Computer Networks 116 (2017) 33–46

Contents lists available at ScienceDirect

Computer Networks

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

Enabling broadcast communications in presence of jamming via probabilistic pairing

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

[a] Nokia Bell Labs, Paris, France
[b] Università di Padova, Math Department, Padova, Italy
[c] KINDI Center for Computing Research, Qatar University, Doha, Qatar

ARTICLE INFO

Article history:
Received 28 March 2016
Revised 12 February 2017
Accepted 15 February 2017
Available online 16 February 2017

Keywords:
Jamming mitigation
Wireless networks
Broadcast communications

ABSTRACT

This paper presents a thorough analysis of Freedom of Speech (FoS): a lightweight, fully distributed, and probabilistic protocol that assures the delivery of a message to be broadcast notwithstanding the presence of a jammer.

FoS enjoys several features when compared to competing schemes: (i) it requires each node to store only N symmetric pairwise keys; (ii) node joining and node eviction require just minimal intervention on the already operating nodes; and, finally, (iii) it is overall highly efficient in terms of required computation and message exchange.

We provide a detailed theoretical analysis of our solution supported by extensive simulations considering different operating scenarios: we start from a simplified network assumption of one only transmitter that wants to broadcast a message and we subsequently move to a realistic scenario where nodes that have received the message act themselves as a proxy.

We propose a theoretical framework to model the protocol performance starting by a benign scenario (no jamming activities). Later, we extend the model to more hostile environments considering firstly a jammer with no knowledge of the nodes' secret keys (external jammer) and subsequently, a jammer aware of a fraction of the nodes' secret keys (internal jammer). The experimental results do confirm our theoretical analysis and show the overall viability of our solution. In particular, FoS outperforms competitor solutions for deployment scenarios characterized by even a moderated degree of node volatility.

1. Introduction

In recent years, wireless communications have become the enabling technology for the majority of the communication infrastructures and solutions, e.g., mobile phones networks, vehicular networks, wearable networks and SCADA systems. In such architectures, preventing legitimate communication among devices by using a malicious radio transmitter (jamming) [1] can be very harmful, in particular for critical infrastructures such as airports, hospitals, power plants, etc.

While jamming was originally a warfare technology adopted to prevent enemy communications, nowadays it is a cheap to implement ready-to-use technology, due to the advent of software defined radios (SDRs) [2], which are also becoming more and more powerful and cheap. SDRs represent the enabling technology to easily and quickly implement virtually any communication system via software, while being an unprecedented opportunity for researchers and developers, SDRs are also a potential threat for all the critical functionalities relying on wireless technologies.

Jamming is an effective Denial of Service (DoS) attack for wireless channels [3,4]. The act of jamming is as simple as effective: an adversary ($\mathcal{ADV}$), generates a continuous noise-signal with sufficient high power in the proximity of a wireless network [5,6]. As a result, the jammer and the sender signals collide at the receiver, and the communication between the transmitter and the receiver is disrupted.

Many recent papers have highlighted the simplicity and the effectiveness of jamming. In [7], authors investigate different jamming techniques in order to find the most effective one against OFDM modulation scheme. Similarly, in [8] authors propose a study of the jamming effectiveness against multiple-input-multiple-output (MIMO) antenna systems. In [9], authors show

[*] Corresponding author.
E-mail addresses: roberto.di_pietro@nokia-bell-labs.com, dipietro@math.unipd.it (R. Di Pietro), goligeri@qu.edu.qa, gabriele.oligeri@gmail.com (G. Oligeri).

http://dx.doi.org/10.1016/j.comnet.2017.02.010
1389-1286/© 2017 Published by Elsevier B.V.

the effectiveness of jamming on vehicular networks being able to completely block the communications even with low power levels of jamming. Over the past years, many techniques have been developed in order to thwart jamming attacks. Preliminary work focused on spread spectrum techniques: Direct Sequence Spread spectrum (DSSS) [10], Frequency Hopping Spread Spectrum (FHSS) [11], and Chirp Spread Spectrum (CSS) [12]. All the previous techniques need a network-wide shared secret in order to generate the same spreading sequences, hopping patterns, or timing of pulse, respectively. The above solutions are ineffective when an adversary is able to compromise a subset of the network devices. Indeed, after compromising a device, the adversary acquires the necessary information (secrets) to successfully target the network communications.

An interesting solution that avoids network-wide secrets was introduced in [13]. There, the authors proposed an Uncoordinated DSSS (UDSSS): network nodes do not need any shared secrets, but the spreading sequence is randomly chosen from a public dictionary. In fact, the sender spreads the message with a random sequence and sends it to the receiver. In turn, the receiver records the signal on the channel and de-spreads it by applying all the sequences from the public dictionary using a trial-and-error-method. This solution turns out to be effective but not efficient: the sender needs to re-transmit the message many times and the receiver has a high computational and communication overhead.

