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. 3, Special Issue 22, April 2016

Utilizing Frequency Agility to Alleviate Active Jamming Attacks in Wireless Networks

Joseph Selva Kumar.A#1, Peter Francis.S#2
[1]Assistant Professor/Information Technology
Idhaya Engineering College for Women, Chinnasalem
[2]Assistant Professor/ Mathematics
Idhaya Engineering College for Women, Chinnasalem

ABSTRACT

Malicious conflict injection or jamming is one of the facile ways to disrupt wireless communications. Prior access can alleviate jamming conflict to a limited extent; they are especially vulnerable to a process jammer i.e., a jammer that injects noise upon sensing a legitimate relocation or wideband jamming. Clearly, via extensive experience, we detect that the jamming signal experiences differing levels of fading across the composite sub-carriers in its relocation bandwidth. Thus if the legitimate relocate were to somehow exploit the relatively unaffected sub-carriers to transmit message to the receiver, it could achieve reasonable throughputs, even in the presence of the reactive jammer. We design and implement JIMS, a Jamming conflict Mitigation Scheme that exploits the above characteristic by overcoming key working challenges. Via extensive test bed experiments and simulations we show that JIMS achieves a throughput restoration of up to 75 percent in the presence of a reactive jammer.

1 INTRODUCTION

Wireless communications can be freely disrupted by malicious injection of conflict, aka jamming. Given the commercial availability of jamming nodes today mounting Denial-of-Service (DoS) attacks using jamming is an easy work. How easy is it to combat jamming? Previous resolution have tried to mitigate jamming by tuning more physical layer knobs. Examples include adaptive power and rate control, or the use of lesser modulation rates in order to decrease the packet error rates (PER) in the presence of jamming conflict. Frequency hopping has also been considered in cases where there is significant additional available bandwidth for use. All of these prior studies conclude that in general, it is very difficult to overcome the crash of active jamming, particularly when jammers account for the inherent properties of MAC layer protocols. Our broad testbed measurements using legacy WiFi as well as programmable wireless boards support such an argument. Our performance however, also reveals a new, promising dimension for malicious conflict avoidance in OFDM (Orthogonal Frequency Division Multiplexing) settings. Clearly, we identify an advantage that can be exploited with OFDM to mitigate jamming; more importantly, this can be applied in conjunction with better previously proposed anti-jamming schemes.

Exploiting an intrinsic form of OFDM signal propagation: OFDM is at present a widely adopted relocation scheme in many various wireless network technologies. In traditional OFDM performance, the relocation power is uniformly distributed across a predefined set of sequence subcarriers; the number and width of these subcarriers code the available channel bandwidth. Due to physical obstructions and conflict, signal power (even that of a jammer) undergoes different levels of fading across the various subcarriers. As a result, on a few of the subcarriers the received jamming signal strength can be high, while on other subcarriers it is expected to be low1. Employing subcarrier-level radio agility. Our test bed measurements also prove that jamming signals are expected to experience varying levels of fading on different OFDM subcarriers. As a result, some subcarriers cannot be "significantly damaged" by the malicious capacity emission; such "cleaner" portions of the usable spectrum could be temporarily used for legitimate packet relocation, as long as a transceiver pair is made aware of which those subcarriers are.

2.SUB-CARRIER RADIO AGILITY AIDS ANTI-JAMMING

In this section, we characterize our test-bed experiments on assessing the behavior of malicious conflict from the perspective of OFDM sub-carrier level propagation. Our performance offer insights on how the jamming capacity is distributed across the subcarriers of the usable spectrum. These insights motivate and mode the foundation of our radio-agile anti-jamming framework design, which we discuss in Section 4. In a nutshell, our measurement-based, key findings are the following:

- The Received Jamming Signal to Noise Ratio (or RJSNR) experienced by legitimate users (transceivers), can often be quite low on a few OFDM subcarriers.
- Due to the asymmetry in the perceived RJSNR per subcarrier, a transceiver pair needs to exchange information regarding the subcarriers with respect to which the RJSNR is low, at one by one end (of the link).
- Due to variations in RJSNR over time, nodes need to periodically send change channel feedback. A low overhead feedback frequency of the order of once every 1,000ms suffices in relatively standard settings.

