Computer Networks 141 (2018) 17–30

Contents lists available at ScienceDirect

Computer Networks

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

Adaptive jammer localization in wireless networks

Tongxiang Wang[a], Xianglin Wei[b], Jianhua Fan[b,*], Tao Liang[b]

[a] Graduate School, PLA Army Engineering University, Nanjing 210007, China
[b] Nanjing Telecommunication Technology Research Institute, Nanjing 210007, China

ARTICLE INFO

Article history:
Received 23 June 2017
Revised 4 April 2018
Accepted 3 May 2018

Keywords:
Wireless network
Directional jammer
Localization
Gravitational search algorithm

ABSTRACT

The shared nature of wireless communication, the open access to wireless medium, the tightly coupled design principle of wireless network protocol and the scarcity of radio spectrum make wireless networks vulnerable to different types of jammers, which prevents the normal communication among legitimate nodes by occupying wireless channel or corrupting network protocols' working process and poses a serious threat to the stability and security of the network. To tackle this security threat, a few anti-jamming schemes have been put forward including channel hopping, spatial retreat, etc. Among these strategies, jammer localization has attracted much attention in recent years since it is very helpful for jamming-avoidance routing and even jammer elimination. However, existing algorithms mainly focus on the localization of jammers equipped with omnidirectional antennas and fail to handle directional jammers, i.e., those attackers with directional antennas. In order to bridge this gap, this paper puts forward an Adaptive Jammer Localization Algorithm (AJLA) which can locating both types of jammers. At first, an identification method is employed to estimate the jammer's antenna type. If a omnidirectional antenna is adopted, typical existing algorithm, such as Centroid Localization (CL), Virtual Force Iteration Localization (VFIL), can be utilized to locate the jammer. Otherwise, an Improved Gravitational Search Algorithm (IGSA) is developed for directional jammer localization. A series of simulation experiments have been conducted to evaluate the performance of the proposed method. Experimental results show that AJLA-IGSA could locate the directional jammer efficiently and accurately. Besides, the complexity of information collection and localization process are also analyzed by experiments.

1. Introduction

We are now living in a huge network interwoven by various wireless communication products, which bring many convenience to our daily life. However, the shared nature of wireless communication, the open access to wireless medium, the tightly coupled design principle of wireless network protocol and the scarcity of radio spectrum make wireless network vulnerable to different kinds of security threats, such as Denial of Service (DoS) attacks, worm attacks, etc. Jamming attack, as one type of Dos attacks, has been widely adopted by attackers for its easily deployment and severe damage to the network [1]. Jamming attack can prevent communications among legitimate nodes by occupying wireless communication channel or damaging the working process of network protocols [2,3]. For instance, a jammer can break down the CSMA/CA protocol through continuously sending fabricated Clear-to-Send (CTS) packets to the network. To restore normal network service, many anti-jamming strategies have been presented at many different protocol layers, among which jammer localization has attracted special attention since it provides us a chance to remove the jammer from the network based on its location.

Jammer localization has been widely investigated in recent years, and a number of algorithms have been proposed. Existing jammer localization algorithms can be divided into two categories, i.e. range-based ones and range-free ones. Typical methods include Centroid Localization (CL), Virtual Force Iteration Localization (VFIL) [4], Double Circle Localization (DCL) [5] etc. However, most of current algorithms only focus on the jammers equipped with omnidirectional antennas and cannot adapt to those scenario where directional antennas are adopted by the jammers. The propagation of the omnidirectional antenna is isotropy and its influenced area is approximately a circle [6]. In contrast, a jammer equipped with direction antenna could impact an irregular area. Furthermore, it is very hard, or if not impossible, for us to know the jammer's type in advance.

To tackle this problem, we need a jammer-type independent localization method which can locate both types of jammers without knowing their antenna models in advance. To fulfill this require-

[*] Corresponding author.
E-mail addresses: tongxiangw@yeah.net (T. Wang), wei_xianglin@163.com (X. Wei), fjh7659@163.com (J. Fan).

https://doi.org/10.1016/j.comnet.2018.05.002
1389-1286/© 2018 Elsevier B.V. All rights reserved.

ment, we face two unique challenges compared with omnidirectional jammer localization problem:

- Our method needs to firstly estimate the antenna type of the jammer since it has not pre-knowledge. In other words, it can distinguish the jamming scenarios caused by omnidirectional and directional jammers.
- We need to develop a new directional jammer localization method since no existing algorithm available to the best of our knowledge. This is more challenging compared with omnidirectional jammer localization since the influenced area of the jammer is irregular.