Finally, authors in [14] introduced the Time Delayed Broadcast Scheme (TDBS): the broadcast communication is achieved by means of a sequence of unicast communications—sometimes assisted by proxies. The solution relies on long frequency hopping sequences that are pre-loaded in each node belonging to the network before nodes deployment.

Our contribution: In this paper we provide a complete solution (Freedom of Speech - FoS) to mitigate jamming in broadcast communications. In particular, we consider first a baseline scenario where an elected node wants to broadcast a message to all its neighbors, and a second, more realistic scenario, in which we consider a network where each of the nodes that have received the correct message, contribute to the broadcast process acting as a proxy.

For both the above scenarios, we proved FoS to be robust to two kinds of adversaries: the *external* adversary and the *internal* adversary. Both of them are able to randomly jam a subset of the communication frequencies, but the latter has also the capability of disclosing the secrets of a subset of the network nodes. Therefore, it can leverage these secrets to enhance the effectiveness of its jamming activity.

Moreover, we provide a theoretical framework for the analysis of the protocol performance in both the benign and jammed scenario and also extensive simulation results that confirm our theoretical findings. Finally, we compare FoS against a competing state-of-the-art solution, and we show that while FoS is overall viable for a wide range of system parameters, it outperforms the competition for deployment scenarios where nodes have an even moderated degree of volatility.

Paper organization: Next section surveys related work in the area; Section 3 introduces both the communication model and the adversarial model, while Section 4 provides a deep analysis of the TDBS protocol. Section 5 introduces FoS, while Sections 6 and 7 show the performance of FoS in the non-cooperative and cooperative scenarios, respectively, with a few highlights in Section 8. Finally, Section 9 presents a detailed comparison between FoS and TDBS (this latter one representing the state-of-the-art solution for the given context), and Section 10 reports some concluding remarks.

2. Related work

In [15], authors showed that even considering an $\mathcal{ADV}$ with a cheap hardware it is easy to choose a location and a power level so that it can effectively corrupt either a bit or a whole packet. In [16], authors proposed a Randomized Differential DSSS (RD-DSSS) scheme to achieve anti-jamming broadcast communication without shared keys. In fact, traditional anti-jamming techniques, such as FHSS and DSSS, require that senders and receivers share a secret key in order to communicate with each other. Such a technique turned out to be ineffective if the adversary learns the shared key from a compromised or malicious receiver, since it can disrupt the reception at normal receivers. RD-DSSS encodes each bit of data using the correlation of unpredictable spreading codes. Nevertheless, RD-DSSS has a not-negligible computational and storage overhead that makes it unfeasible for resource-constrained devices.

Authors in [17], proposed an Uncoordinated Frequency Hopping (UFH) scheme where, in order to achieve jamming resistance, both the sender and the receiver randomly choose the communication channel for message transmission without coordination. The successful reception of a packet is achieved when the two nodes reside at the same frequency (channel) during the same time slot. Nevertheless, UHF needs that the nodes are able to store few megabytes of data and can efficiently perform ECC-based public key cryptography.

In [18] authors further improved the performance of UFH based communication. They jointly consider adaptive frequency hopping and power control and pose these two techniques into an uniform framework. They introduced online learning theory for decision making based on the history of channel variations. Data communication becomes a power game between the sender and the jammer, each one trying to beat the other one by transmitting a signal with a power level greater than the opposite side. The successful reception of packets depends on the link budgets of the sender-receiver pair, jammer-receiver pair, and the signal-to-noise ratio at the receiver side.

In [19], authors present a code-controlled frequency hopping scheme to mitigate jamming. By exploiting the redundancy provided by the block coding, the receiver can retrieve the hopping pattern without a priori knowledge and by leveraging an integrated decoding-and-encoding process, it can also perform partial jamming detection.

In [20], authors propose to transmit an ID sequence along with the information stream. The ID sequence is generated through a cryptographic algorithm using the shared secret between the transmitter and the receiver. It is then exploited by the receiver for effective signal detection and extraction. Authors prove the solution to be robust under jamming and effective disguised jamming.

Another frequency hopping technique is proposed in [21]. Authors combine frequency hopping and transmission rate adaptation to design a model for a power-constrained reactive-sweep jammer who aims at degrading the throughput of the wireless link.

A cooperative anti-jamming technique has been proposed in [22]. Authors investigated a cooperative anti-jamming scheme designed to enhance the quality of links degraded by jammers. To achieve this objective, users are allowed to cooperate at two levels. First, they cooperate to optimally regulate their channel access probabilities so that jammed users gain a higher share of channel utilization. Second, users leverage multiple-input single-output cooperative communication techniques to enhance the throughput of jammed links.

In [23] and [24], authors propose a generalized version of the existing iterative water-filling algorithm whereby the users and the jammer update their power allocations in a greedy manner. Indeed, authors considered a scenario in which K users and a jammer share a common spectrum of N orthogonal tones. Both the