ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 4, Issue 3, DOI: 10.29027/IJIRASE.v4.i3.2020.681-685, September 2020

Packet Hiding Techniques for Jamming Attacks

V .Divya[1], Dr.K.R.Radhika[2]
Department of ISE, B.M.S College of Engineering,
Bangalore, under VTU, Belagavi, India
Email: divya.venkat95@outlook.com

***Abstract* —Wireless local area network has a proliferation of nature leads to a very dangerous intrusion attack, known as Jamming. This Intrusion attack uses wireless technologies as a medium to launch Denial of service attack over these vulnerable networks. The recently jamming attack has been referred to as a very risky attack model. However, experts have been working on these security protocols. Although challengers with interior information and data privacy can execute a jamming attack which is hard to analyze, detect and protect. In this project, we have worked on particular problems of jamming attack in WLAN. In these jammed networks the attackers are active only for some time till the attack is planned as per the level of importance of the data/message shared and according to that attack will be executed. Here we have demonstrated a particular jamming attack by executing real-time packet transmission at the physical layer, to diminish these issues we have established three encryption methods of the physical layer characteristics for preventing from jamming attack. We examine the safety of the encryption hidden techniques and asses algorithmic and transmission overheads.**

Keywords—Jamming attack, wireless Local area networks, jammed networks, Encryption methods, packets, Wireless.

I. INTRODUCTION

As we get in-depth about encryption techniques for the jamming attack, let us understand what jamming attack in WLAN is all about.

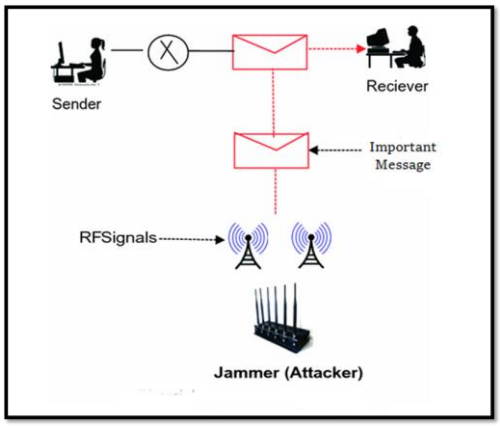

Fig 1: Pictorial view of jamming attack

The jamming attack is harder to detect and counter them as it's done silently without any evidence until the data is lost. The jamming attack is a subgroup of the denial of service attack, where the malignant connections to block genuine nodes without any intrusion in the wireless network, they generally target on information consisting of legal or private messages with High importance. The jamming attack is used as a tool in the military for launching attacks on terrorist conversations. Generally jamming is not caused purposely it could be due to noise or disturbance in a network.

Among all the technologies WLANs have rapidly increased all over the world for local close networks, that's the reason they have been using in various fields like military, pharmaceutical, education, manufacturing, agriculture, and research hence the significance of the wireless local area network technology is standing prominent. WLAN channels are described through frequencies (by sending unnecessary packets of that particular frequency) due to this there are a lot of chances for a jamming attack. In WLAN what jamming attack does is it causes terrific traffic by crashing into the systems and flooding the server with the request, which uses the entire resources in a node and the operator cannot communicate to different computers of the same local network itself and these are undoubted done by the hackers to expose the data and misuse it.

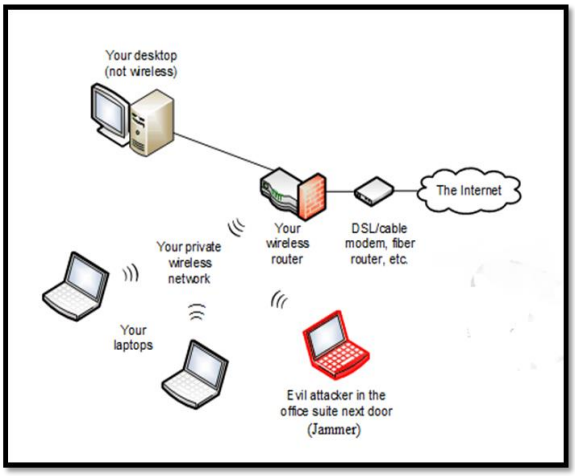

Fig.2: Jamming attack in WLAN

The jamming attack is referred to as one of the most Threatful attack occurring over the wireless networks. These wireless mediums are system network without using any cables to connect them instead it connects the web through waves of radio signals for mobile phones, laptops, Desktops, etc. which benefits the business by saving money on those expensive connector wires into the houses, offices or could between systems in a LAN. The roots of the wireless

mediums are radio signals which are captivating at the physical layer of the operating system. Wireless technologies are signified as equivocal due to its vast range of technologies and it also developing to be most essential by getting the globe closer by using in almost all domains. Network security I sone of the most crucial elements in the world of internet because n number of internet attacks were filled over the years since it's been developed.