In what follows, we describe our threat method and experimental configuration; subsequently we present our observations. The threat method, we consider a jammer (Eve) that transmits OFDM signals with the same transmission capacity budget as legitimate users, thereby imitating a typical legitimate device to avoid detection. Other than this, we do not require any other constraint on the jammer.

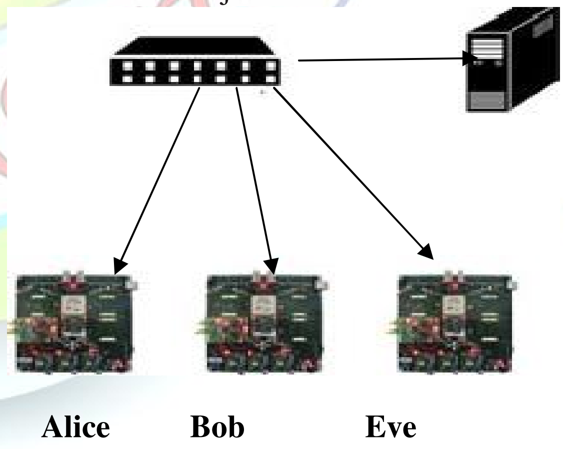

Fig. 1. Alice, Bob, and Eve are over all placed on a straight line.

We perform our experiments late at night in a campus building, and we verify that this channel is not used by some collocated WLAN networks. Christo Ananth et al. [3] discussed about a system,the effective incentive scheme is proposed to stimulate the forwarding cooperation of nodes in VANETs. In a coalitional game model, every relevant node cooperates in forwarding messages as required by the routing protocol. This scheme is extended with constrained storage space. A lightweight approach is also proposed to stimulate the cooperation. The OFDM implementation that we use (WARPLabv6) guide BPSK, QPSK and 16 QAM modulation rates, and a 40MHz sampling rate. Legitimate packets carrying

CSI information have a length of 240 bytes, while information packets have a length of 1,500 bytes; each experiment lasts for 5 minutes and is repeated 20 times.

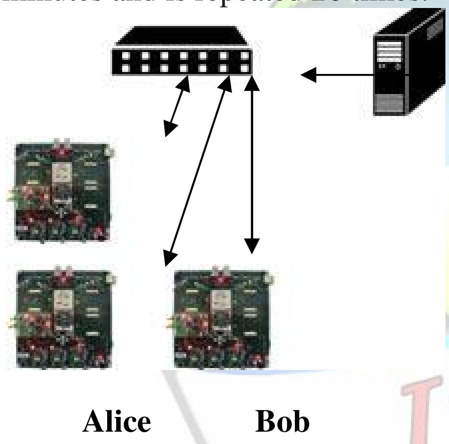

Fig. 2. Eve is placed at 90 degrees to Alice and Bob.

3. OUR SUBCARRIER-LEVEL RADIO-AGILE DESIGN

In this section, we describe the design of our jamming conflict mitigation scheme, which is based on the key observations made in Section 3. The scheme consists of three major steps. First, the legitimate pair of transceivers independently determine the OFDM subcarriers that are relatively unaffected by the jamming signal. Second, by means of using Raptor codes, they exchange the information they have determined (CSI) in the first step. Third, each transceiver uses this information, to transmit symbols on only an appropriately chosen set of subcarriers (that are relatively unaffected at the receiver). To maximize the likelihood of correct reception, and facilitate higher transmission rates on the relatively unaffected subcarriers, we further consider an extended version of JIMS, which involves pooling power from the subcarriers that remain unused (to the extent allowed by regulations) to those subcarriers on which, symbols are actively transmitted. We call this extended version of JIMS as JIMS-PA (for Power Allocation).

