International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No 4, Issue No 6, November, 2016

Jamming avoiding communication using MIMI-OFDM based defense mechanism

G. Karthiga
Department of Electronic and Communication Engineering
Sri Manakula Vinayagar Engineering College
Pondicherry, India

M. Julie Therese
Department of Electronic and Communication Engineering
Sri Manakula Vinayagar Engineering College
Pondicherry, India

Abstract: Wireless sensor networks utilize open transmission media they are prone to radio jamming attacks. Jamming attack as the attack efficiency is maximized while the risk of being detected is minimized. Currently, there are no effective anti-jamming solutions to secure OFDM wireless communications under reactive jamming attack. On the other hand, MIMO has emerged as a technology of great research interest in recent years. These attacks are easy to launch but difficult to defend. These attacks may lead to low network throughput because of jamming signals. Failure of data transmission in sensor networks is due to corruption of packets by reactive jammers. A number of defense techniques have been proposed in recent years to deal with these jammer attacks. However, each defense technique is suitable for only a limited network range and specific jamming conditions. This paper proposes a novel based defense mechanism approach to detect and isolate the reactive jammers by using status interactive channel tracking and sender signal enhancement service to avoid all the problems.

Keywords: Sensor networks, jamming attack, OFDM, Multiple in multiple out (MIMO)

I. INTRODUCTION

Multiple input, multiple output-orthogonal frequency division multiplexing (MIMO-OFDM) is the dominant air interface for 4G and 5G broadband wireless communications. It combines multiple input, multiple output (MIMO) technology, which multiplies capacity by transmitting different signals over multiple antennas, and orthogonal frequency-division multiplexing (OFDM), which divides a radio channel into a large number of closely spaced sub channels to provide more reliable communications at high speeds. Research conducted during the mid-1990s showed that while MIMO can be used with other popular air interfaces such as time division multiple accesses (TDMA) and code division multiple access (CDMA), the combination of MIMO and OFDM is most practical at higher data rates [1]. MIMO-OFDM is the foundation for most advanced wireless local area network (wireless LAN) and mobile broadband network standards because it achieves the greatest spectral efficiency and, therefore, delivers the highest capacity and data throughput.

MIMO multiplies the capacity of a radio link by transmitting multiple signals over multiple, co-located antennas. This is accomplished without the need for additional power or bandwidth. Space–time codes are employed to ensure that the signals transmitted over the different antennas are orthogonal to each other, making it easier for the receiver to distinguish one from another. Even when there is line of sight access between two stations, dual antenna polarization may be used to ensure that there is more than one robust path. A key advantage of OFDM is that fast Fourier transforms (FFTs) may be used to simplify implementation. Fourier transforms convert signals back and forth between the time domain and frequency domain. Consequently, Fourier transforms can exploit the fact that any complex waveform may be decomposed into a series of simple sinusoids. In signal processing applications, discrete Fourier transforms (DFTs) are used to operate on real-time signal samples. DFTs may be applied to composite OFDM signals, avoiding the need for the banks of oscillators and demodulators associated with individual subcarriers. Fast Fourier transforms are numerical algorithms used by computers to perform DFT calculations [2].

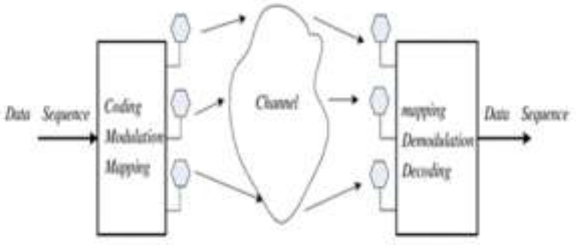

Figure: 1. MIMO based system

Modern society has become heavily dependent on wireless networks to deliver information to diverse users. People expect to be able to access the latest data, such as stock quotes and traffic conditions, at any time, whether they are at home, at their office, or travelling. The emerging wireless infrastructure provides opportunities for new applications such as on-line banking and electronic commerce. Wireless data distribution systems also have a broad range of applications in military networks, such as transmitting up-to-date battle information to tactical commanders in the field.