Wireless mediums are more prone to be attacked especially for the denial of service attack by attacking the genuine users of that particular WLAN who use that website or system by aiming at the message which carries very important information. Wi-Fi communication is the transmission of frequencies by revealing the physical layer for jamming. Study says that the research concentrates on protecting on speech interaction with the help of methodology of broad-spectrum, these methods are executed by methods of broad-spectrum by giving bit by bit safety for increasing the quasi clatter program only for connectivity, Due to this the waves expand to a huge band of periodic waves by creating a restricted amount of power of supply for the jammer by making the jammer to give complete frequency, only such techniques provide security for the wireless mediums which are considered as threatful. Broken congestion can lead to the squalor of speech condition, hence this technique is used to provide safety for the speech connectivity to counter Congestion known as Anti Jamming techniques.

II. LITERATURE SURVEY

Acharya and Thuente worked learned the effects of the particular jamming attacks happening and their goals on different packs at the OSI model, which categorize them. The opponent uses internal packet scheduling data or packet communication.

Law et al. Suggested that the approximation if the distribution and transformation of the internal packet of various packs which is based on the network traffic study. Later on, the communication of different levels was predicted and analysis to its approximated data and its timing with the help of the model. The authors selected some particular jamming strategies of the OSI model protocols.

Brown, James and Sethi think that the issue disturbing the encoded wireless network using jamming also in this paper they have to concentrate on the jamming at the OSI layer by misusing the AODV and transport layer protocols. Strategies in the genuine network which can find the attacker packet kind, but it is assumed that the encrypted data is all covered with the header of the packet such a way that all packets are of the same size, time and order for detecting.

Cagalj, Capkun and Hubaux wireless detector of the network which is categorized by the vulnerable jamming attack in a radio station and DOS attack. An attacker can mask up the network consisting of sensor which should be detected for jamming the subsection of the network this method avoids filing the report the sensor network result, hence although this method would sense different nodes of the network.

This suggests the 3 solutions first which is based on the wired sensor and secondly, the frequency hopping and lastly is the novel idea, using this mathematical paradigm was developed. Where encryption methods of such strategy helped me to develop the code according and work on the cryptographic methods in the protocols.

III. METHODOLOGY

The issue of Jamming attack is one of the bigger threat we are facing in today's world. All the antagonist are aware of all the hidden clandestine of network and implementation strategies of that network procedures at network layer heap as planned

The antagonist with all the network knowledge about the jamming attack and targetting message which is very important for the attacker for seeking internal information. The hacker aims the Route reply or route request packets at the layers to route processes.

To overcome this issue we have developed three encryption techniques for hiding the message packets which are supposed to be very important without any sort of packs of a data loss.

