JES
Journal of Engineering Sciences

Vol 10, Issue 10, Oct /2019
ISSN NO: 0377-9254

MOBILE JAMMER

B .Nandha Kumar[1] Mrs.T.Sathiyabama[2]

[1]MCA Student, Department of Computer Applications (PG), Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore – 641049.

[2]Department of Computer Applications (PG), Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore – 641049.

ABSTRACT:

Dissimilar cellular-systems procedure signals differently, and yet, all cell-phone-network use radio-signals that can be interrupted or, even, blocked, totally. This project highlights the design of a easy, low-cost mobile phone-jammer and aims to now a result for the problem of unsuitable-use of the cell-phones in restricted and prohibited-areas. The main idea of jamming is the releasing of signal (noise) of the same-frequency .which is using by mobile-service-provider to overpower by destruct the user-signal. The creation of the jammer involved simple distinct workings, resistors, capacitors, inductors and transistors to make. the requisite frequency (noise) and then amplifies the incidence generated to range of 800 MHZ to 1.4 GHZ in order to competition the incidence of the mobile-phone being transmitted by the base-station. Relatively-satisfactory jamming of a mobile-signal was inveterate by the jamming of the signal of the mobile-phones in

2G and 3Gnetworks (UMTS / WCDMA) operated via

Safaricom, Airtell, Orange, and YU service-providers, when the phone indicate “no net”, thereby allow no call to go during, with no-intrusion to extra communication-means empirical. Overall recommendation is that more and more deeper-study is ideal to

produce more-stylish and better jamming plans, as not to affect the extra base-station-transmission scheme.

KEYWORDS: Mobile, phone, jammer, design, signal.

I. INTRODUCTION:

Wireless networking play sanim portantrole in achieving ubiquitous computing where network devices embedded in environment provide nonstop connectivity and services, so improving human’s quality of life. However, due to the exposed nature of wireless links, current wireless networks can be simply assault by jamming skill. Jamming can cause Denial-of- Service(DoS)problem which may result in several other higher-layer security problems ,although the seare of ten not adequately address (Wood et al,2007).

Jamming in wireless networks is defined as the disruption of existing wireless connections by decreasing the signal-to-noise ratio at receiver sides during the broadcast of interfere wireless signals. Jamming is different from regular network interferences since it describes the planned use of wireless signals in an attempt to disrupt relations where as inter ferencere fertoun intentional form soft disruptions

JAMMING TECHNIQUES :

Jamming make use of planned radio interferences to harm wireless relatives by care converse average busy, causing a source to back-off whenever it senses busy wireless average, or tainted sign usual at receivers. Jamming usually targets assault at the bodily finish but at time cross-layer attacks are hopeful too. In this part, we complex on diverse types of jammers and the post of jammers to use the jammed area.

TYPES OF JAMMER :

Jammers are hateful wireless nodes planted by an attacker to reason intentional interference in a wireless network .Depending upon the attack approach ,a jammer can also have the same or diverse capability from correct nodes in the scheme which they are attacking. The jamming effect of a jammer depends on its radio spreader power, location and influence on the net or the tar geted node . A jammer may jam sa net in various way stomake the jamming as effective as possible .Basically ,a jammer can be ei there lementary or

Journal of Engineering Sciences

Vol 10, Issue 10, Oct /2019
ISSN NO: 0377-9254

higher depending upon its functionality. For the simple jammers, we estranged them into two sub-groups: practical and hasty. The higher ones are also covert into two sub-types: purpose-specific and smart-hybrid. The detailed organization of different jammers can be found in Fig.1.

PROACTIVE JAMMER :

Proactive jammer transmit jamming (interfering) signals whe theror not there is data communication in a network .It send spacket sor random bit son the channel it is in service on, put all the others nodes on that canal in non-operating modes. though, it does not control channels and operates on only one channel until it senergy is exhausted. There are three basic types of sensible jammers: steady, illusory and random. From here on, whenever we use practical jammers it can mean all these three.

Steady jammer emits incessant, random bits without following the CSMA protocol (Xu et al, 2005). According to the CSMA mechanism, a legal node has to intellect the status of the wireless medium before transmitting. If the standard is incessantly idle for a DCF Inter frame Space (DIFS) duration, only then it is supposed to transmit a frame.

REACTIVE JAMMER :

Reactive jammer starts jamming only when it observe a network action occurs on a certain channel (Xu et al, 2005). As a result, a reactive jammer targets on compromising the response of a message. It can disturb both little and big sized packets. Since it has to constantly observe the network, reactive jammer is less force efficient than random jammer. However, it is much more hard to detect a reactive jammer than a proactive jammer because the packet delivery ratio (PDR) cannot be gritty precisely in practice. According to (Pelechrinis et al, 2011), the following are two different ways to perform a reactive jammer.