A. *Jamming Attacks*

The traditional defenses against jamming include spread spectrum techniques such as direct sequence and frequency hopping. With direct sequence, the data signal is multiplied by a pseudo-random bit sequence, referred to as pseudo-random noise code. As a result, the signal is spread across a very wide bandwidth such that the amount of energy present at each particular frequency band is very small. In frequency hopping systems, the signal only occupies a single channel at any given point of time. The carrier frequency is constantly changing according to a unique sequence. Both techniques spread signal over a wide frequency band, which makes it harder for an adversary to find and jam the signal [3] .

In this paper we investigate efficient anti-jamming schedules for data broadcast. Wireless communications are to communicate with any type of information with anyone, anytime, from anywhere through wireless technology. In wireless technologies, jamming in wireless networks has become a major research problem due to the ease in blocking communication in wireless networks**.**

In our schedules, each packet is encoded by an error-correcting code, such as Reed-Solomon, which allows the schedule to minimize both waiting time of the clients and the staleness of the received data. As power supply is the most important constraint for practical jammers, we focus on jammers that have certain restrictions on the length of jamming pulses and the length of the intervals between subsequent jamming pulses. To the best of our knowledge, this is the first study that investigates anti-jamming schedules for wireless data distribution systems [4].

II. LITERATURE REVIEW

Gang Zhou et al., introduced Jamming is a very effective denial-of-service attack that renders most higher-layer security mechanisms moot—yet it is often ignored in WSN design. We show that an interrupt jamming attack is simple to perpetrate in software using a MICA mote, is energy efficient and stealthy for the jammer, and completely disrupts communication. Solutions are needed to mitigate this insider threat even if more powerful attackers are not thwarted. We present DEEJAM, a novel MAC-layer protocol for defeating stealthy jammers with IEEE 802.15.4-based hardware, to address this problematic area. Results show that DEEJAM defeats the otherwise devastating interrupt jammer, and achieves a packet delivery ratio of 88% in the presence of a pulse jammer. To the best of our knowledge, this work is the first to confront multiple types of jamming on common WSN hardware with solutions that are shown empirically to enable continued communication despite an ongoing attack.

Khattab Daniel Mosse et al., [6] Jamming is a serious security problem in wireless networks. Recently, software-based channel hopping has received attention as a jamming countermeasure. In particular, proactive, or periodic, channel hopping has been studied more extensively than reactive hopping. In this paper, we address the question of which of the two defense strategies, namely proactive and reactive channel-hopping, provides better jamming resiliency than the other. Our results show that reactive defense provides better jamming tolerance than proactive when considering communication availability.

Tassiulas L et al., [7] provided an extensive study on jamming and anti-jamming techniques in wireless networks; we have contributed by classifying and summarizing various approaches and discussing open research issues in the field. Different jammers attack wireless networks 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 medium 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.

Srikanth V. Krishnamurthy ey al., [5] explained the shared nature of the medium in wireless networks makes it easy for an adversary to launch a Wireless Denial of Service (WDOS) attack. Recent studies, demonstrate that such attacks can be very easily accomplished using off-the shelf equipment. To give a simple example, a malicious node can continually transmit a radio signal in order to block any legitimate access to the medium and/or interfere with reception. This act is called jamming and the malicious nodes are referred to as jammers.

Deepti C proposed [8]a trigger identification service for reactive jamming attack in wireless sensor network is simulated to achieve minimum end-to-end delay and to increase the throughput of the network. It has been shown that delay is reduced by using group testing method. Trigger identification requires all testing groups to schedule the detection algorithm and after that performed group testing for isolating reactive jammers. Furthermore, investigation into more stealthy and energy efficient jamming models with simulations indicates robustness of the present proposed scheme.

