March - April 2020
ISSN: 0193-4120 Page No. 9428 - 9435

Jamming and Jamming Discovery Techniques in Wireless Sensor Networks

DR. T. Lalitha[1], DR. S. Jayapraba[2], Dr. S. Saravanakumar[3]
[1]Associate Professor, Department of Computer Application, Sona College of Technology, Tamilnadu.
[2]Assistant Professor, Jayam College of Engineering and Technology, TamilNadu.
[3]Asso.Prof/CSE,Dayanandasagar academy college,Bangalore

Article Info
Volume 83
Page Number: 9428 - 9435
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 09 April 2020*

Abstract
Jamming in WSN is a primary challenge faced because of the ease of blocking WSN contact. Jamming problems are a subset of service-based denial attacks in which affected nodes pre-vent legitimate contact by causing deliberate interference in communication networks on a recur-sive basis. To understand this problem, different strategies for jamming and anti-jamming in WSN need to be addressed and analysed in detail. Specific jamming localisation, countermeas-ure and identification methods are researched to tackle jamming difficulties. The key characteris-tics of jamming methodologies and their types of jammers, and positioning jammers for efficient jamming. In this paper the open problems such as jammer recognition and energy-efficient detec-tion schemes in this area

Keywords; *Jamming, wireless network, jammers classification, placement of jammers, localizing jammers, countermeasure for jamming*

I. INTRODUCTION

WSN plays a significant part in achieving global networking where network appliances are located in locations that offer access and infrastructure at nonstop. It increases other things on the other hand. Current WSN are easily attacked by jamming devices, owing to the open existence of wireless connections. Jamming can trigger Denial-of-Service problem that can lead to several other security issues in higher layers, although these are often not tackled properly.

Jamming in WSN is separate as interrupting current wireless communication by the ratio of single to noise on the receiver sides over the propagation of noisy wireless signals. Jamming is distinct from normal network interferences, as it reflects the intentional use of wireless signals in an effort to impede contact while interfering with unwanted methods of interruption. Wireless communication between nodes may cause unintended interference within the same networks or other strategies. Interference by Intentional equipments is usually done by an intruder who antic-ipates network communications to be interrupted or halted.

Jamming can be accomplished at altered speeds, from obstructing transmission to modifying packets of legitimate communications. To learn how a jammer attacks WSN and how to prevent jamming to achieve effective communication, explore different features of wireless networking:

Types of current jammers Protocols for the identification and countermeasure of jammers and jamming.

There are many ways to jam a network using various kinds of jammers. Understanding how a jammer works is important to avoid network jamming. Hence, we discuss various forms of jammers in-depth, such as proactive, reactive, hybrid-smart jammers, and function-specific jamming achieve the best performance. Examine the latest techniques at the time to find jammers in networks. As a final

Published by: The Mattingley Publishing Co., Inc.

chapter, we are looking at how to deal with the jamming issue. This is the difficult problem, where a lot of inquiries have been carried out. For example, one simple solution is to narrate high transmission power on jammed channels which makes this jam less of a thread.

The use of spinning antennas instead of omnidirectional antennas is an effective counter-measure to jamming. Yet none of the current detection or countermeasure methods can tackle all types of jammers without giving false alarms. Of this reason, further research is required to iden-tify and prevent various forms of wireless network jamming.

This work includes three important contributions. First of all, various types of jammers are being deliberated from the viewpoint of an intruder, and their possible placements. Second, dis-cuss emerging anti-jamming strategies in detail from a security perspective and divide them into different categories. Third, we concentrate on key issues concerning existing countermeasures to jamming attacks and tackle future research challenges to prevent jamming.

The layout of the paper is as follows: Section 2 marks definitions of jamming attacks, jammer classifications and techniques for jammer positions for actual attacks. Giving the critical elements in Section 3 of how to find jammers in networks; Section 5 marks critical problems with current protocols and analysis tasks, and we end our study in Section 6.

II. JAMMING METHODS

Jamming uses intentional radio interferences to interrupt wireless communications by inten-tionally manipulating media busy forcing a transmitter to back off whenever it detects a very real wireless or skewed transmitting signal on the receiver side. Jamming avoids physical layer inci-dents but at times cross-layer attacks are likely. To maximize the jammed area, expand on differ-ent types of jammers and the placement of jammers in this partition.

