Ad Hoc Networks 12 (2014) 193–200

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

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

Information security for sensors by overwhelming random sequences and permutations ☆

Shlomi Dolev [a],*, Niv Gilboa [a], Marina Kopeetsky [b], Giuseppe Persiano [c], Paul G. Spirakis [d]

[a] Department of Computer Science, Ben-Gurion University of the Negev, Beer-Sheva 84105, Israel
[b] Department of Software Engineering, Sami-Shamoon College of Engineering, Beer-Sheva 84100, Israel
[c] Dipartimento di Informatica ed Applicazioni, Università di Salerno, Via Ponte Don Melillo Salerno, 84084 Campania, Italy
[d] Department of Computer Engineering and Informatics, University of Patras and Research Academic Computer Technology Institute, N. Kazantzakis str., University Campus, 265 00 Rio, Patras, Greece

ARTICLE INFO

Article history:
Received 3 March 2011
Accepted 15 September 2011
Available online 7 November 2011

Keywords:
Security
Wireless
Secret creation

ABSTRACT

We propose efficient schemes for information-theoretically secure key exchange in the Bounded Storage Model (BSM), where the adversary is assumed to have limited storage. Our schemes generate a secret One Time Pad (OTP) shared by the sender and the receiver, from a large number of public random bits produced by the sender or by an external source. Our schemes initially generate a small number of shared secret bits, using known techniques. We introduce a new method to expand a small number of shared bits to a much longer, shared key.

Our schemes are tailored to the requirements of sensor nodes and wireless networks. They are simple, efficient to implement and take advantage of the fact that practical wireless protocols transmit data in frames, unlike previous protocols, which assume access to specific bits in a stream of data.

Indeed, our main contribution is twofold. On the one hand, we construct schemes that are attractive in terms of simplicity, computational complexity, number of bits read from the shared random source and expansion factor of the initial key to the final shared key. On the other hand, we show how to transform any existing scheme for key exchange in BSM into a more efficient scheme in the number of bits it reads from the shared source, given that the source is transmitted in frames.

1. Introduction

1.1. State of the art

A major building block in security and cryptography is generating a secret that two parties share. The secret may then be used as a symmetric encryption or authentication key.

We propose a scheme to generate a shared key in the Bounded Storage Model (BSM). The Bounded Storage Model was presented in Maurer's work [11]. This model investigates cryptographic tasks such as encryption and authentication in the presence of an adversary that has bounded storage capacity. While most of modern cryptography limits an adversary's resources, the usual approach is to place a bound on the adversary's time complexity. Given various unproven assumptions on the hardness of computational tasks, modern cryptography has many beautiful constructions of schemes that are secure against an adversary that has limited time complexity.

In the Bounded Storage Model, on the other hand, there is no need for computational assumptions. Given a source

☆ Partially supported by the ICT Programme of the European Union under Contract Number FP7-215270 (FRONTS), Microsoft, NSF, Deutsche Telekom, Rita Altura Trust Chair in Computer Sciences, Lynne and William Frankel Center for Computer Sciences, and the internal research program of Sami Shamoon College. An Extended Abstract of these work was presented in *ACM DIALM-POMC* 2010.

* Corresponding author.

E-mail addresses: dolev@cs.bgu.ac.il (S. Dolev), niv.gilboa@gmail.com (N. Gilboa), marinako@sce.ac.il (M. Kopeetsky), giuper@dia.unisa.it (G. Persiano), spirakis@cti.gr (P.G. Spirakis).

1570-8705/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2011.09.002

of random bits that broadcasts more traffic than the adversary can store, legitimate parties can perform cryptographic tasks in a way that is information-theoretically secure. This is true even if the storage of the legitimate parties is smaller than that of the adversary.

One of the main tasks in cryptography is for two parties to share a key, without leaking any of its bits to an adversary that monitors traffic. [11] showed that in the BSM a key can be shared with information-theoretic security even when the two parties do not share any bits before the protocol begins. This work was improved by Cachin and Maurer [3] that presented a protocol in which the sender and the receiver each choose a small set of locations from the random string and then store the bits in these locations. After the transmission of the random string ends, they exchange their chosen locations. Each shared location is associated with a shared bit. By the birthday paradox, the storage requirement is proportional to $\sqrt{n}$. The analysis of this protocol by Dziembowski and Maurer [7] shows that it is essentially optimal in terms of the amount of data the two parties can share, given the ratio between the storage capacity of the adversary and the storage capacity of the two legitimate parties.