Currently, there are no effective anti-jamming solutions to secure OFDM wireless communication under reactive jamming attack. On the other hand, MIMO has emerged as a technology of great research interest in recent years .These attacks are easy to launch but difficult to defend. They can block unwanted (in and outbound) traffic, allow it at certain time during the day, give priority to certain hosts, and enforce many other related policies. They will optimize the actual traffic as well, providing lower latency and higher throughput for the most critical application A Novel Based Defense Mechanism approach to detect and isolate the reactive jammers as well proactive manner.

III. RESEARCH METHODOLOGY

Transmitted packet after passing through the wireless channel or environment will get impaired or corrupted due various impairments over the path. This leads to poor bit error rate of the wireless system. Hence there is a need to correct this channel impairment using some. technique. To achieve this usually in wireless systems preamble is appended with the information packet to be transmitted. In figure below PS1 and PS2 are two preamble symbols and D1 to D_n are the symbols of the data packet to be transmitted. There are two steps for performing channel correction or channel equalization. First preamble based channel estimation and equalization is done and later pilot subcarriers embedded in the data symbols are used to perform phase rotation of all the data symbols.

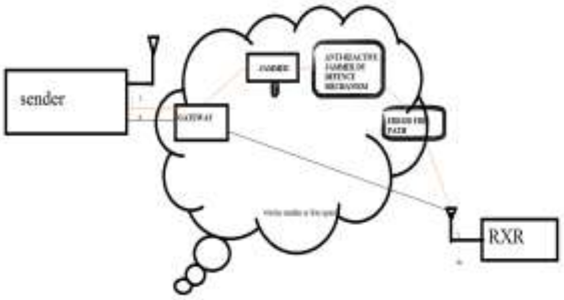

Figure 2 Block diagram for proposed system

A. *Steps involved in proposed system*

STEP1: Channel estimation is done in the time domain. First all the samples of received preamble are divided using reference preamble symbol 1(PS1). This gives channel response in time domain for the preamble symbol-1.
STEP2: De convolve entire packet with this channel response determined in STEP-1.
STEP3: Take FFT of the entire packet. Now determine phase rotation using the pilots embedded in the data symbols D1 to Dn. Take average of phase rotation values of all four pilots.
STEP4: Rotate the values of data symbol-1 using the average phase rotation.
STEP5: Similarly determine phase rotation using pilot carriers embedded in each of the data symbols one by one and de rotates accordingly. For countering the complicated collusion attacks, two different defense schemes were proposed: a scheme using temporal analysis, which explores the information over time (e.g., changing trend of the rating values), and a user correlation analysis, which aims attending patterns between the malicious users.

B. *Attacking zero forcing mechanism*

In order to understand the attack strategy, [11] inspect three special cases in with different received signal spaces. Undoubtedly, the most severe attack is depicted in Figure.8, in which *Jr* overlaps with *Sr* in the received signal space, preventing *Sr* from being recovered. On the contrary, the least powerful attack emits a jamming signal that is orthogonal to the legitimate signal as shown. In this case, the projected signal is equivalent to the original signal, yielding the highest projected signal amplitude. It shows the case between the above two extreme cases, when the angle of two received signals is a small value. Therefore, the key idea of attack strategy is to control the jamming signal direction in order to nullify ZF mechanism. Clearly, the jammer's attack strategy is to shrink the angle between the jamming signal and the intended signal by exploiting the jammer's spatial location. In fact, the difference between h*s* and h*j* deviates according to the distance between *S* and *J* [10]. More specifically, if the spacing between two antennas is narrower than a half wavelength, the channels from these two antennas will become highly correlated [9], which made two received signal directions similar.

Consequently, a smart jammer will simply attempt to approach the sender. In order to demonstrate the effectiveness of such attack strategy, we perform an experiment with varying distances between the jammer and sender's antennas. The *packet delivery rate* (PDR) performance is shown in Figure. 3, from which we can see that when the antenna distance is below 6*cm*, no packet can be successfully delivered.