3.1 Determining the Subcarriers Affected by the Jamming Signal

We consider two ways for detecting the subcarriers that are affected by the jammer. For ease of discussion, let us assume that Alice is executing this step. She simply measures the signal from the jammer when there are no other transmissions in the vicinity. Towards this, we first assume that somehow Alice knows that a jammer is in operation using one of the techniques proposed in . Next, we assume that Alice can simply listen and detect the jamming signal. If the jammer emits energy continuously or without regards to whether or not Alice and Bob are transmitting, this can be done easily. If the jammer is reactive i.e., only transmits upon sensing a transmission from Alice, Alice can send a short pilot to trigger the jammer and subsequently go silent (assuming half-duplex mode of operations as is common with legacy systems); the jamming signal that spills beyond Alice's prompt can then be captured to determine the jammer's profile. The signal can be then decomposed to determine the SNR on each of the subcarriers in the operational band. In other words, the subcarrier level RJSNR can be determined. We call this approach the explicit approach of determining the affected subcarriers. Second, let us assume again that using an appropriate technique from those reported in, the presence of the jammer is detected. Bob then sends a pilot signal to Alice. Alice then determines the SINR on each of the subcarriers in that pilot signal. In a nutshell, if either the signal quality is low and/or the jamming signal is high, on a specific subcarrier, that subcarrier is deemed unfit for communication. Other subcarriers where neither of the above scenarios holds true are appropriate for transmission. We call this approach the implicit approach of determining the affected subcarriers.

3.2 Subcarrier Selection

Using either the explicit or implicit approach, Alice is able to determine the quality of communications on each of her subcarriers. Now, she has to determine the appropriate set of subcarriers for use by Bob, for him to communicate with her. The process of selecting this set is different with the explicit and implicit approaches described above. With the explicit approach, the good subcarriers (to be used for communication by Bob) are chosen based on simple RJSNR threshold. Clearly, if the RJSNR is lower than a certain threshold on a subcarrier it is deemed a good subcarrier. A simple way to choose the RJSNR threshold is to determine average RJSNR from that observed on all subcarriers, and use those that have RJSNRs lower than the average.

Choice of the right threshold, One of the challenges that arises with both the explicit and the implicit schemes is “How do we choose the right threshold (be it RJSNR or SINR depending on whether the explicit or implicit approach is used)?” For simplicity, let us just consider the implicit approach; instead of choosing _ as above, let us assume that we choose a different static threshold _0. If we are liberal, and choose _0 to be low, we include a large set of subcarriers; however, the SINRs on some of these subcarriers will be unacceptably low. If instead, we are conservative and choose a high value for _0, we may end up excluding a large number of subcarriers (on a few of which, communications may in fact be possible), and thus, end up achieving a lower throughput than what is possible. We find via experiments that choosing the average value (as discussed above) to be the threshold, provides a good compromise between the two extreme cases, in most scenarios. We evaluate this choice, by comparing the performance with other cases where a static threshold.

3.3 Exchanging CSI

At this point, both Alice and Bob have determined the set of subcarriers on which, they expect to be able to receive symbols from each other, in the presence of the active jammer. Unfortunately, the subcarriers on which Alice can receive information (known only to Alice at this stage) may be various from those on which Bob can receive information (known only to Bob at this stage). Thus, we need a way for Alice to let Bob know “which subcarriers to use” for communicating with her (Bob needs to do likewise). A low throughput channel using Raptor codes to exchange CSI. Towards, this we leverage Raptor codes to communicate this information (which as previously mentioned is called the CSI). Raptor codes belong to the class of fountain codes with even encoding and decoding times. Fountain codes are rate-less fault-tolerant codes that can enable reliable communications on deletion channels; examples of fountain codes include Raptor codes and LT-codes. Encoded symbols are developing by the encoder on-the-fly. The decoder recovers the source block by collecting a sufficiently huge set of encoding symbols. Hence, Raptor codes facilitate communications in the presence of the jammer (jammed symbols could be considered to be erasures), by utilizing a very low throughput channel (as shown by our experiments later in this paper). Thus, in JIMS we only utilize these for the exchange of CSI information, and later simply utilize the relatively unaffected carriers without applying Raptor codes. Clearly, Alice uses a bit vector to indicate the subcarriers to be used by Bob, and encodes this using Raptor code. She transmits the encoded bit vector repeatedly (each time, the vector is encoded differently), until Bob is able to retrieve the source block (the bit vector).