2.1 Types of jammers

Jammers are malicious wireless node plants of an attacker which cause intended interference in a wireless network. A jammer can either possess the same or different functionality from the legal network nodes they are targeting, based on the approach to the attack. The jamming effect of a jammer depends on the power, location, and impact of its own radio transmitter on the ad-dressed network or node. Jammers jam up a network in several ways to make the jamming as effective. In addition a jammer may be either basic or advanced depending on its use. We split them into two classes, the jammers: constructional and reactive. The advanced jammer was split into two subtypes, too: function-specific, and smart-hybrid.

2.2 Proactive jammer

Proactive jammer conveys the jamming signals whether or not there is a DCN (data commu-nication network). It sends packets of other random bits to the system where it operates to put all other nodes in non-operating methods on that channel and position all the other nodes on that network. However, it doesn't switch channels and only operates on one channel until its capacity is depleted. There are three styles of aggressive jammers: manipulative, persistent, and by chance.

Deceptive jammer can conveys regular packets, rather than random bits. This fools some other nodes into making sure there is a legitimate connection, and they stay in receiving states until the jammer is turned off or dies. Compared to a persistent jammer, finding a fake jammer is easier, as it transmits real packets rather than random bits. Similar to the persistent jammer misleading jammer, the continuous transmission is too energy intensive but can be introduced very easily.

Constant jammer emits unpredictable, nonstop bits without having to obey CSMA. As per the CSMA

Published by: The Mattingley Publishing Co., Inc.

protocol, a lawful node must check the status of the wireless media before transmitting. If the medium is continually idle for the DCF Interframe space length, the transmission of a frame is composed only then. If the channel is busy during the DIFS time the station will postpone the transmission. A recurrent jammer inhibits the contact of relevant nodes with one another by causing continuous occupancy of the wireless network. This type of attack is slow drive and easy to execute, and can interrupt network traffic to the point where no-one can connect at any time.

Random jammer periodically transmits either random bits or standard packets into the net-works. Unlike the above two jammers, it's intended for legal capital. It constantly switches be-tween the two states: the sleeping and jamming phases. It sleeps for some time, and then gets ac-tive in jamming before going to sleep. The sleeping and jamming time period is one set or the other, or unpredictable. There is a trade-off between jamming efficiency and saving energy, as it can't jam during its sleep time. It is possible to manipulate the ratios measured between sleep and jamming time to adjust this trade between efficiency and efficacy.

2.3 Reactive Jammer

Reactive jammers only continue to jam when a network operation is detected on a given channel. Receipt of the document as a result. It is capable of interrupting both small packets and huge packets. Meanwhile, the network reactive jammer is less energy-competent than random jammer that has to be constantly monitored. Nonetheless, it is much more difficult to identify a reactive jammer than a constructive jammer, since the packets ' propagation ratio can not be accurately measured in practice. There are two different ways, according to the following, to implement a reactive jammer

Reactive RTS/CTS jammer interferes with the network when it detects a request from a sender to send a message. Once the RTS is sent it's jamming the network. That means the recipient won't return a clear-to-send address because it distorts a sender's RTS packet. The sender should not send data, because it is likely that another communication will be engaged with the recipient. Alternatively, when the receiver sends CTS jammer will wait for RTS and jams reception. That will also result in the transmitter not sending data and the receiver constantly waiting for the data packet.

Reactive ACK / Data jammer blocks the network by corrupting data transfers or packet recog-nition.This does not respond until the transmitter ceases as transmission of data begins. The jammer approach can encrypt data packets, or it can delay until the data packets reach the recipi-ent and the ACK packets are corrupted. Both data packet corruptions and ACK messages can result in sender-end retransmission.The receiver side does not view the data packets properly in the first case; they must be retransmitted. For example, in the second method, buffer overflow, the sender does not receive the ACK which implies something on the receiver side is false. So it will retransmit the data packets again.