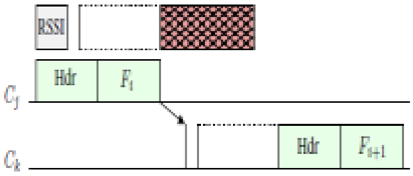

Figure 3. Jammer detects packet on channel *Cj* , but sender hops to *Ck* before jamming can begin, evading the attack.

C. *Proposed detecting algorithm for reactive jamming*

For detecting the reactive jammers, every sensor node periodically sends a control details message to the base station. There is a possibility that jammers may be activated during this period. Because of this event occurred on the network, the victim nodes will not send the control message to the base station based on this the base station can decide whether reactive jamming attack has occurred in the network or not by comparing the received report messages to a per stored threshold. When the status report message is generated by each sensor node, they can locally obtain their jamming status to determine the value of the label field. If the sensor node hears the jamming signals, it will not send the messages to base station, but will initialize the label as Victim.

A simple model was designed to incorporate MDDM in multiple-input single-output (MISO) and MIMO systems. This design was simulated and analyzed to demonstrate its performance. The system was implemented with binary phase shift keying (BPSK) in MATLAB and was tested in both an additive white Gaussian noise (AWGN) channel with no fading and a slow multipath fading channel with AWGN. The receiver design was based on the maximal ratio combining (MRC) technique with the assumption of perfect knowledge of channel state information (CSI) at the receiver end. The simulated performance results and theoretical analysis results were compared with the conventional single-input single output (SISO) system results. The performance metric of bit error probability versus (energy per bit to noise power spectral density ratio) was used. To establish a fair comparison, the transmitted power for the SISO, MISO and MIMO systems was maintained equal.

IV. PERFORMANCE ANALYSIS

In MIMO-OFDM system, 2-D channel estimation have been used where the time and frequency correlation of the training sub-carriers are used to estimate the channel. Weiner filter which implemented is an example of 2-D channel estimation, also called Minimum Mean Square Error (MMSE) estimators, has greatly increased computational complexity for the improved SNR performance.

To apply the decision algorithm the transmitter has to determine the following three metrics, *a)PDR (Packet Delivery Ratio):* Traditional approaches for the detection of jamming in wireless sensor networks use the packet delivery-ratio (PDR) and the received ambient signal strength as the main decision criteria. Jamming is detected as soon as the (averaged) PDR exceeds a predefined threshold.

PDR sender= Total number of ACK received ⁄ ACK send by the receiver (1)

PDR receiver=Packet passed CCR ⁄ Received packet (2)

b)RSSI (Received Signal Strength Indication): In wireless sensor networks, received signal strength indicator compares the signal level with the threshold value which is defined previously.

c) Noise: Detection of jamming signal will possible by calculating Signal-to-noise ratio on the network, this is applicable only to pro-active jammers.

SNR=Signal Power / Noise Power (3)

Table 1 Performance metrics

Parameters	**Specifications**
Carrier frequency(MHz)	5.8
Sample frequency (MHz)	40
Bandwidth(MHz)	40
FFT	128
Cyclic prefix ratio	2:1
Constellation	16-QAM
Data sub carriers	108/6

The flow chart results obtained show that as SNR increases, the data rate also increases for both conventional 2x2, 4x4, 8x8 MIMO and hybridized MIMO-OFDM antenna, but the hybridized MIMO-OFDM system has higher data rate than conventional MIMO. Similarly, BER values for the hybridized MIMO-OFDM are lower than the values obtained for the conventional MIMO indicating better performance in 4G than conventional MIMO. Also, as the number of antenna configuration increases, better performance is observed. This paper has shown that hybridization of MIMO-OFDM in 4G system reduces the errors which can hinder the quality of service in the faded environment.

