Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.955 – 961

RESEARCH ARTICLE

LOCALIZATION AND ROUTING AGAINST JAMMERS IN WIRELESS NETWORKS

Usharani[1], Asst.Prof. Anita Patil[2]

M.Tech 4th Semester[1], Department of CSE, BITM, Bellary, Karnataka, India
Ushinde66@gmail.com

Assistant Professor[2], Department of CSE, BITM, Bellary, Karnataka, India
Anitha.bijapur@gmail.com

ABSTRACT: Jammers are the devices that disturb the communication in wireless networks. If the actual position of jammer is located then it is possible to eliminate the disturbances in communication networks. This project designs a framework to locate the position of a single or multiple jammers more accurately. Many present jammer localizing schemes use indirect methods considering the hearing ranges, packet delivery ratio etc. This project uses direct methods that are the jamming signal strength. Estimating jamming signal strength is very challenging because the signals may be embedded in other signals. And the existing methods of locating do not provide global optimal solutions so this project performs some search algorithms for achieving the global optimal solution.

INTRODUCTION

The increasing need of wireless technologies, and the use of limited number of unlicensed bands, makes the radio environment crowded, this leads to the unintentional radio interference across the devices with different communication technologies sharing the same spectrum such as cordless phones, Wi-Fi network adapters, Bluetooth headsets. Regardless of whether it is unintentional interference or malicious jamming, one or multiple jammers may coexist and make an direct impact on network performance. To ensure the successful deployment of pervasive wireless networks, it is important to localize jammers, since the locations of jammers allow a better physical arrangement of wireless devices that cause unintentional radio

interference, or enable a wide range of defence strategies for combating malicious jamming attackers.

This project focuses on localizing one or multiple stationary jammers. The goal is to extensively improve the accuracy of jammer localization. Current jammer localization approaches mostly rely on parameters derived from the affected network topology, such as packet delivery ratios, neighbour lists, and nodes hearing ranges. The use of these indirect measurements derived from jamming effects makes it difficult to accurately localize jammers positions. Furthermore, they mainly localize one jammer and cannot cope with the cases that multiple jammers located close to each other and their jamming effects overlap. The constant jammer continually emits the radio signals. This project uses the direct measurements that are the strength of jamming signal (JSS). Localizing jammers using JSS is challenging. First, jamming signals are embedded in the regular network traffic. The commonly used received signal strength (RSS) measurement associated with a packet does not correspond to JSS. To overcome this challenge, this project uses a scheme that can effectively estimate the JSS utilizing the measurement of the ambient noise floor (ANF), which is readily available from many commodity devices (e.g. MicaZ motes).

Jamming localization may be different for the following reasons: 1) Most jammers start to disturb network communication after network deployment, which makes it difficult to obtain a site survey of radio fingerprints around jammers beforehand 2) No detailed prior knowledge about the jammers transmission power is available. 3) Multiple jammers with overlapped jamming areas may disturb network communication together, while attempting to hide their true locations.

To overcome these challenges and increase the localization of jammers accurately, this project formulates the jammer localization problem as a nonlinear optimization problem and define an evaluation metric as its objective function. The value of evaluation metric reflects how close the estimated jammers locations are to their true locations, and thus it can search for the best estimations that minimize the evaluation metric. Because traditional gradient search methods may converge to a local minimum and may not necessarily yield the global minimum, this project adopt several algorithms that involve stochastic processes to approach the global

optimum. This project also examines three algorithms: a genetic algorithm (GA), a generalized pattern search (GPS) algorithm, and a simulated annealing (SA) algorithm. So to estimate the positions of multiple jammers simultaneously, making it especially useful for identifying unintentional radio interference caused by multiple wireless devices or a few malicious and collaborative jammers.

RELATED WORKS

Jamming attacks have become prevalent during the last few years, due to the shared nature and the open access to the wireless medium. Finding the location of a jamming device is of great importance for restoring normal network operations. After detecting the malicious node it is necessary to find its position, in order to take further actions. The goal in this paper is the design and implementation of a simple, lightweight and generic localization algorithm. This scheme is based on the principles of the gradient descent minimization algorithm. The key observation is that the Packet Delivery Ratio (PDR) has lower values as we move closer to the jammer. Hence, the use of a gradient-based scheme, operating on the discrete plane of the network topology, can help locate the jamming device. The contributions of this work are: (a) it demonstrates, through analysis and experimentation, the way that the jamming effects propagate through the network in terms of the observed PDR. (b) Designing a distributed, lightweight jammer localization system which does not require any modifications to the driver/firmware of commercial NICs. (c) Implementing and evaluating localization system on 802.11 indoor test bed. An attractive and important feature of this system is that it does not rely on special hardware. [1]

Wireless communication is susceptible to radio interference and jamming attacks, which prevent the reception of communications. Most existing anti-jamming work does not consider the location information of radio interferers and jammers. However, this information can provide important insights for networks to manage its resource in different layers and to defend against radio interference. In this paper, it investigates issues associated with localizing jammers in wireless networks. In particular, it formulates the jamming effects using two jamming models: region-based and signal-to-noise-ratio (SNR)-based; and categorizes network nodes into three states based on the level of disturbance caused by the jammer. By exploiting the states of nodes, it proposes to localize jammers in wireless networks using a virtual-force iterative approach. The virtual-force iterative localization

scheme is a range-free position estimation method that estimates the position of a jammer iteratively by utilizing the network topology. [2]