In this paper, an Adaptive Jammer Localization Algorithm (AJLA) is presented which can tackle the above two challenges simultaneously. AJLA firstly identifies the jamming scenarios to determine the jammer's type. Then, existing localization algorithms (e.g., CL and VFIL) are employed directly to locate the omnidirectional jammer. For the directional jammer, a novel jammer localization based on Improved Gravitational Search Algorithm (IGSA) is designed. The main contributions of this paper are three-fold:

- A jamming scenario identification method is put forward based on the jammed area's topology information. At first, an information collection protocol is designed to gather the Received Jamming Signal Strength (RJSS) values from boundary nodes. Then, with no prior knowledge of the jammer's antenna type, the boundary nodes' positions and RJSS values are utilized to reflect the influenced area's characteristics and identify the jammer's antenna type. With typical network settings, this method can accurately distinguish directional and omnidirectional antennas.
- A novel localization algorithm based on IGSA is proposed to locate the directional jammer since no available localization algorithm can accomplish this task to the best of our knowledge. Compared with current adopted Multilateral localization method, our IGSA-based localization method can decrease the mean localization error from 7.5 m to roughly 1.1 m under typical directional jamming scenarios. Furthermore, the proposed method can also be adapted to locate omnidirectional jammer, and it can achieve better accuracy than existing algorithms.
- A series of experiments have been conducted to evaluate the performance of our proposed algorithm. Simulation results show that AJLA can accurately and effectively locate both jammer types.

The organization of the rest of the paper is as follows. Existing jammer localization algorithms have been summarized in Section 2. Section 3 formulates the problem of jammer localization. AJLA is presented in Section 4 and its evaluation method and results are shown and analyzed in Section 5. The last section briefly summarizes the paper.

2. Related work

Over the past few years, jamming detection and jammer localization have been investigated a lot and several strategies have been proposed to detect or locate the jammer. Generally speaking, the process of mapping jammed area or locating the jammer is usually conducted after detecting the jamming attack.

2.1. Jamming attack and detection

The impact of jamming attack on the network was analyzed by Xu et al. firstly and four types of jammers were presented in reference [7], i.e., constant jammer, random jammer, reactive jammer and proactive jammer. As the rapid development of wireless network technologies, more intelligent ways could be utilized by adversaries to launch jamming attack. Zhang et al. put forward the jamming ACK attack to disrupt the traffic flow of IEEE 802.11 networks [8]. When the receiver sent back the ACK to the sender, the jammer would send out packets to collide with the ACK packets. Law et al. put forward several jamming ways, i.e. S-MAC, LMAC, B-MAC, to attack the data link layer of the network [9]. Little efforts would be expended to launch such energy-efficient jamming attacks. A synchronization-based distributed denial of service (DDoS) attack was put forward by Subir Biswas et al. to attack the vehicular networks [10]. The jitter and background period of road-side units (RSUs) were synchronized by the attacker in order to launch a successful attack. The jammer was assumed to be equipped with learning ability by Yang et al. against low-duty-cycle networks [11]. They formulated the problem of learning and attacking for the jammers as a joint optimization problem and an iterative method was proposed to solve it.

Correspondingly, a series of detection methods have been proposed to determine the existence of the jammer. For the physical jamming attack, Xu et al. put forward several strategies to detect the jammers [12], such as distance consistency or position consistency detection. Fragkiadakis et al. combined the simple threshold algorithm and Dempster–Shafer algorithm to detect physical layer jamming attacks [13]. This collaborative detection method increased the performance by more than eighty percent. As for the intelligent jammers, simple detection method based on Signal to Noise Ratio (SNR) would fail to cope with them. In such case, more information in physical, MAC or protocol layer should be collected before conducting the detection process. The correlation between three parameters, i.e. Packets Delivery Rate (PDR), signal strength, was utilized by Sufyan et al. to detect the jamming attack in IEEE 802.11b network [14]. Different types of jamming attacks were considered when detecting the jammer. Punal et al. put forward one detection method based on machine learning for IEEE 802.11 network [15]. A helper metric including PDR, max.IT, channel time, busy time, was employed as the input of the detection system. Typical machine learning methods, i.e. C4.5 Decision Tree, AdaBoost, Support Vector Machine (SVM) and Expectation Maximization (EM) were utilized to detect the jamming attack. Zou et al. aimed to detect the CTS jamming attack by comparing the destination address in the CTS frame with the information of neighbor nodes [16]. The address should belong to the two-hop neighborhood set, or the control packets can be viewed as fabricated. The neighborhood information needed to be updated by sending periodic HELLO packets. Soryal et al. took the DoS attack on MAC layer into consideration and the variety of network throughput was utilized to detect and identify the MAC-layer jamming attack [17], which can increase the probability of successful transmitted packet. Then, the maximum throughout was derived in terms of maximum number of packets for the nodes in order to decide the baseline for the detection threshold. Li et al. also took this kind of selfish node with smaller backoff time into consideration and put forward a real-time detection scheme [18]. Instead of comparing the backoff time between nodes, the observer calculated the joint probability of the events that one node chose shorter backoff time and then, a confidence level was proposed to qualify the confidence of detection results.

2.2. Omnidirectional jammer localization

Without depending on specialized devices, Anthony D. Wood et al. have proposed a Jammed-Area Mapping Service for sensor networks to detect and map jammed areas through protocol interaction [19]. The output of jamming detection module is a JAMMED or UNJAMMED message broadcast to the node's neighbors. The boundary nodes inside the jammed area broadcast the message to the mapped nodes outside the region. The mapped nodes collaborate to map the jamming reports, then reroute traffic around