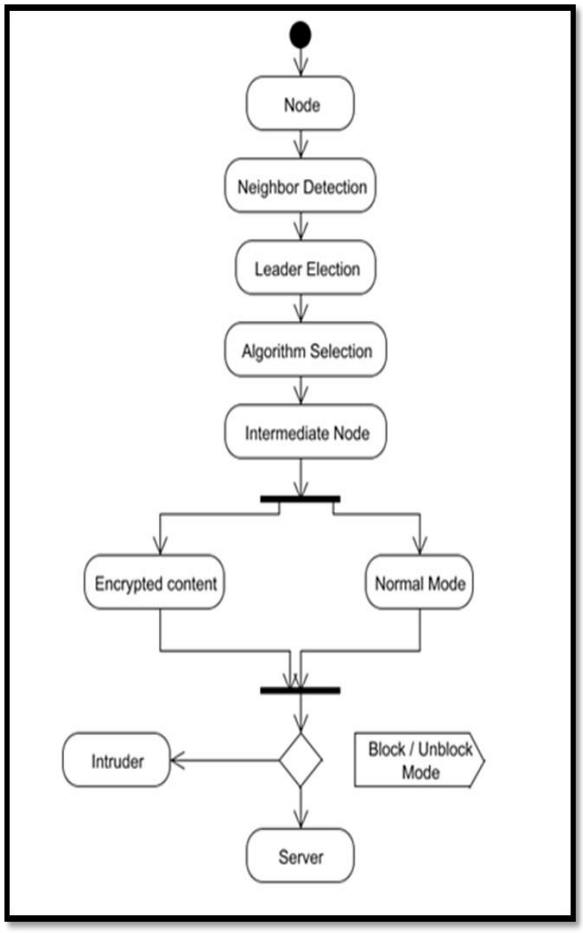

Fig 3: Flow chart for prevention of jamming attack

Those encryption algorithm techniques as follows:-

A. Real Time Packet Classification or Normal Mode

In this encryption method, real-time packets are transferred. In the OSI model which consists of a physical layer, there is a small pack of packets which are broken down into fragments.

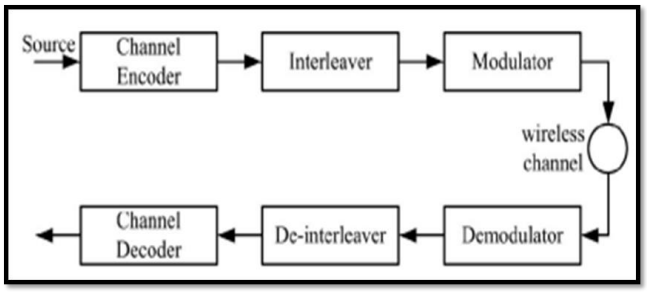

Fig4: Communication model of Real time packets transmission

For instance, a packet/data "msg" is encrypted, interspersed, Fine-tuned afore the packets are transferred through the wireless medium. At the other end i.e the receiver. The packets there are de-tuned, de-interspersed to recuperate he real packet "msg". Nodes 'P' and 'Q' connect through a wireless medium in the transmission range of 'P' and 'Q' between there consists of a jamming link node "jammer" for instance "A" want to communicate with "B" so "A" transfers a packet "msg" to "B" and a "jammer" categorize a message "msg' by getting only starting bytes of the message. The jammer can debase "msg" without being able to recover them when corrupted with its signal "B".

B. Strong Hiding Commitment Technique

In this encryption technique, there is a strong encryption method which is built on the symmetric cryptography. Let us get in detail. This Technique delivers a strong encryption method which is all computed and interacted to keep the overheads as less as possible.

In this module, it implemented with an encryption key using this method of cryptography like DES. Later on, the information is distributed into packets, where cryptography techniques are applied and encrypted with the key. Next to that few bits are added along with the data that is encrypted known to be a padding strategy for hiding the data. Later data is transformed and transferred to the receiver end node.

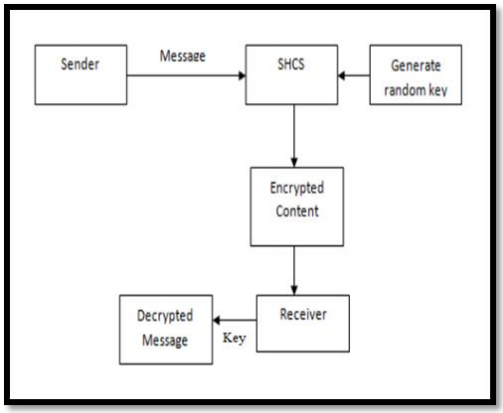

Fig 5: Process of SHCT Encryption method

For instance, think that the transmitter wants to send a message to the receiver, so now he builds the "message" first which is a function of cryptographic processes known to be as permutations and "S" is the irregular key of length "L" note, the key can be f the desired length according to the requirement. After the reception of data when the receiver receives the data to the destination node and "R" can be computed easily.

C. Cryptographic Puzzle Hiding technique

In this encryption technique, the use we are using two internal encryption algorithms i.e using time puzzle and another is a mathematical equation puzzle. Here A transmitter "T" sends a data "M" for communication, The receiver should be selecting any key (required length) as per his desire or wish for unlocking the puzzle. The transmitter 'T" would construct a puzzle [Key, Time]. The puzzle is the creator task to construct and "t" is referred to as time, time is given here for this algorithm so that the puzzle expires and no one can misuse is. So the time is entered for solving the puzzle constructed by the transmitter for revealing the message. In this, the limit is measured in seconds and they are directly relying on the antagonist "J" capacity to break the puzzle within the given time per sec. Once the puzzle is constructed denoted as "P" is transmitted to the receiver. And any receiver can break the puzzle when the key is computed.