Subsequent works [1,4,6,10,12] presented schemes to expand a shared but short initial key to a much longer key that can be used as a One Time Pad (OTP). Both the initial key and the OTP are shared by the legitimate parties, but are unknown to the adversary. It is assumed that the adversary has no information on the initial key with probability 1, while the probability that it has some information on the one-time pad is less than some parameter ϵ.

1.2. Our contribution

We propose a pair of two-stage schemes that first use the process for initial key generation of Cachin and Maurer [3] to generate a short, shared key. The schemes then employ a novel method for expanding a short initial key into a longer key. Our schemes have the basic property of key exchange protocols that passive attackers, who only monitor traffic, do not obtain information on the shared key, while active attackers may mount Man-in-the-Middle attacks. Typically, such active attacks are foiled by an authentication process, distinguishing between non-corrupted and corrupted nodes. We note that authentication of a wireless node for which a shared secret should be established may be based on physical identification (e.g., [2]).

The schemes we present are applicable to any setting in which two parties wish to share key, while the adversary has bounded storage. Both schemes are especially attractive in sensor networks for several reasons. The low computational complexity of our schemes makes them a good alternative to traditional cryptography in terms of computational resources and power source requirements for a sensor. Additionally, the simplicity of our schemes ensures compact implementation in software. Finally, the natural use we make of frames in practical communication protocols, which are in use in sensor networks, makes them often more efficient than other BSM protocols (see below for details).

The basic step of our schemes is to use the initial key for both the sender and the receiver to select several blocks of bits from the shared random source. After all the random bits have been transmitted, the sender chooses a random permutation on all the stored bits and exchanges it with the receiver. After permuting the bits, both parties exclusive-or all the bits in a contiguous block of bits, thus obtaining a single bit of the OTP. Given enough such blocks, they construct the whole OTP.

We present two protocols, the *Permutation Revealing Protocol* PRP and *Permutation Encrypted Protocol* PEP. The permutation in PRP is sent as clear text, deriving a single OTP from a shared random string of length n. In order to obtain another OTP, the two parties must perform the full key exchange protocol again. In PEP the permutation is kept secret forever. Thus, PEP may be used with the same permutation to derive an exponential number of One Time Pads.

We use the following notation: k denotes the security parameter which means that all schemes are information-theoretically secure with probability at least $1 - \epsilon = 1 - 2^{-k}$. The length of the random string is denoted by n and the length of the OTP is denoted by m.

We view the random string as a matrix, where the number of columns is $m(k + \log m)$ and the number of rows is denoted by b and is equal to $n/m(k + \log m)$. We refer to the parameter b as the number of channels. A physical implementation of the random source may allow transmission in parallel over b channels in our protocol. If the implementation does not allow such parallel transmission, the b channels just define sections of size $m(k + \log m)$ bits within the n-bit random string.

We use the fact that wireless protocols transmit data in frames of several bits together for various reasons such as efficiency and error correction. The transmission of a shared random string requires just such a wireless protocol and we denote the frame length of this protocol by α bits.

The complexity of PRP under various measures is as follows. The computational complexity is $m(k + \log m)$. The number of bits read from the random source is $\lceil \frac{m}{\alpha} \rceil \alpha(\log m + k)$. The expansion factor, which is defined as the ratio between the initial secret (the product of the first stage of the protocol) and the OTP length m is $\frac{m}{\log b(\log m + k)}$. The storage required for the second stage of PRP is $O(m(k + \log m))$. The storage required for the first stage is $O(\sqrt{n})$ bits, see [3] for a detailed analysis.

In addition to the two novel protocols we construct we also describe a generic transformation of a key exchange scheme that accesses distinct bits in the random strings into a scheme that accesses blocks of bits (where each block is identified with a frame of the wireless protocol). Such a transformation is useful for any practical wireless protocol, in which data is sent and received in such frames. The transformation reduces the number of bits that each party reads from the random source. Applied to Vadhan's scheme [12], in which the number of bits a party reads is the least of all known schemes, we obtain a scheme that reads $k + \log m$ bits (compared to $k + \log n$).

1.3. Comparison with previous work

In all of the works that expand an initial shared key to a longer shared OTP, [1,4,7,10,12], the main measure of a