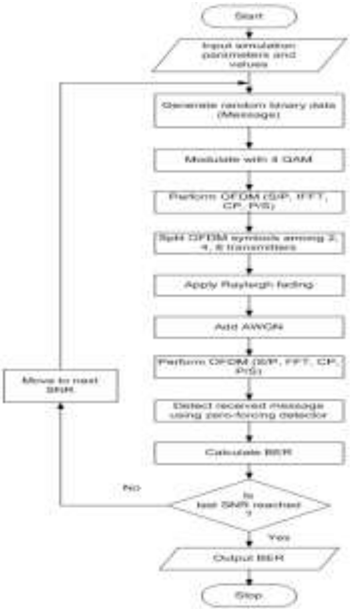
Start
Input simulation parameters and values
Generate random binary data (Message)
Modulate with 4 QAM
Perform OFDM (S/P, IFFT, CP, P/S)
Split OFDM symbols among 2, 4, 8 transmitters
Apply Rayleigh fading
Add AWGN
Perform OFDM (S/P, FFT, CP, P/S)
Detect received message using zero-forcing detector
Calculate BER
Is last SNR reached ?
NO
Yes
Move to next SNR
Output BER
Stop

Figure 4. Implementation flow diagram

V. RESULT AND DISCUSSION

The simulated bit error rate (BER) for the MIMO system is plotted in Figure 5 where L = 2 is the number of transmit antennas and J = 1 is the number of receive antennas. For comparison of performances, this figure also includes the theoretical probability of bit error for a baseband equivalent of the system. The simulated results follow the theoretical results very closely. The MIMO system with performs better than the system for lower (Eb/En0) values and the performance of the MIMO system is poorer than that of system for greater than 6.5 dB.

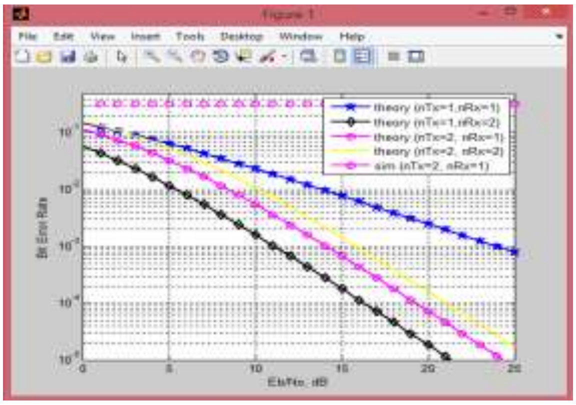

Figure 5. performance of BER VS SNR under jamming

The simulated and the numerically computed theoretical results of the MIMO system (with 2 transmit antennas and 3 receive antennas) over a frequency non selective slowly fading Rayleigh channel are shown in Figure 6. For comparison of the performances, this figure are also includes the theoretical and the simulated bit error probability for a OFDM system. This figure shows that for low (Eb/En0) values the theoretical results are more optimistic and for high (Eb/En0) values, the simulation results are more optimistic by using equation (1). This deviation of simulation results from the theoretical results calculated by using equation (2) may also be due to the reasons as discussed in previous sections.

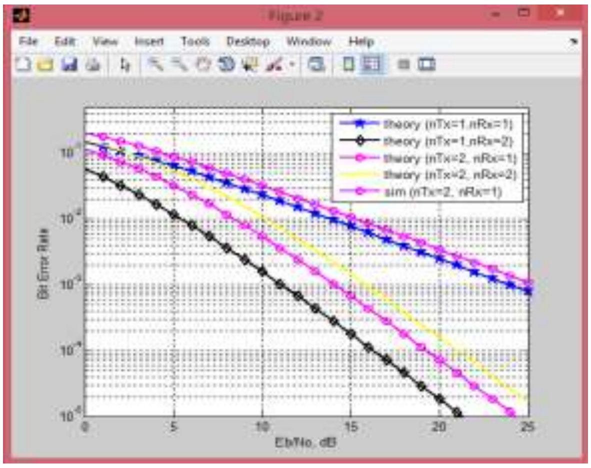

Figure 6. Performances of BER VS SNR under eliminated jammed communication

To perform experiments in 2 × 2 OFDM-MIMO networks, with one jamming antenna. Figure 7plots the PDR performance of one transmit antenna under different bandwidth settings. This figure are shows the jammer is very effective in degrading packet delivery performance in OFDM-MIMO networks, as none of the packets gets through using the traditional MIMO decoding method.

