Mitigation of Jamming xxxx____Sample work____)

First Author[#], Second Author[*], Third Author[#]

[#]*First-Third Department, First-Third University*
Address

[1]first.author@first-third.edu
[3]third.author@first-third.edu

[*]*Second Company*
Address Including Country Name

[2]second.author@second.com

ABSTRACT

Jamming attacks drastically degrade the performance of wireless networks; some effective mechanisms are required to detect and to avoid them. Constant, deceptive, reactive, intelligent, and random jammers are few jamming techniques used in wireless medium. xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxxThis chapter proposes a fuzzy model based on RSSI, PDR, and PSR for detection and classification of jamming attack precisely. The proposed architecture is simulated in MATLAB based on simulation parameters.

Keywords

Multi-model detection technique
Jamming attacks
Wireless networks
Jammer
Detection of service

1. Introduction

Wireless networks make use of shared transmission medium; therefore, they are open to several malicious attacks. An attacker with a radio transceiver intercepts a transmission, injects spurious packets, and blocks or jams the legitimate transmission. Jammers disrupt the wireless communication by generating high-power noise across the entire bandwidth near the transmitting and receiving nodes. Since jamming attacks drastically degrade the performance of wireless networks, some effective mechanisms are required to detect their presence and to avoid them. In this chapter we propose a multi model system for the detection of jamming attack.

Accurate detection of radio jamming attacks is challenging in mission critical scenarios. Many detection techniques have been proposed in the literature, but the precision component is always an issue. Some of them either produce high false alarm rates or do partial detection of jamming attacks. Moreover, the results are based on simulations [8,9,10,11,12 125-131]. After detection, classification of jamming attacks is necessary to launch appropriate recovery techniques like channel hopping or spatial retreat. The classification of jamming attacks plays an important role not only to differentiate them from each other but also to identify different network performance degradation phenomena like network congestion or channel fading.

The development of multi-model detection technique can help in detecting jamming attacks with lower false alarm rate and high precision. The following sections of the paper were organized as follows. ~~In the following way, the remainder of the paper is arranged.~~ A short background on the performance anomaly in 802.11 is provided in the Sect.2 moreover jamming attacks, and discussion related studies are also included. The implicit jamming detection our anti-jamming system and mitigation with FIJI are described in Sect. 3. The implementation of FIJI and evaluation of its effectiveness are dealt in Sect. 4. The elaboration on certain FIJI attributes and discussion of the applicability of our framework in various settings are described in Sect. 5. Sect. 6 is conclusion.

2. Background and Related Works

Overview of network and jamming model

Based on the jamming behaviour, earlier studies classified it in to four different models. The constant jammer model continuously transmit bit with out considering any protocol [1], perhaps, they lack power efficiency. The Deceptive jammer worked based on the target network protocol and transmit legitimate packets over a span of time continuously at high rate to hold the carrier captured, but it is inefficient at constant jammer. Random jammer function were based on the arbitrary manner, however it is much energy efficient than previous jammers.

Through succeeding S-MAC protocol energy effective jammers for attacking network is recommended [2], it encloses Periodic Control Interval Jammer, Data Packet Jammer, Cluster Jammer and Listening Interval Jammer. However, Interrupt, Scan, Activity and pulse jamming attack prototypes have also been proposed [3]. Single-Tone jammer at a time attack single channel, whereas multi-Toner can attack entire or certain channel receiver. The pulsed – Noise Jammer transmit pulse jamming signals by turn on and off occasionally at slow and fast rate in wide band jammer. ELINT is commonly a passive model which attempts to examine communication or radar TCF signals or break down; hence it is not a jamming attack model strictly [4].~~Based on their behaviour, several authors have classified jammer. For example, four types of jammer models where constant jammer model continuously transmitter bits over time span without considering any protocol, are proposed in the research done by [1] perhaps, they are ineffective in power efficiency.~~

~~Deceptive jammer is on the basis of the target network's protocol and the network is jammed by transmitting legitimate packets over a span of time at a high rate continuously to hold the carrier captured, perhaps energy is not efficient at the constant jammer. On the arbitrary manner, random jammer functions are based, however it is little efficient than the previous jammer while it is much energy efficient.~~