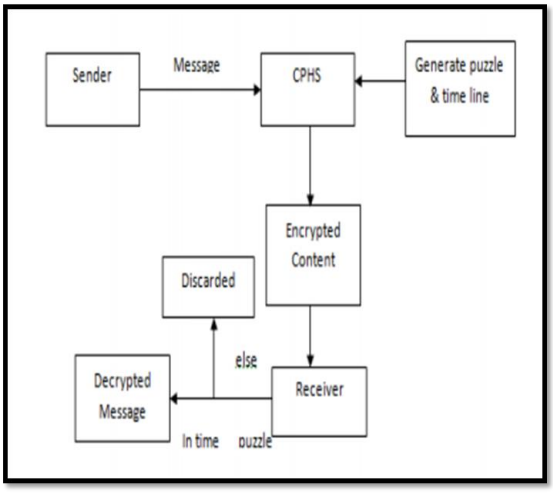

Fig.6: Process of puzzle hiding encryption technique

D. Hiding Technique based on All-Or-Nothing Transformations

In this encryption technique which might look similar to the strong Hiding technique but it is not, encryption methods are different the process of execution is different. Here the message/ date are converted with the help of the above algorithm afore its transmission to keep it as it is un-crypto graphed. Hacker fails to play his role of classification of packets unless the fake message which is sent corresponding to the real data/packet which is been transmitted to the receiver is receive and also it should be reversed transformed. Packets "P" is divided into small

packs P= [P1, P2, P3...] acting as key inputs for the fake packets p= [p1, p2, p3...] sent through a wireless network

IV. RESULT AND ANALYSIS

In this we would be using the three java program files one for the Server, intermediate/intruder and node with the help of the NetBeans application in windows. Ones their file is "run file" it starts executing and works as per expected.

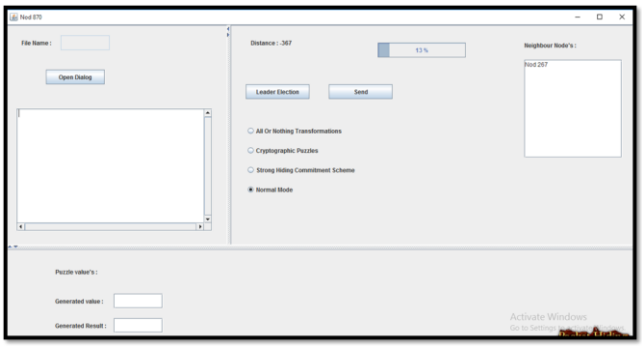

Fig 7: Front end of the application to execute

In figure 7 which consist of "open dialogue box" where the message can type to transmit., next is "leader election" this clicked every time you run the program initially, it designates a single process as it organises the task in a distributed network. There are "4 option" button to select which mode of encryption which is to be selected for execution in "block mode". "Puzzle value" on the bottom of the screen is for the cryptographic puzzle encryption techniques where it generates a puzzle with tie puzzle and executes. "Send" is to send the packets/message. Next in the server file, there are two modes one is "BLOCK MODE" and "UNBLOCK MODE" block mode is when there is an attacker in the network, and unblock mode is no intruder or attacker existing.

A. Real Time Packet Classification or Normal mode

In this encryption technique using the block mode, we are executing for the paper. Where the message is sent from the node as below picture

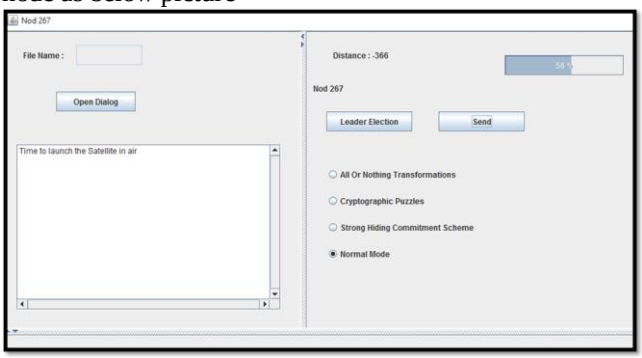

Fig 8: Message which is to be sent in normal mode

After the message is sent and in the server-side it selected as block mode ones it's in block mode and message is sent the intruder gets a message as ' intruder block the packets' which means the packets are blocked and corrupted. So hence the below encryption methods are to be applied

