Pervasive and Mobile Computing 41 (2017) 83–105

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Secure communication through jammers jointly optimized in geography and time☆

Yair Allouche [a], Esther M. Arkin [b], Yuval Cassuto [c], Alon Efrat [d], Guy Grebla [e], Joseph S.B. Mitchell [b], Swaminathan Sankararaman [g], Michael Segal [a,*]

[a] Department of Communication Systems Engineering, Ben-Gurion University, Beer-Sheva, Israel
[b] Department Applied Mathematics and Statistics, Stony Brook University, Stony Brook, NY 11794, USA
[c] Department Electrical Engineering, Technion–Israel Institute of Technology, Haifa 32000, Israel
[d] Department of Computer Science, The University of Arizona, Tucson, AZ 85721, USA
[e] Department Electrical Engineering, Columbia University, New York, NY 10027, USA
[g] Akamai Technologies, 150 Broadway, Cambridge, MA 02142, USA

ARTICLE INFO

Article history:
Received 17 March 2017
Received in revised form 5 June 2017
Accepted 24 July 2017
Available online 5 August 2017

ABSTRACT

Security-sensitive applications, such as patient health monitoring and credit card transactions, are increasingly utilizing wireless communication systems, RFIDs, wireless sensor networks, and other wireless communication systems. The use of interference-emitting jammers to protect such sensitive communication has been recently explored in the literature, and has shown high potential. In this paper we consider optimization problems relating to the temporal distributions of jammers' activity, and the suitable coding regimes used for communication. Solving the joint problem optimally enables comprehensive security in space, at a low power consumption and low communication overhead. The joint optimization of jamming in space and time is driven by a new framework that uses the *bit-error probability* as a measure of communication quality. Under this framework, we show how to guarantee information-theoretic security within a geographic region, and with increased flexibility to tailor the coding regime to the problem's geometry. We present efficient algorithms for different settings, and provide simulations for various scenarios using the bit-error probability functions. These simulations demonstrate the efficiency of the scheme. We believe that our scheme can lead to practical, economical and scalable solutions for providing another layer of protection of sensitive data, in cases where encryption schemes are limited or impractical.

1. Introduction

More and more, highly sensitive and private information is being transferred via wireless communication. Example systems include contactless smart cards [1], military sensor networks [2], emergency response systems employing wireless networks [3], and ambient living-assistance systems [4]; these systems use wireless communication to transmit banking/financial data, military intelligence, medical data from patient monitoring, and other private information. The open nature of the wireless medium mandates that precautions be taken to protect the privacy of information, e.g., from potential

☆ Extended abstracts of this paper appeared as parts in Allouchelu et al. (2015) [5] and Arkin et al. (2015) [6].

* Corresponding author.
E-mail address: segal@cse.bgu.ac.il (M. Segal).

http://dx.doi.org/10.1016/j.pmcj.2017.07.011
1574-1192/

eavesdropping. Unprotected communication, e.g. within sensor networks, also opens the door for various types of attacks on the network, such as sensor impersonation, sybil attacks and wormhole attacks.

Communication devices, such as RFID devices in smart cards, have limited computational capabilities, making cryptographic techniques impossible. Further limitations may come from application constraints, in which, e.g., emergency personnel are unable to enter passwords or use authentication methods to secure data transfer. To make the situation more complex, there may be multiple types of communication nodes, utilizing different frequencies, and the nodes may be changing over time, as nodes are removed or added or become mobile; thus, we are motivated to pursue security techniques that are impervious to variations in the structure of the system or the network.

Wireless jamming has been explored as a means of achieving security from eavesdroppers through the selective introduction of artificial noise [5–8]. In addition to making sure the eavesdropper's channel quality is degraded sufficiently, the quality of legitimate channels must not be compromised. This additional constraint marks a contrast between friendly jamming and traditional offensive jamming.

Sensitive communication may be on single or multiple frequencies and it is often imperative to secure all frequencies. In such scenarios, channel degradation at eavesdroppers may be achieved through several jamming techniques [9]. Some examples are *barrage jamming*, which transmits noise on all frequencies continuously, *narrowband jamming*, which is restricted to a single frequency, and *pulse jamming*, which sends periodic bursts of noise.

In many cases, legitimate communication is restricted to within a geographic region such as a warehouse, hospital or bank and must be protected from eavesdroppers outside this region. For example, consider a bank or hospital where highly sensitive information such as financial or health data is transmitted within a physically restricted area and wireless communication of such information must be protected from eavesdroppers outside this restricted area. Persons may be communicating sensitive information using a mixture of mobile and static devices; e.g., a doctor may scan a patient's health monitor through their smartphone and transmit elsewhere. The area itself is physically restricted but needs to be shielded from eavesdroppers in the outside world.

Since the communication inside the region may be highly dynamic, i.e., nodes may be mobile or may be added/removed, it is of interest to have jammers only use minimal information about the communication taking place in order to intelligently configure themselves. In addition, the existence of only minimal information implies that jammers must be proactive rather than reactive, i.e., they cannot synchronize themselves with legitimate transmissions, nor with each other. Moreover, jammers do not need to have a (common) clock, and synchronization is not required. These assumptions render a collections of such jammers highly dynamic and easily adaptable to changes in the environment they protect. However, we do assume (and actually take advantage of) that jammers could produce noise for some portion of the time (affecting only a subset of the bits in a transmitted message), and burst distributions could be controlled by the user. These temporal jammers fall under the category of pulse jammers in [9].

We argue that temporal jamming has multiple advantages over continuous jamming in eavesdropping mitigation:

1. *Randomness*: The inherent randomness of the duration and timing of the bursts indicates the difficulties in studying their behavior (limited only by our ability to obtain a source of "true randomness").
2. *Energy savings*: Guaranteed jamming can be achieved with low operation duty cycles.
3. *Simplicity*: Jammers can be fixed-power, and flexibly placed in space.
4. *Spatial separation:* A single-radio jammer can be active on different frequencies at different times, thus being able to secure multi-frequency communications.
5. *Robustness*: Temporal jamming is significantly more difficult to cancel at the eavesdropper's receiver, due to their bursty nature.
6. *Feasibility:* There are examples where successful jamming that provides full privacy (in the formal meaning defined below) is not possible with a given set of continuous jammers, and yet, with random temporal jamming, it is possible.

A central benefit of temporal jamming we explore in this paper is the possibility to employ advanced unconditionally secure coding techniques. Operating the jammers in the time domain allows us to reason about their effect on the most fundamental information unit: a single bit. Therefore, existing jamming optimization techniques can be complemented by coding performed on the transmitted information. When designed together, coding and intelligent jammer layout using the geometry of the environment can simultaneously provide reliable communication for legitimate nodes and unconditional privacy from eavesdropping.

Problems statement. In this paper, we adopt the above approach and consider the combined problem: How should one select the fractions of time in which temporal jammers are active and transmitting noise to secure communication, and at which coding regime does this information needs to be communicated. The solution to this problem relies upon three important elements: a new framework for modeling temporal jamming using bit-error probabilities, a geometric optimization algorithm, and information theoretic definitions of reliable and secure communication. The geometric optimization problem aims at minimizing the total jamming power required to achieve reliability and secrecy constraints given the problem's geometry. It is important to note that the output of this optimization is some set of minimal activity fractions for all jammers, whose deployment does *not* require coordination between jammers on when to transmit.

We consider different aspects of the optimization problem that address how to optimize (temporal or fixed-duration) jammers' effectiveness through intelligent placement. We believe that this would pave the way to global all-parameters optimizations.