~~By [2] four kinds of energy-effective jammers for attacking a network is recommended through succeeding the S-MAC protocol, which encloses Periodic Control Interval Jammer, Periodic Data Packet Jammer, Periodic Cluster Jammer and Periodic Listening Interval Jammer. Moreover, Interrupt, Scan, Activity and pulse jamming attack prototypes have also been proposed by [3].~~

~~It is shown by the Models of [4] that single channel at a time is attacked by the Single-Tone Jammer, while the Multi-Tone Jammer can attack entire or certain channels of a multi-channel receiver, perhaps, the Pulsed-Noise Jammer transmit pulsed jamming signals by turn-on and off occasionally at a slow and fast rate and is a wide band jammer. ELINT is commonly a passive model which attempts to examine communication or radar TCF signals or break down; hence it is not a jamming attack model strictly.~~

Previously proposed anti-jamming techniques

Earlier reports focused on anti-jamming technique (individual node level), perhaps these techniques were based on the threshold values of metrics or digital signal processing technique, thus legitimate and jamming signals were differentiated. Whereas other ~~Prior works focused on the anti-jamming techniques are implemented at the individual node level. Moreover their technique is either based on threshold values of some of the metrics, as discussed before, or to use digital signal processing techniques to differentiate between a legitimate signal and an illegitimate (jamming) signal. Other~~ methods used compared nodes with ~~those of neighbors to fine tune their findings.~~

Formatted: Space Before: 0 pt

Formatted: Space After: 10 pt, Pattern: Clear (White)

The jamming attack detection was extensively studied using MICA2 Mote platform [1]. ~~Carried out intense study of the jamming attack detection mechanism with experiments using the MICA2 Mote platform~~. ~~The HOC method can distinguish the constant and deceptive jamming from the normal traffic, but cannot distinguish the random and reactive jamming~~. ~~from the normal traffic. If PDR is used with consistency checks like, checking its signal strength, distance and comparing with those of neighbor and the combinations can very effectively detect and discriminate various forms of jamming. Inspite of the sound methodology, a complete process is lacking for WSN node, which may not be able to communicate with its neighbors during jamming to get the required statistics for comparison. If PDR is used with consistency checks like, checking own PDR and signal strength and comparing the same with those of the neighbors, and/or ascertaining own distances from the neighbors, then the combination can very effectively detect and discriminate various forms of jamming. Even though the study is rigorous and suggested sound methodology is sound, it encounters limitations like complete process has to be done by the WSN node which is taxing and the node may not be able to communicate with its neighbors during jamming to get the required statistics for comparison, as required in the method.~~

xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxxin jamming. It is computation-intensive and taxes the resource-starved WSN node and fixes the threshold of decision parameter for each node and based on evolutionary algorithm, it is difficult to ascertain time and space, perhaps it is important to important to minimized for any resource-constrained network, like the WSN.

~~[2] Use ‘*the swarm intelligence and ant system’* wherein they create an agent (ant) which proactively uses the WSN node’s information (key performance parameters), as it traverses a route from node to node, to predict or anticipate jamming, and accordingly, changes the route to avoid jamming. They suggest a decision threshold, called probability of selecting a link between nodes *i* and *j*, called P_{ij}, to be calculated at node *i*. The limitation of this study indicates that it lacks the readily available data, some are complicate to ascertain and involves communication with other nodes which is not possible in jamming. It is computation-intensive and taxes the resource-starved WSN node, it involves fixing threshold of the decision parameter for each node under different conditions and based on evolutionary algorithms whose complexities in terms of time and space is difficult to ascertain; but are important to be minimized for any resource-constrained network, like the WSN.~~

[5] Have proposed two algorithms for detecting a jamming attack. The first algorithm is based on threshold values of three detection parameters (BPR, PDR and ECA) and considered ~~.there is no jamming if all the detection parameters or PDR exceeds the threshold, if not jamming exist If all three parameters are below the thresholds, or if only the PDR exceeds the threshold, then it is concluded that there is no jamming; otherwise, there is jamming exist. The second one is an improved version algorithm is an improvement over the first one~~ where the neighboring nodes’ conditions, ascertained through queries to be raised and replies there-to to be received within the threshold time periods, are also taken into account to enhance the jamming detection rate the suggested models suffer from fixing of too many thresholds and processing at the node levels, which have their own problems. The limitation of ~~in~~ this model is ~~the~~ PDR, measured at the transmitter-end, as in the instant case, is not suitable for the resource-constrained WSN because it imposes the avoidable burden of acknowledgements.

xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxx_Sample work____ xxxx____Sample work____xxxxfirst compute the root mean square value of the clean signal, C_{rms}, and then use it for other computations.