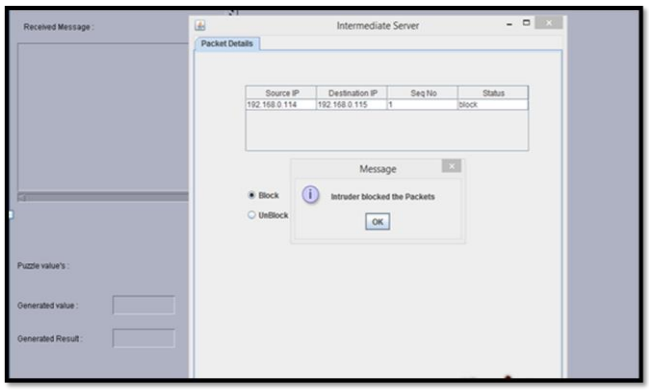

Fig 9: After its attacked and the message it displays

B. Strong Hiding Commitment Technique

Strong hiding encryption techniques where a strong key has to be entered when a message has to be sent to the receiver node

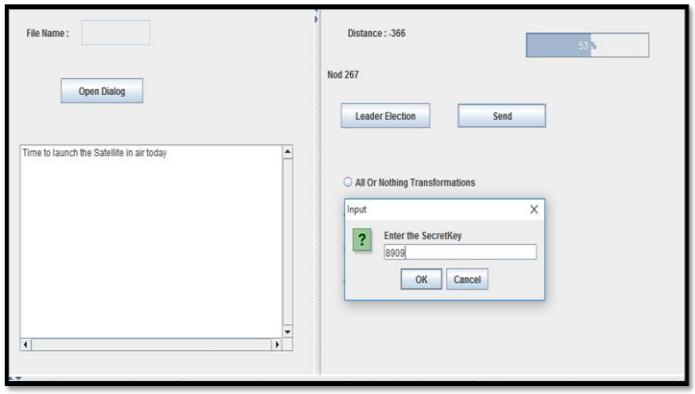

Fig 10: The key to being entered for SHCS

Then in the server-side, he has to enter the key and he receives the key

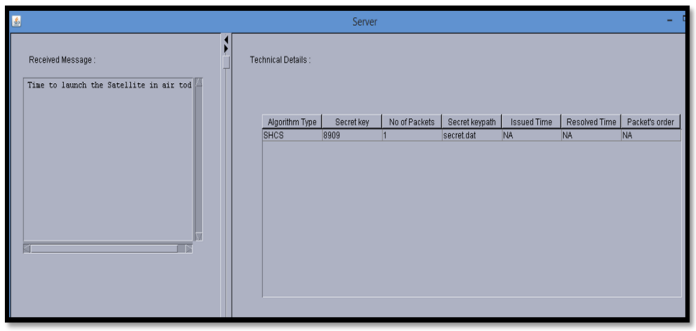

Fig 11: Message received

C. Cryptographic Puzzle Hiding technique

In this cryptographic method we use to puzzle technique, one is by solving a mathematical equation and the other is time puzzle. Where the message is entered in the dialogue box and sent to the receiver. Before that, it generated the puzzle and time puzzle and sends. Then when received the message the receiver has to solve the mathematical equation in the given time or else it would get expired.

