Computer Communications 86 (2016) 75–85

Contents lists available at ScienceDirect

Computer Communications

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

Jammer localization in wireless networks: An experimentation-driven approach☆

Konstantinos Pelechrinis[a,*], Iordanis Koutsopoulos[b], Ioannis Broustis[c], Srikanth V. Krishnamurthy[c]

[a] University of Pittsburgh, United States
[b] AUEB, Greece
[c] UC Riverside, United States

ARTICLE INFO

Article history:
Received 8 August 2015
Revised 7 March 2016
Accepted 17 April 2016
Available online 23 April 2016

Keywords:
Wireless networks
Jamming attacks
Gradient descent
Location discovery
Testbed experimentation

ABSTRACT

Jamming attacks have become prevalent during the last few years facilitated by the open access to the shared wireless medium as well as the increased motivation and easiness to create damage as a result of sophistication of wireless devices, both legitimate and jamming ones. Among the challenges that a wireless network faces while trying to confront the jammer, jammer localization is of utmost importance. This entails estimating the physical location of the jammer. Successful jammer localization can trigger a series of corrective measures to ensure sustainable network operation. However, locating the jammer is a difficult problem. Our primary goal in this paper is to design a simple, lightweight and generic approach for localizing a jamming device through a set of measurable parameters. The key observation guiding our design, is that the Packet Delivery Ratio (PDR) that can be readily measured locally by a device decreases as a receiver moves closer to the jammer. Further, we draw on the gradient-descent principle from optimization theory, and we adapt it to operate on the discrete plane of the network topology so that the jamming device location can be estimated. The very nature of the gradient-descent algorithm allows the distributed execution of our localization scheme. In this paper, we compute and experimentally validate the impact of jammer on the PDR of a link and we show that this impact decreases as the link moves away from the jammer. We further design a distributed, lightweight jammer localization system, which does not require any modifications to the driver/firmware of commercial NICs, while we implement a prototype system to evaluate our scheme on our 802.11 indoor testbed. Finally, we evaluate the performance of our system via extensive simulations in larger scale settings. Its performance in terms of average location estimation error in combination with its simplicity and distributed operations hold great promise.

1. Introduction

The widespread proliferation of 802.11 wireless networks makes them an attractive target for various types of attacks [1–3]. Its open access nature makes it fairly easy for saboteurs with jamming devices [4,5] to disrupt WiFi communications. A jamming device continuously emits electromagnetic energy on the medium. Numerous jamming attacks have been reported in the recent past [6–9]. The effect of this behavior on a CSMA/CA network is twofold: **(a)** at the transmitter side it renders the medium busy resulting in large back-off times and, **(b)** at the receiver side, it dramatically decreases the SNR resulting in a large number of packet collisions. Jamming effects may also occur due to accidental activation of devices that do not serve a malicious cause, such as microwave ovens, cordless phones [10], etc. Following the detection of the presence of an attacker [11], localizing the jammer allows an administrator to pursue further countermeasures (such as deactivating the jamming device, isolating the attacker and capturing, punishing or even destroying it).

In this work, we design and implement a simple, lightweight approach for jammer localization. The main attribute of our approach that makes it attractive to use and straightforward to implement, is that it relies on Packet Delivery Ratio (PDR), a metric that is readily available at each node and is an indication of transmission corruption. Our technique exploits an intrinsic

☆ An earlier version of this work has appeared in IEEE Globecom 2009.

* Corresponding author. Tel.: +195182244780.
E-mail addresses: kpele@pitt.edu (K. Pelechrinis), jordan@aueb.gr (I. Koutsopoulos), broustis@cs.ucr.edu (I. Broustis), krish@cs.ucr.edu (S.V. Krishnamurthy).

http://dx.doi.org/10.1016/j.comcom.2016.04.009
0140-3664/

characteristic of the wireless medium: since the power of the jamming signal degrades with distance, farther transmitters do not sense strong jamming signals. As a consequence, the requirements for successful packet delivery at such transceivers are satisfied. This property cannot be manipulated by an attacker. A transceiver pair located further away from a jammer is more likely to be successful in exchanging packets; the transmitter is able to send more packets, while the receiver can decode more of those, due to increased SINR, resulting in an increased PDR.

Taking this property into account we design a simple localization algorithm, that borrows its rationale from the gradient-descent method in a continuous-valued variable space. Our algorithm starts from an initial node and terminates at another node, that is closer to the jammer than any of its neighbors. In particular, it is distributed and is progressively executed by nodes moving towards the proximity of the attacker. Specifically, nodes successively forward PDR measurements to neighbors towards assessing patterns related to PDR growth or degradation. The above structure of the algorithm is reminiscent of the iterative gradient-descent algorithm for identifying the minimum of a real-valued function f. The gradient-descent algorithm iteratively searches for a global optimum by moving from one point $\vec{x}_n$ of the function's domain S to another $\vec{x}_{n+1} \in S$. The point $\vec{x}_{n+1}$ is towards the opposite direction of the gradient of f at $\vec{x}_n$; this is the direction in which f exhibits the largest decrease with regards to its value at point $\vec{x}_n$. Note that in our case, the domain set consists of the discrete locations of the nodes. Hence, our scheme can be viewed as a discretized version of a gradient-descent algorithm. If the algorithm cannot proceed further, an optimum is declared[1]. As one can deduce, our scheme is greedy in nature, since each node takes the locally optimal choice to derive the global optimum (i.e., the position of the jammer).