FUNCTION_SPECIFIC JAMMER :

Function-exact jamming is implement by having a pre-determined reason. In adding to being either practical or reactive, they can either work on a single channel to conserve energy or jam multiple channels and exploit the jamming throughput irrespective of the power usage. Even when the jammer is jamming a single straight at a time, they are not fixed to that canal and can modify their canal sac cording to their specific functionality.

SMART_HYBRID JAMMER :

We call them smart as of their power efficient and successful jamming nature. The main aim of these jammers is to magnify their jamming effect in the net they propose to jam. also, they also mind of them selves by conserving their energy. They place plenty energy in the right place so as to delay the statement bandwidth for the total net or a major part of the network, in very large networks. Each of this type of jammer can be implement edas both proactive and reactive, hence hybrid.

Journal of Engineering Sciences

Vol 10, Issue 10, Oct /2019
ISSN NO: 0377-9254

II . PLACEMENT OF JAMMERS :

OPTIMAL JAMMING ATTACKS :

The jammers and transmitters/receivers are distributed in a specified area use Poisson distribution. The possible values of winning broadcast are add to in terms of prospect. If a difficult area is jammed, next the monitor node is predictable to send the jamming note out of the area (using multi- hop transmission); this also suffer starting the jamming in the area. Using a dream of analysis and a arithmetical proof, the author sproved that the optimal tactic for the attacker tends to be quite soft and long-term.

JAMMING UNDER COMPLETE UNCERTAINTY:

Commander et al (2008) use a lively approach to calculate the location for placing jamming devices by integrating the limits of the locale to be jammed. They assume as quare-shape dareaen closes the network where the jammers are placed at the inter sections of a consistent grid. They formulate the problem as follows. If the jammer shave to optimally jamall the nodes of the net next somewhere should they be placed? Sub-problems are created and solve in arrange to attain an best result.

LIMITED_RANGE JAMMING ATTACKS:

The usual variety jammers contain the same transmission range as legitimate nodes; which makes their interference variety double that of the transmission diversity. Similarly, the partial-range jammers are formed with partly the broadcast array and hence ,interference variety equal to the broadcast range of the lawful nodes. Experiments on these jammers in an OPNET simulator show that the discovery of these limited-range jammers is firm as the broadcast power is half that of the lawful nodes. They finished to partial-range jammers are hard to note as they decrease the metrics that are mostly usually used for detection ,such as SNR and PDR.

JAMMING DETECTION AND COUNTER MEASURE :

- JAM: jammed-area mapping protocol
- ANT SYSYTEM
- Hybrid System
- Channal Suffering and Spatial retreat
- Using PDR with consistency checks
- Fuzzy interference system
- Game theoretic modeling

III.DISCUSSION :

In this section, we first analyze the potential issues in existing jamming exposure and countermeasure strategies. Then, we point out the open research challenges which need more research work.

ANALYSIS OF EXITING APPROACHES :

There are various solutions to the discovery of jamming attacks and anti-jamming countermeasures. Although various approaches present very good techniques with high quality results, others are not perfect. Therefore, we discuss the potential issues with each of them below.

The JAM mapping process advance only maps a jammed area; it is not able to quantify the type of attack experienced by a node. Moreover, it does not seem possible to efficiently notice reactive jamming using this scheme.

Fuzzy Interference machine is well-suited for detection of jamming in information warfare environments. In the algorithm “2 means clustering of neibor hood nodes,” a densely deployed network would yield better results contrast to a sparsely deployed network. Therefore, it is not suitable for networks with fewer adjacent nodes. Channel hopping can be implemented in denseors parse networks .There Is very little overhead required for implementing the hopping practice. Since this scheme uses carrier sense time as the metric, it is not possible to notice immediate jammers in the network.

OPENRESEARCH CHELLANGE:

After analyzing many jamming and anti-jamming technique, we end to there is currently no universal anti-jamming technique which deals with all kinds of jammers. compare to implementing a jammer, it is more difficult to diagram a discovery and countermeasure strategy. In addition, there are increasingly more newer wireless net technology (e.g. vehicular network, Wi Max), making anti-jamming a more difficult issue. In this part, we list a few middle research challenges which are still open problems, such as

Journal of Engineering Sciences

power competent jamming discovery, detection based on jammer classification, anti-jamming in IEEE 802.11n and wireless mobile networks.

ENERGY EFFICIANT JAMMING DETECTION

In surveying basic jamming detection and countermeasures, we understand that a well drafted reactive jamming discovery method is not accessible. A good detection mechanism should be able to distinguish if the package loss is caused by weak radio connect or due to interference signal. Moreover, there are various implementations of low-power jamming techniques such as imprudent jammers. However, there is no low-power discovery plan that provide efficient exposure of low-power jamming.