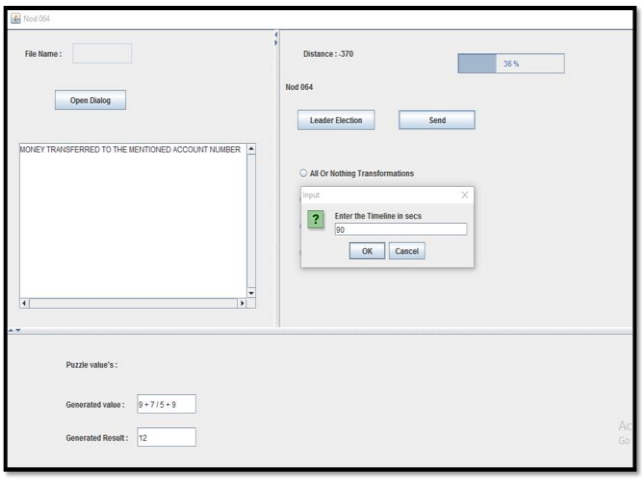

Fig 12: Set time in seconds to solve the puzzle

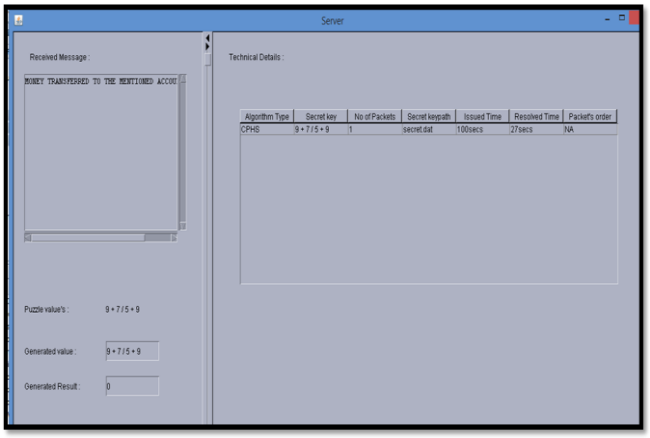

Fig 13: puzzle solved within the given time and message delivered

.

D.*Hiding Technique based on All-Or-Nothing Transformations*

In this cryptographic method, we use the key encryption method to transmit the packets from the source. Which is similar to strong hiding encryption method but the encryption process varies completely in this.

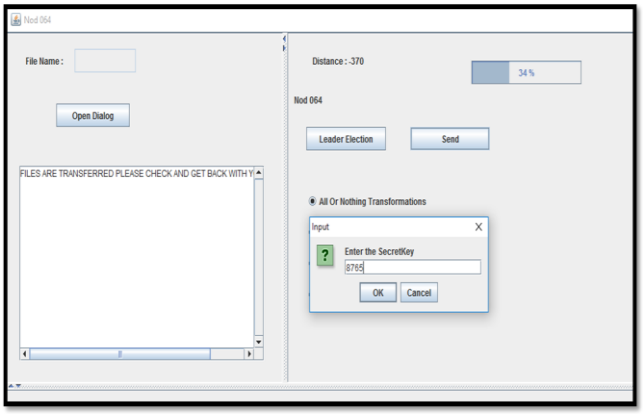

Fig 14: key generated to send the packets

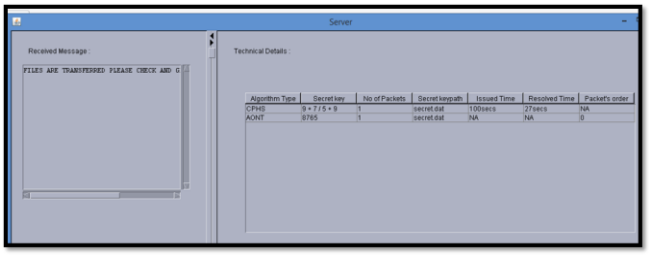

Fig 14: Message delivered after the key is entered

V. CONCLUSION

In this paper, we have discussed and provided prevention techniques for the jamming attack through a wireless local area network. We have also studied the in-house antagonist design where the hacker is playing a role in the network and he knows all te the process and its planned specifications of the distributed privacy of a network.

We have also executed in a way where the hacker has categorized the communication message in real-time by decrypting the transmitted packet. We analyzed the effects of the jamming attack on the routeing layer and MAC layer and provided Four encryption techniques to battle with it. Thus through these techniques, a drastic amount of packet loss can be prevented and saved

Acknowledgement

I would like to express my sincere gratitude to my guide Dr Radhika K.R for allowing me to write this paper and for providing her valuable guidance and encouragement throughout to implement this project. It was my great privilege to work and study under her guidance.

REFERENCE

[1] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.

[2] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.

[3] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti-Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[4] R. Rivest, A. Shamir, and D. Wagner, "Time-Lock Puzzles and Timed-Release Crypto," technical report, Massachusetts Inst. Of Technology,.

[5] D. Stinson, "Something about All or Nothing (Transforms)," Designs, Codes and Cryptography, vol. 22, no. 2, pp. 133-138.

[6] P. Tague, M. Li, and R. Poovendran, "Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution," Proc. IEEE Int'l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC), 2007

[7] D. Thuente and M. Acharya, "Intelligent Jamming in Wireless Networks with Applications to 802.11 b and Other Networks," Proc. IEEE Military Comm. Conf. (MILCOM), 2006.

[8] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders, "Reactive Jamming in Wireless Networks: How Realistic Is the Threat," Proc. ACM Conf. Wireless Network Security (WiSec), 2011.