Future Generation Computer Systems 78 (2018) 1027–1039

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

# Collaborative mobile jammer tracking in Multi-Hop Wireless Network

Xianglin Wei [a], Tongxiang Wang [b], Chaogang Tang [c], Jianhua Fan [a,*]

[a] *Nanjing Telecommunication Technology Research Institute, Nanjing 210007, China*

[b] *College of Communications, Engineering and Electronic Engineering, PLA, University of Science and Technology Nanjing, 210007, China*

[c] *School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China*

## HIGHLIGHTS

- A distributed mobile jammer tracking scheme is put forward.
- The scheme contains four steps.
- A handover scheme is adopted among the monitoring nodes.
- Experimental results have validated the effectiveness of the proposed scheme.

## ARTICLE INFO

*Article history:*
Received 22 June 2016
Received in revised form
10 October 2016
Accepted 28 November 2016
Available online 6 December 2016

*Keywords:*
Jamming attack
Jammer
Localization
Tracking
Multi-Hop Wireless Network

## ABSTRACT

How to accurately locate and track mobile jammers in Multi-Hop Wireless Network (MHWN) is critical to restore network service and promote the quality of service of MHWN since its performance may severally be influenced by jamming attacks. Current research mainly focuses on object tracking in cooperative network configuration where the tracked object actively provides useful information to the tracking applications. However, this cooperative assumption will not hold for the jammer localization problem since jamming attacks can seriously affect network transmission. Moreover, the mobility property of the jammers makes current static jammer localization methods fail in this case. Therefore, in order to bridge this gap, a distributed mobile jammer tracking scheme is put forward in this paper which contains four steps, i.e., monitoring node selection, jamming signal measurement and result collection, jammer localization and monitoring node handover. In order to evaluate the effectiveness of the proposed scheme, a series of simulation experiments have been conducted. Experimental results have validated the effectiveness of the proposed scheme.

## 1. Introduction

Recent years have witnessed the rapid development of various wireless networks which provide the communication infrastructure for newly emerged computing paradigms, such as Internet of Things (IoT), Mobile Cloud Computing (MCC) and so on. As a feasible framework to achieve the universal connection among heterogeneous sensor devices in IoT environment, Multi-Hop Wireless Network (MHWN) has become a focus in academic and industry circles in recent years.

A MHWN usually contains untethered nodes that communicate with each other over multiple wireless hops, with participating nodes collaboratively forwarding ongoing traffic without any pre-existing infrastructure, like cables or access points. In different application scenarios, a number of different MHWN instances have been put forward. Typical MHWN instances include Wireless Sensor Network (WSN), Wireless Ad Hoc Network (WAHN), Wireless mesh network (WMN), Wireless Local Area Network (WLAN), Mobile Ad hoc NETworking (MANET) etc.

However, the shared nature of wireless communication, the open access to wireless medium and the self-organized network composition make MHWN vulnerable to multiple network attacks, including the mutual interference of normal nodes, malicious attacks from adversary, denial-of-service attacks and forge.

Among various security threats that MHWN faces in real world deployment, jamming attack is the most common one since it can be easily launched by simple radio devices and it will cause seriously performance degradation to the network [1,2]. Actually, based on limited jamming resources, a few jammers can remarkably impair network performance, partition the network, interrupt network applications and even damage physical infrastructure. For

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

http://dx.doi.org/10.1016/j.future.2016.11.032
0167-739X/© 2016 Elsevier B.V. All rights reserved.

instance, in smart grid, overdue message delivery caused by jamming attacks may lead to instability of system operations, and even cascading failures [3]. In intelligent transportation systems, transient control message loss may cause serious accidents. For the emergency response and military applications, jamming attacks may be fatal to the military units. In the IoT environment, jamming attacks can cut off the connection between the sensor devices and the system. Therefore, the IoT operator cannot correctly deliver their control commands to the isolated devices.

Jamming attacks has been a challenge to overcome since World War II, when they were launched against radars. Nowadays, jamming attacks continue to be a serious problem even for the most refined communication protocols implemented in the most sophisticated devices. Recent studies have demonstrated that such attacks can be accomplished very easily using off-the-shelf equipment. Furthermore, various commercial jamming devices and jamming strategies are readily available for attacking MHWN. Besides, the jamming effects may also occur due to accidental activation of devices that do not serve a malicious cause [4].

Adamy et al. have defined jamming as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission [5]. In the context of WSN, jamming is the type of attack which interferes with the radio frequencies used by network nodes [6]. Jamming attack may be viewed as a special case of Denial of Service (DoS) attacks, which is defined as "any event that diminishes or eliminates a network's capacity to perform its expected function" [7]. Typically, DoS prevents or inhibits the normal use or management of communications through flooding a network with 'useless' information.