2.4 Function-Specific Jammers

Clear jamming of computers with preset purpose is introduced. In addition to being either proac-tive or reactive, both can work on a single channel to conserve energy or jam multiple channels to optimize the jamming efficiency regardless of energy usage. Even if jammer jams a single channel at a time, they are not safe to that channel and can change their networks to match their specific functions.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9428 - 9435

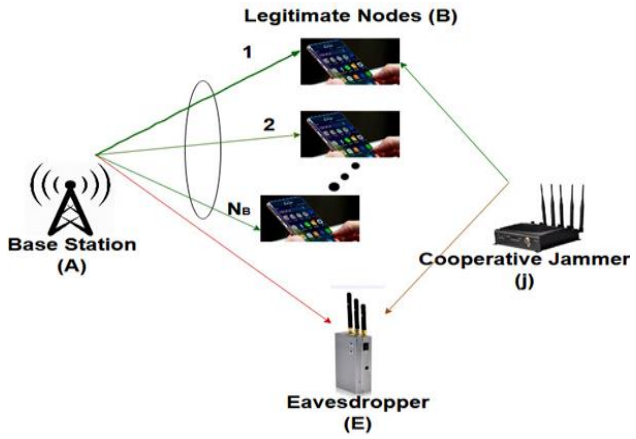

Fig 2.1: Eavesdropper Jammer

Follow-On Jammer hops often performed all available channels and jams and channel for a short time. If a transmitter hears the jamming and pushes the follow-on jammer and the whole band onto their channel and looks for another frequency to jam again. Otherwise a quasi random frequency hopping structure might follow. This form of jammer retains power by reducing its assault to one frequency before switching to another. Because of its high frequency hopping, it is especially effective against certain anti-jamming tactics to score the following on jammer, for e.g. frequency hopping is spread spectrum that uses a slow hopping rate.

Channel-Hopping Jammer proactively hops between the various channels. This form of jammer has direct channel access by overriding the MAC layer provided CSMA algorithm. It can also propagate simultaneously through several networks. The jammer is quite and elusive to its neighbors throughout the phases of its detection and vertex drawing. It begins executing attacks at specific times on multiple networks according to an encoded pseudo-random sequence.Pulsed-noise jammer will switch channels and jam over modified bandwidths at different times. The spinning off and on can also save energy according to the plan for which it is designed as compared with the random jammer pulsed noise jammer. Unlike that, the basic constructive random jammer targeting one channel would hit multiple channels with pulsed jammer of noise. In addition it can be added to concurrently block multiple channels.

2.4 Smart-Hybrid Jammers

We find this jammer smart because their jamming ability is efficient and effective in nature. The main purpose of these jammers is to magnify their jamming effect within the network they're at-tempting to jam. Equally, they protect their wealth by taking care of themselves. In very large networks, they place enough energy in the right position to limit the propagation capacity for the entire network, or for a significant part of the network. These jammer forms can be used as both positive and reactive, mixed.

Control channel jammers operate on multichannel networks by controlling the control channel or channel used to manage network activity. Binary jammer targeting the control channel can cause the basic network output to deteriorate while an unbroken jammer targeting the control network will block access to the entire network. Usually these attacks are qualified when the network has a vulnerable node. Additionally, potential control channel locations can be accessed from corrupted nodes.

Implicit jamming attacks are those that trigger dos (denial of service) status at other network nodes as well as disabling the intended target's functionality. This attack aims at the rate adapta-tion algorithm used in WSN, where the AP caters to the vulnerable node by decreasing the rate. This method means that the AP spends more time connecting with the weak node than with the other nodes. Therefore, if the tacit intruder jams a node that communicates with the AP, the ef-fect of rate reduction will maximize the AP's focus on the jammed node while inflicting distress on other clients.

III. OPTIMAL JAMMING ATTACK

If both the attacker and his transmitting powers are attentive to the network approach, the possibility of jamming can be made strong. The jammer must also have knowledge of the proba-bility of access to the

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9428 - 9435

network channel and number of neighbors to monitor the node.

All other network nodes perform regular IEEE 802.11 simplex communication. The con-trol node uses the Successive Possibility Ratio Test (SPRT) to sequentially test the possibility of a false alarm and the risk of missing detection between two hypotheses.

The jammers and receivers are spread by way of distribution over a given area. In terms of prob-ability the predicted values of an effective transmission are determined. The n control node is expected to send the jamming warning out of the system if a particular area is jammed, which also grieves at the area's jamming. Using distributed probability and a statistical proof the authors showed that the attacker's optimal strategy appears to be very mild and long-term. The table below shows the form of jammers and has changed their positionings.

