ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

# Wireless Communications Via Unjammed Bits Using Reactive Jamming

[1]ARIVUSELVI.P, [2]RAMYA.R, [3]KALA.M[1,2,3]
Master of Engineering in Computer Science and Engineering
arivu.skp@gmail.com
[4]Ms.VALARMATHI.S, M.E., Assistant Professor[4], Department of Computer Science and Engineering
Bharathiyar Institute of Engineering for Women
Tamil Nadu, India

**Abstract -** A reactive jammer jams wireless transmissions only if target devices are sending. Examine to constant jamming, reactive jamming is trouble to bring in and balance against Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) have been generally used as countermeasures against jamming attacks. However, both will fail if the jammer jams all frequency channels or has high transmit power. Propose an anti-jamming communication system that allows communication in the presence of a broadband and high power reactive jammer. The proposed system transfers messages by curb the reaction time of a reactive jammer. It does not assume a reactive jammer with limited spectrum coverage and transmit power, and thus can be used in scenarios where traditional approaches fail. Develop a prototype of the proposed system using GNU Radio. The experimental evaluation shows that when a powerful reactive jammer is presence, the prototype still keeps communication, whereas other schemes such as 802.11 DSSS fail completely.

**Index Terms -** Wireless Communication, Jamming Attacks, Reactive Jammer, Broadband.

## I. INTRODUCTION

Jamming attacks are well-known threats to wireless communication. A jammer uses a radio

frequency device to transmit wireless signals. Because of the collective environment of wireless standard, signals of the jammer and the sender collide at the receiver, and the signal reaction process is disrupted. Anti-jamming techniques have been extensively studied and proposed in the literature over the past decades). Frequency Hopping Spread Spectrum and Direct Sequence Spread Spectrum are dominantly used for the anti-jamming purpose. In FHSS, the sender and the receiver switch their communication channels periodically to avoid being jammed. In DSSS, the sender multiplies the original message with a pseudo-random sequence to obtain the spreading gain. If the jammer's power is not strong enough to overwhelm the DSSS signals with the spreading gain, the receiver can use the same

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

pseudo-random sequence to recover the message. Although FHSS and DSSS techniques were developed more than 30 years ago, until now these techniques and their variants are all limited by a common assumption that the jammer can only jam part of the communication channels or has limited transmit power. Unfortunately, if the jammer is broadband (i.e., it can jam all channels simultaneously) or has a high transmit power to overcome the spreading gain, these methods fail to maintain the anti-jamming communication. Hence, it seems that a broadband and high-power jammer is perfect and invincible. However, when such a jammer adopts reactive jamming Reactive jamming attacks are among the most effective jamming attacks. Compared to constant jamming, reactive jamming is not only cost effective for the jammer, but also hard to track and remove due to its intermittent jamming behaviors. When the direct is inactive but starts transmit a radio signal as soon as it senses activity.

## II. PROBLEM STATEMENT

In FHSS, the sender and the receiver switch their communication channels periodically to avoid being jammed. In DSSS, the sender multiplies the original message with a pseudo random sequence to obtain the spreading gain. If the jammer's power is not strong enough to overwhelm the DSSS signals with the spreading gain, the receiver can use the same pseudo random sequence to recover the message. Although FHSS and DSSS techniques were developed more than 30 years ago, until now these techniques and their variant sare all limited by a common assumption that the jammer can only jam part of the communication channels or has limited transmit power. Unfortunately, if the jammer is broadband (i.eit can jam all channels simultaneously) or has a high transmit power to overcome the spreading gain, these methods fail to maintain the anti-jamming communication. Hence, it seems that a broadband and high-power jammer is perfect and invincible.

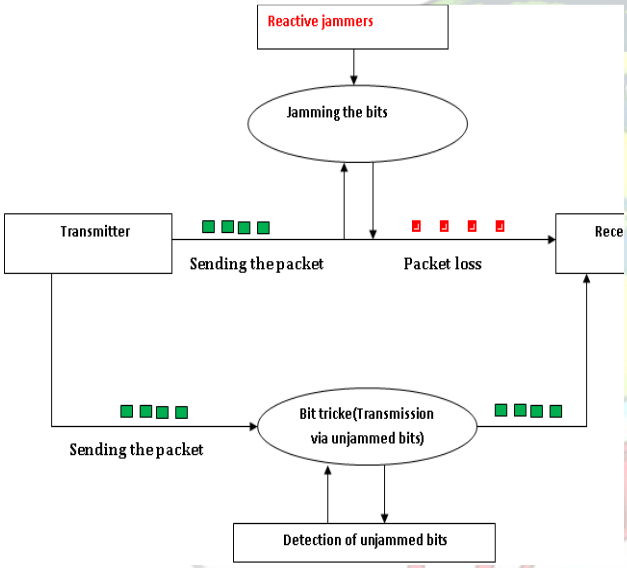
## III.SYSTEM ARCHIECTURE

A technique that can solve the major challenges in utilizing the un jammed bits survive din the reaction time of a reactive jammer to establish the anti jamming communication. Based on the proposed techniques, implemented a real-world prototype anti-jamming system, which can collect un jammed bits and assemble them into an original message under the broadband and high-power reactive jamming attacks. Developed novel techniques to harness the reaction time of a reactive jammer for anti-jamming communication and designed a communication system that integrates the proposed techniques to enable information exchange between wireless devices under broadband and high-power reactive jamming attacks and implemented a prototype using the USRP platform, and evaluated the performance on top of the prototype implementation. Since we are using the same path to transmit the data to make the data more secure we are going to implement MD5

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

algorithm to secure the file and then we transmit the file so that even if the data gets hacked the data cannot be misused my the attacker. Hence, it seems that a broadband and high-power jammer is perfect and invincible. However, when such a jammer adopts reactive jamming strategy, a closer examination on the jammer's behavior reveals its "Achilles Heel".