The initiator of the jamming attack is called jammer while its affected area is usually referred to as the jammed area or the jammed region. As mentioned above, the jamming or interference may be launched intentionally or accidentally. However, regardless of unintentional interference or malicious jamming, jammers/interferers may have detrimental impact on network performance [8], including throughput, bandwidth as well as packet loss ratio. Therefore, in this paper, we do not distinguish intentional jamming attacks from accidental ones since they are all harmful to network performance in the viewpoint of MHWN. To apply various anti-jamming mechanisms in multiple protocol layers and thus to restore network service and ensure Quality of Service (QoS) [9,10], it is critical to find out the skeletonization of the jammed area or even the accurate location of the jammer since these mechanisms usually rely on this information. Therefore, how to accurately locate jammers in the network becomes a hot topic in academic and industry circles in recent years.

The jammer localization problem bears some similarities to the node localization problem in WSN [11] or WAHN [12], which needs to collect transmission information and calculate the locations of nodes whose coordinates are unknown. However, the non-cooperation relationship between the jammer and MHWN nodes makes jammer localization problem more challenging than sensors localization. Therefore, besides the challenges sensor localization problem faces in WSN, such as inaccurate measurement data caused by environmental factors and measurement devices, data insufficiencies due to sparse node density or packet loss, jammer localization faces a few unique challenges:

- Communication disruption caused by jamming attacks makes the information collection step hard to accomplish timely;
- In order to avoid being caught, there exist a few elementary jamming strategies including random jamming, reactive jamming, deceptive jamming and constant jamming. Besides, the jammer may adopt some kind of intelligent jamming strategies [13,14];
- The jamming signal is usually embedded in the legitimate traffic and is hard to extract. This is especially true for those reactive jamming signals.

According to the information used during location computation, current jammer localization algorithms can be divided into two categories: range-based and range-free methods. In the former category, such as Packet Delivery Ratio (PDR) based jammer localization method [4], Least Squares (LSQ) problem based jammer localization method [15], CrowdLoc [16] etc., the distance information between the jammer and MHWN nodes derived from physical measurement is utilized to some extent to estimate the position of the jammer. In contrast, the range-free jammer localization methods including Virtual Force Iterative Localization (VFIL) [17], Double Circle Localization (DCL) [18], Weighted Centroid Localization (WCL) [19] and X-ray [20] usually rely on the geometric characteristics of the jammed area to locate the jammer. These methods are brought forward based on different assumptions about jamming models and network environments and can achieve desired accuracy in dedicated network configurations. However, we also notice that most of existing methods cannot cope with the challenges brought by mobile jammers, which are those jamming entities equipped with motors and can move around the deployed area of MHWN.

The mobile jammer can dynamically change its position and thus it can adjust jamming signal's spatial distribution which will enable it to adapt to network configuration change. This mobility will make the jammer localization process more challenging: (1) for the range-based algorithms, the measured distances are biased due to high mobility; (2) the shape of the jammed area may change rapidly due to jammer mobility for the range-free algorithms; (3) jamming attack can severely affect or even disrupt legitimate transmission or information sharing in the jammed region which increases the difficulty of information sharing. Therefore, how to efficiently locate and track mobile jammers is difficult and will be the focus of this paper.

In this paper, a distributed mobile jammer tracking scheme is put forward which contains mainly four steps, i.e., monitoring node selection, jamming signal measurement and result collection, jammer localization and monitoring node handover. Firstly, a few monitoring nodes are generated from the MHWN nodes which are affected by jamming attack; Secondly, the affected nodes measures their received jamming signal strength and each monitoring node collects a few measurement results; Thirdly, each monitoring node performs jammer localization to find out the jammer's position; Finally, a handover method is designed to transfer the tracking task when the jammer is about to move out of a monitoring node's monitoring area.

The rest of this paper is organized as follows. Section 2 summarizes related work. Section 3 formulates the problem investigated in this paper. In Section 4, the distributed mobile jammer tracking scheme is put forward. The simulation experiments and results are shown in Section 5. Section 6 is a brief conclusion of this paper.

## 2. Related work

### 2.1. Jammer localization

There exist a few Radio Frequency (RF) direction-finding and emitter location techniques based on specialized signal process devices. For example, to know a radio emitter's geoposition in Electronic Warfare (EW), one can use a few EW intercept sensors to collaboratively confirm the transmitter's position through triangulation, trilateration or other refined methods based on direction of arrival (DOA) or time difference of arrival (TDOA) measurements [21]. These dedicated powerful sensors are usually