Placement Strategy	Detection Level	Transmission Power	Network Knowledge	Number of Jammers
Placement Strategy	Detection Level	Transmission Power	Network Knowledge	Number of Jammers
DSS for locating the VHF / UHF Jammer	Easy	High	Yes	Several
Optimal Jamming Attacks	Difficult	Manageable	Yes	One
Limited range of Jamming Attacks	Difficult	Low	No	Several
Jamming below complete uncertainty	Moderate	Calculated	Limited	Several

Table 3.1: Different types of Jammers and their Placement.

3.1 Jamming under complete ambiguity

Commander et al use a dynamic approach to location estimation by adding the region's borders to be jammed to place jamming instruments. They understand a square-shaped area circling the network where the jammers are connected by a structured grid. If all the other network nodes need to optimally block the jammers how are they going to be positioned? To achieve an optimal result, subproblems are formed and solved. We presume the hacker has partial information about the network, i.e. the perpetrator knows only the bounding field and the jammers have omnidirec-tional antennas. We return that the jamming power to form an apparatus decreases inversely to the square size. This scheme also measures the least number of jamming devices to jam the entire network, given that jamming happens at any point when the total power recognized at a par-ticular point is greater than the starting power required to jam the wireless communication.

3.2 DSS for location VHF/UHF jammer

Gencer et al identifies a jamming mechanism which should be located at the best location in or-der to fully demolish the contact ability of the target system. Typically military implementations use certain types of systems. To order to structure the jammer scheme, additional candidate points or selected points shall be considered to relation to the goal points and the number of available jamming systems. We presume there's a line of sight between the target systems and the actual jammer objectives are within the antenna range, and the jamming device's acceleration power is stronger than the target system's signal strength.

The basic purpose of this decision support system is to identify or consider the location of the radio jammer systems in such a way as to jam the maximum possible area. And they use the full cover to solve it using the LINGO-8 method. LINGO is a hybrid framework for communicating

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9428 - 9435

optimisationframeworks with a flexible language. Due to the number of target points candidate points and the available jamming devices, the places for deploying jammers are attained.

3.3 Nano size jammer

Panyim et al encourages the use of a huge number of tiny low-power jammers which are difficult to detect because they are difficult to detect because they are not visible to the small eye. In a network system, such jammers are introduced. With the overall jamming capability remaining unchanged, we attain a phase evolution of jamming throughput. Sensitive jammers are organized across the Network.

Experimental results from this paper indicate superior success at traditional jammers. Hence, the number of jammers will increase their jamming power and keep the power absorbed by the jam-mers steady. They made use of the scaling theory for percolation efficiency. We have shown the difficulty in detecting their jammers because of their small size low power and high performance in network building. To sum up, these four jammer positioning strategies are addressed in Table 3.1, in which we analyze how network knowledge includes jammer transmission power to detect the number of jammers and the difficulty.

IV. JAMMING DETECTION AND COUNTERMEASURE

Since jamming is a very dangerous attack on the DOS it is very important to successfully detect and countermeasure against it. This section covers some of those computer simulation and metric detection techniques. In this section we discuss current baseline jamming schemes and enhanced jamming identification and countermeasure. We evaluate the work for detection systems from and track measurements, costs, overheads, and implementation difficulties. Remember the form of jammer they're objected to for countermeasures, both punitive or aggressive, working upstairs, cost, difficulty of execution, and testing methods. Further examine the state of the network type for each of these approaches, and whether network expertise is needed.

V. ANALYSIS OF EXISTING APPROACHES

There are many methods available to countermeasure the detection of jamming threats. Many methods offer very good techniques, others aren't suitable for high quality performance. And, for each of them we think about hypothetical issues below.

The JAM mapping protocol solution only maps a jammed region that can not measure the type of attack that a node has encountered. The efficient detection of reactive jamming using this method also doesn't seem feasible. Mapping communications also reduces network overheads. Also it supports ram overhead as well. They use network metrics to measure network efficiency and determine whether or not certain nodes are a part of network jamming based on certain values. The network restrictions and metrics considered are rational, but the calculation and judgment in jamming detection do not seem to be in doubt. For the base station imitation technique all data must be copied to the whole replicated BS. Suppose there is a fixed period of time after alteration of all replicated BS data, then data loss occurs for the remainder of the BS sequence. In shirking strategies the communication overhead and network reconfiguration are discussed here. Multi-path routing can only be effective if there are several ways to access a destination from a single source, and if not one of the paths is blocked. Channel misery at the bridge layer would need cooperation between two contact nodes, which is an exclusive option of time.