If ̄ isgreater than σ, they conclude that it is a jamming signal; else, it is a clean signal. As evident, the calculations have to be done by the WSN node over a period of time (from $t = a$, to $t = b$), ~~very~~ frequently, almost all the time, to keep differentiating the clean and jammed signals. The major limitation of this model is the jamming ~~. This is a great disadvantage of this method, if used for jamming~~ detection in the WSN scenario and discriminate jamming signal, ~~. Also, it cannot discriminate a jamming signal,~~ if the jammer uses the same power in the jamming signal as that in the clean signal.

[7] have suggested a ~~very~~ effective method of detecting a reactive jammer ~~(which otherwise is so difficult to be detected)~~ through Received Signal Strength (RSS) and Bit Error Rate (BER) samplings and inferring the presence of the reactive jammer in the event of high BER despite the RSS being normal ~~or better than the normal~~. This method involves ~~The method involves three steps:~~ (1) error sample acquisition, (2) interference detection~~,~~ and ~~(3)~~ sequential jamming test to infer presence or absence of reactive jamming. Thise method has a sound mathematical foundation and is capable of detecting all types of jamming attacks, including reactive jamming, but lacks it cannot discriminate different types of jamming attacks. It also involves ~~of~~ sampling/fixing thresholds and values.

Various other jamming analysis, detection and mitigation schemes have been proposed in the literature [8, 9, 2, 10, 11, 3, 12, 13],~~. All of these~~ suggested the mechanisms which has~~are~~ to be implemented at the individual node level to crisply conclude whether the node is jammed or not. Their technique is either based on threshold values ~~of some~~ of the metrics, as discussed before, or to use digital signal processing techniques to differentiate between a legitimate signal and an illegitimate (jamming) signal and thus conclude about the presence or absence of the jammer.

xxxx____Sample work____xxxx_Sample work____
xxxx____Sample work____xxxx_Sample work____
xxxx____Sample work____xxxx_Sample work____
xxxx____Sample work____xxxx xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx

Acknowledgements

References

[1] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks. MobiHoc '05, Proceedings of the Sixth ACM International Symposium on Mobile ad hoc Networking and Computing (2005).

[2] Y.W. Law, L. van Hoesel, J. Doumen, P. Hartel, P. Havinga, Energy efficient link-layer jamming attacks against wireless sensor network MAC protocols, Proceedings of ACM security sensor ad-hoc networks (2009).

[3] A.D. Wood, J.A. Stankovic, G. Zhou, G. DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks, The 4th Annual IEEE Communications Society Conference on Sensor, San Diego, CA: Mesh and Ad Hoc Communications and Networks, (2007).

xxxx____Sample work____xxxx_Sample work____
xxxx____Sample work____xxxx_Sample work____
xxxx____Sample work____xxxx_Sample work____
xxxx____Sample work____xxxx xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx_Sample work____ xxxx____Sample
work____xxxx

[8] M. Li, I. Koutsopoulos, R. Poovendran, Optimal jamming attacks and network defense policies in wireless sensor networks, http://www.computer.org/csdl/trans/tm/2010/08/ttm2010081119-abs.html

[9] M. Cagalj, S. Capkun, J. P. Hubaux, Wormhole-based anti-jamming techniques in sensor networks, IEEE Transactions on Mobile Computing 6(2007) 100–114.

[10] R. Mallik, R. Scholtz, G. Papavassilopoulos, Analysis of an on-off jamming situation as a dynamic game, IEEE Transactions on Communications 48 (2000) 11360–1373.