DETECTION BASED ON JAMMER'S CLASSIFICATION :

In classifying jammers ,we discover that there are different type of jamming attack which can be organized in Fig. 1. We think it is possible to detect a jammer based on its behavior by examining its classification. For instance ,the detectional gorithm can decide the character of jammers from top down in Fig. 1. The first step is to determine whether the jammer is basic or advanced. Then, it further classifies the jammer at the next level as being proactive, hasty, function-specific or smart-hybrid. Although a bottom- up come up to can also be taken, it seems to be easier to apply a top-down approach.

ANTI_JAMMING IN IEEE 802.11N NETWORKS :

There is very few explore work on jamming and anti- jamming techniques in IEEE 802.11n network. Since the IEEE 802.11n is very various from its predecessor IEEE 802.11a/b/g, the results of applying existing jammingandanti-jammingtechniquesonIEEE802.11n net can be very different. For example, XXXX shows that due to the channel bonding effect in IEEE 802.11n, proactive frequency hopping is not a suitable countermeasure for jamming. On the extra hand, since theIEEE802.11ntechnologyusesorthogonalfrequency dissection multiplexing (OFDM), it will be easier to apply an effective reactive counter measure.

ANTI_JAMMING IN WIRELESS MOBILE NETWORKS:

Most jamming discovery and counter assess are designed and evaluated in static network. The anti- jamming difficulty becomes more challenging in a mobile network environment where jammers may go and reason the malfunction of jammer detection and localization algorithms. So far, spatial retreats seem to be the only strategy implemented on the mobile nodes .Having an effective approach for wireless mobile network with suitable over head is still an open issue. The anti-jamming system for mobile networks must give fast-detecting and fast-reacting mechanism.

UNIVERSAL ANTI_JAMMING TECHNOLOGY:

Finally, we want to pose the final question: is it promising to have a single sensible anti-jamming solution which can deal with all types of wireless networks (whether it is static or mobile, sensor or Wi-Fi, infrastructure-based or ad-hoc) and notice all kinds of jammers (e.g. constant, deceptive, random, reactive, follow-on, channel hopping manage channel, implicit, flow jammers)? In addition, since we have so many effective jamming techniques, beside prevent eavesdropper's attack, can we use them for any useful purpose.

Journal of Engineering Sciences

IV.CONCLUSION :

In this extensive study on jamming and anti-jamming techniques in wireless network, we have contributed by classifying and summarizing various approaches and discussing open research issues in the field. Different jammers attack wireless network in various ways so that their attack effects are significantly different. For instance, a constant jammer consumes all resources available and continuously jams the network, but it is easily detected. On the other hand, a reactive jammer senses the average and only attack when a certain condition is satisfied, so it is a good choice for resource- constrained hardware. In summary, if a jammer is a periodic low power one, it is hard to be detected; a powerful jammer will certainly jam most of the networks but will be easily detected.

We also examine the placement of jammers which is considered to be helpful in making jamming more effective. For example, to achieve a better jamming effect, it is possible to reduce the power of jammers by tactically placing them in the interference range of communicating nodes. No matter how smart or effective a jammer is, there is forever one or more corresponding anti-jamming techniques. After elaborate on various types of jamming detection and countermeasure schemes, we discover that anti- jamming is such an interesting problem that many method are tried to solve this issue. For model, artificial intelligence, game theory, mobile-agent, cross- layer, spatial retreat, consistency check, and channel or frequency hopping have all been applied to this field. Some approach, e.g. JAM, map out the area that is jammed to avoid forwarding packets within that area .The basic open issues in this field includes:1)energy efficient discovery scheme, 2) jammerclassificationindetectionscheme,and3)jamming andanti-jamming in mobile networks and IEEE802.11nnetworks.

REFERENCE :

[1]Alnifie G, Simon R (2007) A multi-channel defense against jamming attack in wireless sensor network. In: Proceeding softhe3rdACMWorkshoponQoSand Security for Wireless and Mobile net,pp95–104.

[2]Alnifie G, Simon R (2010) MULEPRO: a multi- channel response to jamming attacks in wireless sensor net. Wireless Communications and Mobile Computing10(5):704–721.

[3]Bayraktaroglu E, King C, Liu X, Noubir G, Rajaraman R, Thapa B (2008) On the performance of IEEE.
802.11 under jamming. In: IEEE the 27th Conference on processor relations, pp 1265–1273.

[4]Bellardo J, Savage S (2003) 802.11 denial-of-service attacks: Real vulnerabilities and rational solutions. In: events of the 12th Conference on USENIX Security convention, pp 15–28.

[5]Broustis I, Pelechrinis K, Syrivelis D,Krishnamurthy SV, Tassiulas L (2009) FIJI: hostility implicit jamming in 802.11 WLANs. Security and retreat in contact net 19:21–40.

[6]ChiangJT, HuYC(2011)Cross-layer jamming detection and mitigation in wireless transmit networks. IEEE/ACM Transactions on net 19(1):286– 298.

Journal of Engineering Sciences