5.1 Energy efficient jamming detection

We accept that a well-designed method of effective jamming detection is not possible when sur-veying the identification and countermeasure of jamming. A effective identification system should be able to distinguish whether a faulty radio link or

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 9428 - 9435

interference signals are causing the packet loss. The implementation of low-power jamming instruments such as reactive jammers is various. However, there is no low-power detection technique which offers the effective detection of low-power jamming.

5.2. Detection based on jammer classification

In the classification of jammers it is discovered that there are many types of jamming attacks which can be coordinated. Believe a jammer can be sensed by examining its description, depend-ing on its behaviour. The first step is to see if the jammer is gradual or fundamental. Then at se-cond level it categorizes the jammer as being positive, reactive and function-specific, or smart-hybrid. Adopting a top-down strategy can also appear easier as a bottom-up approach.

5.3 Anti-jamming in IEEE 802.11 networks

The IEEE 802.11 networks need very little analysis of the jamming and anti-jamming approach-es. Since the 802.11n IEEE is very different from the 802.11a / b / g IEEE predecessor, the ef-fects of using new 802.11n IEEE jamming and anti-jamming techniques could be very different. For example, Fig.2.1 shows that positive event hopping is not a viable countermeasure for jam-ming because of the channel bonding effect in IEEE 802.11n. The IEEE 802.11n technologies will promote the implementation of an effective reactive countermeasure by using or multiplexing the orthogonal frequency separation. For static networks, detection and countermeasure jamming is created and measured. The anti-jamming problem becomes more interesting in a mobile network world where jammers can switch and trigger jammer detection and localisation al-gorithms to malfunction. Therefore spatial retreats appear to be the only strategy applicable to the handheld nodes. Having a real alternative with reasonable overheads for mobile WSN remains an open question. The anti-jamming tool should provide fast identification and rapid reaction mechanism for mobile networks that can recognise a jammer easily and deter it.

VI. CONCLUSION

We also contributed to this analysis on jamming and jamming exploration techniques in networks by classifying and summarizing different approaches and addressing open research problems in the area. Specific jammers attack WSN in a variety of ways, and are markedly different in their hazard impacts. For eg, a persistent jammer absorbs fully available energy and confuses the network constantly but is easily detected. On the other hand, a sensitive jammer detects the medium and strikes only when there is a specific condition so it is a good choice for resource-limited equipment. In short, if a jammer is a standard low-power jammer, then a good jammer would jam the most positively

The jammer positioning work which is intended to help make jamming more efficient. For ex-ample, by strategically positioning them within the intrusion ranges of organizing nodes, the ef-fect of jammers can be reduced in order to achieve a better result of jamming. Even though a jammer is clever or successful, one or more competing anti-jamming methods are still possible. Since focusing on different forms of jamming detection and countermeasure strategies, we find that anti-jamming is such a fascinating topic that many approaches seek to solve this problem. Of example, artificial intelligence, game theory, cross layer, spatial elimination, usability testing, and frequency hopping have all been applied to this field. For one, certain processes.JAM, map the jammed region so that packets are not routed within that market. Any system senses jamming stations and switches, or transfers nodes to a new physical location. In summary, either choose to move the jammed station to an unjammed forward packet outside the jamming regions after find-ing jamming in network nodes, or switch it to an unjammed field only. The main open questions in this area include:

Energy-efficient surveillance scheme Jammer detection system recognition, and network jamming

Published by: The Mattingley Publishing Co., Inc.

and anti-jamming of mobile networks and IEEE 802.11n.

Although the most important job of an anti-jamming system is to accurately detect jammers, for example sensor networks for low-powered networks should be viewed as energy efficiency. Although a jammer can be detected, organization of the type of the observed jammer is actually difficult for a detection system.

REFERENCES

[1] Jamming and Anti-jamming Techniques in Wireless Networks: A Survey ,Intenational Jour-nal of Ad Hoc and Ubiquitous Computing.

[2] Jammer Localization in Multihop Wireless Networks Based on Gravitational Search,Security and communication networks,2018

[3] A Survey on Jamming Attacks and Its Types in Wireless Networks Journal of Technology Research and Management ISSN (Online): 2348-9006Vol 4Issue 6,2017