3.4 JIMS with Power Allocation (JIMS-PA)

Thus far, JIMS simply identified those subcarriers that were relatively unaffected by the jamming signal from Eve, and used those subcarriers for the exchange of information between Alice and Bob (in Eve's presence). Since, the information on the other subcarriers, i.e., those that are heavily affected by Eve are relatively unusable, "Can we reallocate some of the power from such subcarriers, to the subcarriers that are being used in order to enhance the throughput?" The comment to this query is that, such a reallocation is possible to some extent. However, one cannot simply reallocate all the power onto the "good" subcarriers for two reasons. First, because of the spectral flatness regulations specified in the 802.11 standard (clearly 802.11n), the difference in the powers allocated to two subcarriers cannot exceed 2 dB. Second, if we blindly assign high powers to the good subcarriers, Eve will notice the anomaly, and can target those subcarriers. Thus, we can only reallocate powers to some extent, and we seek to do so here while adhering to the first constraint.

CONCLUSIONS

In this paper, we seek to mitigate the crash of an active jammer (e.g., a reactive or wideband jammer). To do so, we exploit the inherent features of OFDM. Clearly, we perform experiments that show that the jamming signal has different fading levels with respect to different OFDM subcarriers. We propose a jamming conflict mitigation scheme, using which, transceivers can identify subcarriers that are relatively unaffected by jamming and utilize them for communications. We show that JIMS restores throughput up to 75 percent, in the presence of an active jammer via experiments on our WARP test bed. At this time, we rely on prior schemes to detect the jammer, and utilize JIMS only when a jammer is detected. Integrating JIMS with such detection schemes effectively will be considered in future work.

REFERENCES

[1] PKI 6650 Wideband Jammer. (2015) [Online]: http:// bit.ly/10us5My

[2] Neco Defense Systems. (2012). [Online]: http://www.necodefence.com/rfj.php

[3] Christo Ananth, M.Muthamil Jothi, A.Nancy, V.Manjula, R.Muthu Veni, S.Kavya, "Efficient message forwarding in MANETs", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1,Issue 1, August 2015,pp:6-9

[4] G. Noubir, R. Rajaraman, B. Sheng, and B. Thapa, “On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming,” in Proc. ACM 4th Conf. Wireless Netw. Security, 2011, pp. 97–108.

[5] K. Pelechrinis, I. Broustis, S. V. Krishnamurthy, and C. Gkantsidis, “ARES: An anti-jamming reinforcement system for 802.11 networks,” in Proc. ACM 5th Int. Conf. Emerging Netw. Exp. Technol., 2009, pp. 181–192.

[6] C. Orakcal and D. Starobinski, “Rate adaptation in unlicensed bands under smart jamming attacks,” in Proc. 7th Int. ICST Conf. Cognitive Radio Oriented Wireless Netw. Commun., 2012, pp. 1–6.

[7] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, “Using channel hopping to increase 802.11 resilience to jamming attacks,” in Proc. IEEE Int. Conf. Comput. Commun., 2007, pp. 2526–2530.

[8] K. Pelechrinis, C. Koufogiannakis, and S. V. Krishnamurthy, “On the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks,” IEEE Trans. Wireless Commun., vol. 9, no. 10, pp. 3258–3271, Oct. 2010.