Our full-fledged localization approach considers different starting points for the gradient-descent-based algorithm. We examine two algorithms as candidates for our approach. The first considers the distribution of the stopping points/nodes and applies a weighted centroid algorithm to estimate the position of the jammer. The second, which we include in our approach as the best solution, considers all the nodes where the *kernel*[2] algorithm stops, and declares as the jammer's position, the one with the smallest PDR. As might be evident, the latter scheme, similar to the kernel algorithm, always exhibits a non-zero error (since the position of the jammer is always assumed to be the same as that of a network node). However, as our evaluations indicate, it significantly reduces the uncertainty with respect to the position, as compared to both the vanilla gradient-descent-based algorithm and the weighted centroid algorithm.

Our main contributions in this work can be summarized as follows:

- **Analytical and experimental assessment of the spatial effects of jamming:** As previously mentioned, the jammer may affect both the transmitter and receiver operations; this has an impact on the PDR. We provide an analytical expression for quantifying the change in PDR at different locations in the network (relative to the jammer's location). We validate the analytically computed expression via real experiments on our 802.11 wireless testbed. Specifically, we show that the tranceivers that are further from the jammer exhibit lower (or no) degradation in terms of PDR as compared to transceivers that are located closer to the jammer.
- **Design of a lightweight jamming localization algorithm:** Having shown that PDR is minimized in the vicinity of the malicious device, we design a gradient-descent based algorithm to locate the adversarial node. We further design two algorithms that are built on top of the above core algorithm to improve accuracy; one is based on weighted centroid localization and an *annealing*-like extension which provides the best performance in terms of localization and thus, it is used in our approach. The main advantages of our approach (as compared to previously proposed localization approaches) are: (a) simplicity, (b) does not require any special hardware support, and (c) can be easily integrated with higher layer functions, such as routing, to circumvent the jammer's location.
- **Implementation and evaluation of our scheme:** We implement a prototype of our approach on our wireless testbed using the `Click modular router` [12]. We validate its performance through experiments on our indoor 802.11 testbed. We also evaluate the scalability of our approach through simulations (with larger topologies).

Our work in perspective: Our goal is to exploit the inherent propagation characteristics of the wireless channel in order to expose the presence of jamming devices and localize them. The jamming attacker might be able to hide itself from all but the wireless channel's propagation characteristics. The attributes of the jamming signals (and in particular their spatial properties) can affect measurable attributes (such as the PDR) to varying degrees in different parts of the network, thereby revealing important information with regards to the location of the malicious device. The key novelty of our scheme is its distributed nature and its lightweight operations.

In particular, our proposed algorithms offers the benefit that they rely on the operations of existing network functionalities and measurable quantities at a device level. Hence, no additional hardware or mechanisms are needed. Moreover, to reiterate, the nature of the gradient-descent algorithm allows the distributed execution of our localization scheme. Furthermore, the achieved localization error, which is at the range of one communication hop[3] significantly reduces the area that one needs to search for locating the misbehaving device. Equally novel and crucial is the adoptability of the designed scheme. In particular, the kernel can be used as a standalone module, the output of which can be processed in many various ways (e.g., a simulated annealing-like algorithm, a simple centroid calculation algorithm etc.). This flexibility further allows for building systems that can deal with more advanced attack models (see Section 5.5).

The rest of the paper is organized as follows. Section 2 provides the required background and describes related studies. Section 3 describes our analytical framework for quantifying the jamming effects on the PDR. Section 4 provides a progressive description of our component algorithms starting from the basic version to the full-fledged scheme. We present our experimental setup and evaluations in Section 5. Our conclusions form Section 6.

2. Background and related studies

In this section we present representative studies of different types of localization algorithms. We further briefly introduce the gradient-descent optimization method and discuss approaches that have utilized it for network operations.

Signal processing-based localization techniques: Secure mobile device localization, and in particular jammer localization, has been studied in the literature. Various approaches have been

[1] As we will see later this optimum is possibly local.

[2] We will use the words core, kernel and *vanilla* interchangeably in the rest of the manuscript.

[3] We prefer referring to this relative notion of error, since it puts results in perspective. For instance, a localization error of 20 m can be considered small for a WiFi network but it is certainly not small in the context of sensor or bluetooth networks, whose communication ranges are much smaller.