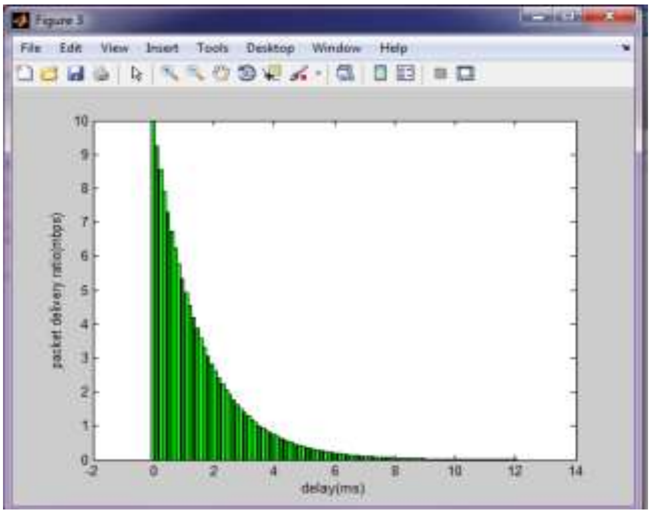

Figure 7. Delay vs Packet delivery Ratio

VI. CONCLUSION

In this extensive study on jamming and anti-jamming techniques in wireless networks, we have contributed by classifying and summarizing various approaches and discussing open research issues in the field. Different jammers attack wireless networks 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 medium 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. In this paper, a trigger identification service for reactive jamming attack in wireless sensor network is simulated to achieve minimum end-to-end delay and to increase the throughput of the network. It has been shown that delay is reduced by using group testing method. Trigger identification requires all testing groups to schedule the detection algorithm and after that performed group testing for isolating reactive jammers.

Furthermore, investigation into more stealthy and energy efficient jamming models with simulations indicates robustness of the present proposed scheme. Thus the challenging and, most importantly, improving currently existing solutions to cope with jamming.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” Computer Networks, vol. 38, no. 4, pp. 393–422, Oct 2002.

[2] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley Computer Publishing, pp. 326–331, Jan 2001.

[3] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, “Theory of spread spectrum communications—a tutorial,” IEEE Transactions on Communications, vol. 20, no. 5, pp. 855–884, Dec 1982.

[4] Chipcon AS, subsidiary of Texas Instruments, CC1000 and CC2420 Radio Transceiver Products, URL: www.chipcon.com.

[5] Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR -WPANs), IEEE 802.15.4-2003 Standard for Information Technology, Oct 2003.

[6] R. M. Kling, “Intel mote: an enhanced sensor network node,” in Int’l Workshop on Advanced Sensors, Structural Health Monitoring, and Smart Structures, July 2003.

[7] Wireless MAC and PHY Specifications for Wireless Personal Area Networks (WPANs), IEEE 802.15.1-2005 Standard for Information Technology, (Bluetooth), sep 2005.

[8] W. Xu, T. Wood, W. Trappe, and Y. Zhang, “Channel surfing and spatial retreats: defenses against wireless denial of service,” in Proc. of WiSe, pp. 80–89, Apr 2004.

[9] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” in Proc. of MobiHoc. ACM Press, pp. 46–5 , Oct 2005.

[10] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” IEEE Computer, vol. 35, no. 10, pp. 54–62, June 2002.

[11] H. Chan, A. Perrig, and D. Song, “Random key pre distribution schemes for sensor networks,” in IEEE Symposium on Research in Security and Privacy, pp. 197–213, Mar 2003.

[12] K. Sun, P. Nina, and C. Wang, “TinySeRSync: secure and resilient time synchronization in wireless sensor networks,” in Proc. of CCS, pp. 264–277, Apr 2006.

[13] H.-S. W. So, G. Nguyen, and J. Walrand, “Practical synchronization techniques for multi-channel MAC,” in Proc. Of MOBICOM, pp. 134–145, Nov 2006.