a challenging issue [2–4]. In particular, secure communications in wireless networks strongly rely on the effectiveness of key distribution schemes. Many solutions have been proposed in order to cope with this problem, and they can be roughly divided into two main families: key pre-distribution schemes [5,6] and over-the-air key establishment protocols [7]. Predistribution of secret keys mainly relies on loading the nodes, prior to their deployment, with a set of secret keys. There are two naïve solutions to this problem: loading on all the nodes a common master key, or loading $N-1$ secret keys in each of the N nodes in such a way that each pair shares a unique common secret. Both solutions have major drawbacks [6]. Between these two extreme solutions, there are the probabilistic key pre-distribution schemes, such as [6]

[*] Corresponding author. Tel.: +39 3490841051.
E-mail addresses: roberto.di_pietro@alcatel-lucent.com (R. Di Pietro), oligeri@mat.uniroma3.it (G. Oligeri).

http://dx.doi.org/10.1016/j.comnet.2015.04.006
1389-1286/© 2015 Elsevier B.V. All rights reserved.

and [5], in which nodes are pre-loaded with a subset of keys drawn by a shared pool of keys. After the deployment phase, each pair of nodes probabilistically shares a common secret key. As for over-the-air key establishment protocols, we distinguish between asymmetric techniques and cyber-physical approaches. Asymmetric crypto techniques allow to establish secret keys without relying on pre-deployment procedures: after the deployment, nodes cooperate in order to share pairwise secrets among their neighbors. Asymmetric cryptographic schemes, such as [8], turn out to be particularly expensive from the energy perspective due to their high computational overhead [1,9]. Cyber-physical solutions provide real-time key establishment leveraging physical phenomena such as the received signal strength and the multipath fading. Interesting solutions are provided in [10] and [7]: the authors propose to extract shared secrets from the observation of the received signal power (RSS) at both the peers.

A different approach leveraging anonymous channels was introduced for the first time in [11] and subsequently improved by [12]. The main idea relies on establishing a secret key between two peers without using crypto functions but leveraging source indistinguishability of an anonymous channel [9]. Recently, authors in [1] presented COKE: a crypto-less over-the-air key establishment protocol. COKE allows just two wireless communicating parties to commit on a shared secret, even in the presence of a globally eavesdropping adversary. Yet, the authors proved the security of the proposed solution by means of a theoretical model supported by extensive simulations.

1.1. Contribution

In this work we present ESC: an efficient, scalable, and crypto-less solution to secure wireless networks. ESC is inspired by COKE [1]: ESC leverages channel anonymity to build up a peer-to-peer key establishment protocol and provides security at a network level, even in presence of multiple adversaries. In particular, we derive a theoretical lower bound for the security provided by our solution and support our findings with extensive simulation results. All the parameters (e.g. key length, resilience assurance probability) of ESC are completely tunable. Simulations also show the viability of our proposal—the introduced overhead is negligible. For instance, given 4 pre-deployed global eavesdropper adversaries, ESC guarantees that 90% of the network links are safe (protected by a 96 bits secret key) with about 370 local communications for each pair of neighboring nodes in the network. Moreover, we provide a formal proof of the protocol under the Canetti–Krawczyk model [13]. Finally, further research directions are also highlighted in the conclusion.

1.2. Organization

Next section surveys related work in the area. Section 3 shows how to leverage channel anonymity to build-up a key-establishment protocol, introduces our solution (ESC), and depicts the network scenario. In Section 4 we present the details of the ESC protocol, while in Section 5 we introduce the security analysis at link level: starting from the safe-bit probability, we derive a theoretical model for the safe-link probability and prove a lower bound for the overall security of the network. In Section 6 we provide the security analysis at network layer. In particular, we introduce two intuitive and useful metrics to assess the security of the ESC protocol, namely *network safety* and *largest safe component*. Finally, the protocol resiliency against multiple adversaries is shown in Section 7, while in Section 8 we present a formal security proof of the COKE protocol and in Section 9 we report some concluding remarks.

2. Related work

A seminal solution to key-distribution in wireless network was provided by Eschenauer and Gligor [6], and further extended in [5]. In these solutions, enough symmetric keys are pre-loaded on each node so that any two nodes, after deployment, share a key with a given probability. The proposed model has been refined and tight, closed results about its resilience to compromising appeared in [14]. In [15], authors presented two extremely efficient algorithms for key establishment in distributed environments, namely key infection and key whispering. They argued that a real world adversary: (i) is not likely to be deployed in advance in the network scenario; (ii) it has local eavesdropping capabilities; and finally, (iii) it has a completely passive behavior, i.e., no active attacks such as jamming or flooding are played. Nevertheless, we observe that in many scenarios, e.g. military, the target deployment area may be known in advance by both the network owner and the adversary. In order to deal with a pre-deployed adversary, only few solutions have been proposed. In fact, to be resilient to a pre-deployed eavesdropper, the devices must rely on a shared secret to be leveraged for the subsequent (online) computations and communications [14]. There are also solutions that leverage just path diversity [48,49], but they require that the adversary is not a global eavesdropper. Another solution comes from asymmetric cryptographic primitives, such as [16], nevertheless, asymmetric crypto is computationally expensive, and therefore, not suitable for massive devices deployment such as wireless sensor networks or devices that, once deployed, will be substantially unattended—operating life being at premium. On-line key establishment without leveraging asymmetric crypto is a challenging issue that can be solved in mainly two ways: RSS based key establishment [7] or by means of anonymous channels [1,11,12]. The former solves the key establishment issue by transforming the observation of the RSS values in a shared secret: it has been proved that the received signal power estimated at both the peers of a communication link can be “transformed” on a shared secret between the two peers. In this case, the key-establishment is protected against a pre-deployed adversary: the RSS experienced by the adversary is as much as different as its position differs from the position of both the two peers. However, these solutions are exposed to recently introduced attacks [17]. Other solutions leverage anonymous channels [1]: the sender is anonymous, and the secret key is established as a function of the sender identity (ID) by a sequence of anonymous transmissions. The adversary easily eavesdrops the transmitted bits but cannot (deterministically) infer on the source identity, and therefore the key is (probabilistically) secure.