Jamming attacks are especially harmful when ensuring the dependability of wireless communication. Finding the position of a jammer will enable the network to actively exploit a wide range of defence strategies. In this paper, it focuses on developing mechanisms to localize a jammer by exploiting neighbor changes. It first conducts jamming effect analysis to examine how the communication range alters with the jammer's location and transmission power using free space model. Then, it shows that a node's affected communication range can be estimated purely by examining its neighbor changes caused by jamming attacks and thus, can perform the jammer location estimation by solving a least-squares (LSQ) problem that exploits the changes of communication range. Compared with the previous iterative-search-based virtual force algorithm, the LSQ based algorithm exhibits lower computational cost (i.e., one-step instead of iterative searches) and higher localization accuracy. Furthermore, it analyze the localization challenges in real systems by building the log-normal shadowing model empirically and devising an adaptive LSQ-based algorithm to address those challenges. The extensive evaluation shows that the adaptive LSQ-based algorithm can effectively estimate the location of the jammer even in a highly complex propagation environment. [3]

Wireless networks are built upon a shared medium that makes it easy for adversaries to launch jamming-style attacks. These attacks can be easily accomplished by an adversary emitting radio frequency signals that do not follow an underlying MAC protocol. Jamming attacks can severely interfere with the normal operation of wireless networks and, consequently, mechanisms are needed that can cope with jamming attacks. In this paper, it examines radio interference attacks from both sides of the issue: first, it studies the problem of conducting radio interference attacks on wireless networks, and second examines the critical issue of diagnosing the presence of jamming attacks. Specifically, it proposes four different jamming attack models that can be used by an adversary to disable the operation of a wireless network, and evaluate their effectiveness in terms of how each method affects the ability of a wireless node to send and receive packets. It then discusses different measurements that serve as the basis for detecting a jamming attack, and explore scenarios where each measurement by itself is not enough to reliably classify the presence of a jamming attack. In particular, it observes that signal strength and carrier sensing time are unable to conclusively detect the presence of a jammer. Further, it observes that although by

using packet delivery ratio it can be able to differentiate between congested and jammed scenarios, nonetheless unable to conclude whether poor link utility is due to jamming or the mobility of nodes. The fact that no single measurement is sufficient for reliably classifying the presence of a jammer is an important observation, and necessitates the development of enhanced detection schemes that can remove ambiguity when detecting a jammer. To address this need, it proposes two enhanced detection protocols that employ consistency checking. The first scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, while the second scheme employs location information to serve as the consistency check. Throughout our discussions, we examine the feasibility and effectiveness of jamming attacks and detection schemes using the MICA2 Mote platform. [4]

Location estimation is a critical step for many location-aware applications. To obtain location information, localization methods employing Received Signal Strength (RSS) are attestative since it can reuse the existing wireless infrastructure for localization. Among the large class of localization schemes, RSS-based lateration methods have the advantage of providing closed-form solutions for mathematical analysis as compared to heuristic-based localization approaches. However, the localization accuracy of RSS-based lateration methods is significantly affected by the unpredictable setup in indoor environments. To improve the applicability of RSS-based lateration methods in indoors, it proposes two approaches, regression-based and correlation-based. The regression-based approach uses linear regression to discover a better fit of signal propagation model between RSS and the distance, while the correlation-based approach utilizes the correlation among RSS in local area to obtain more accurate signal propagation. [5]

Jamming attacks are especially harmful when ensuring the dependability of wireless communication. Finding the position of a jammer will enable the network to actively exploit a wide range of defence strategies. Thus, in this paper, it focuses on developing mechanisms to localize a jammer. It first conducts jamming effect analysis to examine how a hearing range, e.g., the area from which a node can successfully receive and decode the packet, alters with the jammer's location and transmission power. Then, shows that the affected hearing range can be estimated purely by examining the network topology changes caused by jamming attacks. It solves the jammer location estimation by constructing a least-squares problem, which exploits the changes of the hearing ranges. Compared with the previous iterative search-based virtual force algorithm, this proposed system hearing-range-based

algorithm exhibits lower computational cost (i.e., one-step instead of iterative searches) and higher localization accuracy. [6]

PROPOSED SYSTEM

Based on jamming signal strength (JSS) location of jammers can be known accurately, and routing against jammer can be achieved.

The below three algorithms are used:

- Genetic algorithm (GA).
- Generalized pattern search algorithm (GPS).
- Simulated annealing algorithm (SA).

CONCLUSION

The problem of localizing jammers can be achieved by using the jamming signal strength and using the three algorithms genetic algorithm, generic pattern search algorithm, the accurate location of jammer can be found. This helps the network communication to perform properly without the effect of jammer.

REFERENCES

[1] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S.V. Krishna- murthy, Lightweight Jammer Localization in Wireless Networks: System Design and Implementation," Proc. IEEE GLOBECOM, 2009.

[2] H. Liu, Z. Liu, Y. Chen, and W. Xu, "Determining the Position of a Jammer Using a VirtualForce Iterative Approach," Wireless Networks, vol. 17, pp. 531-547, 2010.

[3] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 3, pp. 547-555, Mar. 2012.

[4] W.Xu, W.Trappe,Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Net- works," Proc. ACM MobiHoc, 2005.

[5] J. Yang, Y. Chen, and J. Cheng, "Improving Localization Accuracy of RSS-Based Lateration Methods in Indoor Environments," Ad Hoc and Sensor Wireless Networks, vol. 11, nos. 3/4, pp. 307-329, 2011.

[6] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Wireless Jamming Localization by Exploiting Nodes' Hearing Ranges," Proc. IEEE Int'l Conf. Distributed Computing in Sensor Systems, 2010.