Jamming attacks are well-known threats to wireless communication. A jammer uses a radio frequency device to transmit wireless signals. Anti-jamming techniques have been extensively studied and proposed in the literature over the past decades. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are dominantly used for the anti-jamming purpose. In FHSS, the sender and the receiver switch their communication channels periodically to avoid being jammed. In DSSS, the sender multiplies the original message with a pseudorandom sequence to obtain the spreading gain. If the jammer's power is not strong enough to overwhelm the DSSS signals with the spreading gain, the receiver can use the same pseudorandom sequence to recover the message. Although FHSS and DSSS techniques were developed more than 30 years ago, until now these techniques and their variants are all limited by a common assumption that the jammer can only jam part of the communication channels or has limited transmit power. Unfortunately, if the jammer is broadband or has a high transmit power to overcome the spreading gain, these methods fail to maintain the anti-jamming communication.

**NODE CREATION AND ROUTING:**

A wireless network is created. All the nodes are randomly deployed in the network area. Our network is a mobile network, nodes are assigned with mobility (movement).Source and destination nodes are defined. Data transferred from source node to destination node. Since we are working in mobile network, nodes mobility is set ie., node move from one position to another Adversary Model The goal of the adversary is to prevent the sender(s) from communicating with all, or a subset of the intended receivers. For this purpose, the adversary deploys a set of jamming devices capable of collectively jamming any J frequency bands. The jamming devices can switch between frequency bands on a per-slot basis. Note down with committed hardware, the jammer might be bright to hop at a much higher rate than that of regular nodes. However, the jammer's hopping rate is limited by the time that he has to remain on a particular band (dwell time) to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

corrupt a sufficient number of bits from the targeted packet(s).

**PACKET TRANSMISSION:**

Transmission intervals between the sender and the receiver to deal with pollution attacks. Note that the common transmission intervals should be confidential to the jammer, such that the jammer cannot follow them to jam the communication. In traditional FHSS and DSSS systems, a shared secret key is used to generate common frequency hopping patterns or spread spectrum sequences only known to the communicators for the anti-jamming purpose. Similarly, the sender and the receiver can utilize such a shared secret key to generate their transmission intervals.

**DETECTION OF UNJAMMED BITS:**

Jamming signals can introduce a large distortion to signals transmitted by the sender, since the goal of the jammer is to corrupt the signals. If a received symbol is jammed, it may greatly deviate from its ideal point in the constellation diagram and can hardly be recovered. To get more insights in this process, we perform experiments to examine the impacts of jamming on symbol locations. To collect the received symbols which are radio frequency (RF) front ends equipped with analog to Digital (AD) and digital to analog (DA) converters. In our experiments, three USRPs are used as the sender, the receiver, and the jammer, respectively, each of which is connected to a computer. Automatic gain control (AGC) is employed by USRPs. We set the bit rate as 1Mbps, carrier frequency and modulator as QPSK.

## IV. JAMMING TECHNIQES

Jamming makes use of intentional radio interferences to harm wireless communications by keeping communicating medium busy, causing a transmitter to back-off whenever it senses busy wireless medium, or corrupted signal received at receivers. Targets attacks at the physical layer but sometimes cross-layer attacks are possible too. In this section, we elaborate on various types of jammers and the placement of jammers to maximize the jammed area.

**Types of jammers**

Jammers are malicious wireless nodes planted by an attacker to cause intentional interference in a wireless network. Depending upon the attack strategy, a jammer can either have the same or different capabilities from legitimate nodes in the network which they are attacking. The jamming effect of a jammer depends on its radio transmitter power, location and influence on the network.A jammer may jams a network in various ways to make the jamming as effective as possible. Basically, a jammer can be either elementary or advanced depending upon its functionality. For the elementary jammers, we divided them into two sub-groups: proactive and reactive. The advanced ones are also classified into two sub-types: function-specific and smart-hybrid. The detailed classification of different jammers can be found.

**Proactive jammer**

Proactive jammer transmits jamming signals whether or not there is data communication in a network. It sends packets or random bits on the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

channel it is operating on, putting all the others nodes on that channel in non-operating modes. However, it does not switch channels and operates on only one guide until its power is tired. There are three basic types of proactive jammers: constant, deceptive and random. From here on, whenever we use proactive jammers it can mean all these three. Constant jammer emits continuous, random bits without following the CSMA protocol According to the CSMA mechanism, a legitimate node has to sense the status of the wireless medium before transmit. If the medium is constantly inoperative for a DCF Interface Space (DIFS) duration, only then it is Supposed to transmit a frame. If the direct is found busy during the DIFS interval, the station should defer its transmission. A constant jammer prevents rightful nodes from communicating with each other by causing the wireless media to be constantly busy. This type of attack is energy inefficient and easy to detect but is very easy to launch and can damage network communications to the point that no one can communicate at any time. Deceptive jammer continuously transmits regular packets instead of emitting random bits It deceive other nodes to believe that a legitimate transmission is taking place so that they remain in receiving states until the jammer is turned off or dies. Compared to a constant jammer, it is more difficult to detect a deceptive jammer because it transmits legitimate packets instead of random bits. Similar to the constant jammer, deceptive jammer is also energy inefficient due to the continuous transmission but is very easily implemented. Arbitrary jammer irregularly transmits either random bits or regular packet into network. Contrary to the above two jammers, it aims at saving energy. It continuously switches between two states: sleep phase and jamming phase. It sleeps for a certain time of period and then becomes active for jamming before returning back to a sleep state.

**Reactive Jammer**

Reactive jammer starts jamming only when it observes a network activity occurs on a certain channel. As a result, a reactive jammer target on negotiation the reception of a message. It can disrupt both small and large sized packets. Since it has to constantly monitor the network, reactive jammer is less energy efficient than random jammer. However, it is much more difficult to detect a reactive jammer than a proactive jammer since the packet delivery ratio (PDR) cannot be determined accurately in practice.

## V. IMPLEMENTATION AND EVALUATION

We develop a prototype anti-jamming communication system, which we name as Bit Trickle, to facilitate the experimental evaluation of the proposed techniques under reactive jamming. The model system consists of a sender and a receiver, both implement as a USRP connected to a commodity PC that runs the sender (receiver) program. . For both the transmitter and receiver component, we set the parameter “samples per symbol” the minimum value supported by GNU Radio to reduce the processing delay

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

## VI. CONCLUSION

To developed an anti-jamming system that can enable wireless communication when a broadband and high power reactive jammer is present. The designed system delivers information by harnessing the reaction time of a reactive jammer. It does not assume a reactive jammer with limited spectrum coverage and transmit power, and thus can be used in scenario where traditional approaches fail. We implemented a trial product of such system based on GNU Radio. Our results showed that the prototype achieved a reasonable throughput when 802.11 DSSS and GNU Radio benchmark were completely disabled by the jammer.

## REFERENCES

[1] L. Baird,W. Bahn, and M. Collins. Jam-resistant communication without shared Secrets through the use of concurrent codes. Technical report, US Air Force Academy, 2007.

[2] A. J. Berni and W. D. Greeg. On the utility of chirp modulation for digital signaling.IEEE Trans.on Communications, 21:748–751, 1973.

[3] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In Proceedings of the 14th ACM international conference on Mobile computing and networking (MobiCom '08), pages 116–127, 2008.

[4] D. Cabric, A. Tkachenko, and R. W. Brodersen. Experimental study of spectrum sensing based on energy detection and network cooperation. In ACM TAPAS '06:Proceedings of the First International Workshop on Technology and Policy for Accessing Spectrum, 2006.

[5] J. Chiang and Y. Hu. Dynamic jamming mitigation for wireless boradcast networks.In Proceedings of IEEE International Conference on Computer Communications (INFOCOM '08), 2008.

[6] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. Introduction to Algorithms, 2nd. MIT Press, 2001.

[7] B. Danev, H. Luecken, S. Capkun, and K. E. Defrawy. Attacks on physical-layer Identification. In Procceedings of the 3nd ACM Conference on Wireless Networking Security (WiSec '10), pages 89–98, March 2010.

[8] M. Edman and B. Yener. Active attacks against modulation-based radiometric identification. Technical Report TR 09-02, Rensselaer Polytechnic Institute,2009.

[9] A. Goldsmith. Wireless Communications. Cambridge University Press, August 2005.

[10] S. Hengstler, D. P. Kasilingam, and A. H. Costa. A novel chirp modulation Spread spectrum technique for multiple access. In Proceedings of the IEEE International Symposium on Spread Spectrum Techniques and Applications pages 73–77, September 2002

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

[11] H. Kim and K. G. Shin. In-band spectrum sensing in cognitive radio networks: energy detection or feature detection? In MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking, pages 14– 25, 2008.

[12] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of 2nd ACM Conference on Wireless Networking Security (WiSec '09), March 2009.

[13] M. Li, I. Koutsopoulos, and R. Poovendran. Optimal jamming attacks and Network defense policies in wireless sensor networks. In Proceedings of IEEE International Conference on computer Communications (INFOCOM '07), 2007.

[14] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang. Defending DSSSbased roadcast Communication against insider jammers via delayed seed-disclosure. In Proceedings of the 26th Annual Computer Security Applications Conference ACSAC '10, December 2010.

[15] Y. Liu and P. Ning. Poster: Mimicry attacks against wireless link signature. In Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS'11), 2011.