International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-782-787 ISSN: 2249-6645

Enhanced Anti-Jamming Protocol in Wireless Mesh Networks

R. Senthil kumar[1], Mahalakshmi. V. J.[2]
[1]PG Scholar, [2]Assistant Professor
SNS College of Technology, Coimbatore.

***Abstract*- Nowadays jamming causes the major data loss in mobile communications. During the transmission time Anti-jamming technique can be used to transmit intermittently at low power in order to conserve energy. Here we use 802.11wireless network technology and this is to access the functions of the physical layer. There are two functions called Rate Adaptation and Power Control are used to find out whether the attackers involve over the transmission. Attackers involve and send the unwanted messages from source to the destination and use more power. During the transmission time the original messages were not sent properly and occupy more power. First, the Rate Adaptation Algorithm controls the data rate during transmission and increases the packet delivery ratio. Second, Power Control technique is used to find out who is using unwanted powers. Attackers are motivated to use a random jammer to make the jammers to sleep intermittently and increase its lifetime and decrease the probability of detection. The two types of jammers are Deceptive-random jammer and Reactive jammer model. So we primarily consider the Deceptive-random jammer model. Moreover, Reactive jammers are not easily available since they are harder to implement and require special expertise on the part of the attacker.**

Keywords: IEEE 802.11, jamming, power control, rate control.

I. INTRODUCTION

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 traveling. 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. New applications place high demands on the quality, reliability, and security of transmissions. In order to provide a ubiquitous and powerful communication infrastructure that can satisfy security and reliability demands, sophisticated network technology, protocols and algorithms are required. Due to their open and ubiquitous nature, wireless information systems are extremely vulnerable to attack and misuse. Wireless systems can be attacked in various ways, depending on the objectives and capabilities of an adversary.

Due to high availability and relatively low cost of powerful antennas, *jamming*, i.e., the use of active signals to prevent data distribution has emerged as an attractive way of attack. As the current data communication standards such as IEEE802.11 [1] and Bluetooth [2] are not designed to resist malicious interference, a small number of jammers with limited energy resources can disrupt operation of an entire network. Jamming is a common method of attack in military networks, where transmissions are often performed in the presence of an adversary whose goal is to disrupt the communication to a maximum degree. For example, the Global Positioning System (GPS) relies on extremely weak signals from orbiting satellites and, as a result, is very vulnerable to jamming. This constitutes a significant threat for GPS-based weapon and navigational systems. Jamming can be viewed as a form of *Denial-of-Service* (DoS) attack, whose goal is to prevent users from receiving timely and adequate information.

This makes the defense against such attacks very critical. A jammer transmits electromagnetic energy to hinder legitimate communications on the wireless medium. A jamming attack can cause the following effects in an 802.11 network: 1) due to carrier sensing, co-channel transmitters defer their packet transmissions for prolonged periods; and 2) the jamming signal collides with legitimate packets at receivers. Frequency-hopping techniques have been previously proposed for avoiding jammers [5], [6]. Such schemes, however, are not effective in scenarios with wideband jammers [7], [8]. Furthermore, given that 802.11 operates on relatively few frequency channels, multiple jamming devices operating on different channels can significantly hurt performance in spite of using frequency hopping [9]. ARES1 (Anti-jamming Reinforcement System), a novel measurement driven system, which detects the presence of jammers and invokes rate adaptation and power control strategies to alleviate jamming effects.

II. JAMMING ATTACKS

The goal of the jammer is to disrupt the normal operation of the broadcast system, which results in high waiting time and excessive power consumption of the clients. To that end, the jammer sends active signals over the channels that interfere with the signal sent by the server (see Fig. 1). 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.

While spread-spectrum techniques constitute an important tool for combating jamming, an additional protection is required at packet-level. First, the pseudo-random noise code or frequency hopping sequence may be

known to the adversary, as in the case of the standard wireless protocols such as IEEE802.11 and Bluetooth. Second, even if no information about the spread-spectrum protocol is available to the adversary, it can still destroy a small number of bits in each transmitted packet by sending a strong jamming signal of short duration. If no other protection mechanism is used at the packet-level, as in the case of IEEE802.11 and Bluetooth, the few destroyed bits will result in dropping of the entire packet.

Accordingly, there is a need to provide an additional packet-level protection, which has to be built on top of traditional anti-jamming techniques. Accordingly, in this paper we investigate efficient anti-jamming schedules for data broadcast. 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.

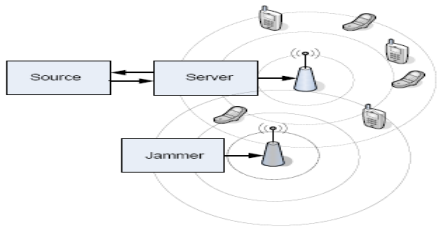

Figure.1 Jamming Attacks

A. Types of Jamming Attacks

Jammers can be distinguished in terms of their attack strategy. A detailed discussion can be found in

1) *Nonstop Jamming:* Constant jammers continuously emit electromagnetic energy on a channel. Nowadays, constant jammers are commercially available and easy to obtain [1], [7]. While constant jammers emit non decipherable messages, *deceptive* jammers transmit seemingly legitimate back-to-back dummy data packets. Hence, they can mislead other nodes and monitoring systems into believing that legitimate traffic is being sent.
2) *Intermittent Jamming:* As the name suggests, these jammers are active intermittently; the primary goal is to conserve battery life. A *random* jammer typically alternates between uniformly distributed jamming and sleeping periods. It jams for Tj s, and then it sleeps for Ts s. A *reactive* jammer starts emitting energy only if it detects traffic on the medium. This makes the jammer difficult to detect. However, implementing reactive jammers can be a challenge.

For the purposes of this paper, we primarily consider the deceptive-random jammer model. Attackers are motivated into using a random jammer because putting the jammer to sleep intermittently can increase its lifetime and decrease the probability of detection [14]. Furthermore, it is the most generalized representation of a jammer. Appropriately choosing the sleep times could turn the jammer into a constant jammer or (with high probability) a reactive jammer. Moreover, reactive jammers are not easily available since they are harder to implement and require special expertise on the part of the attacker.

III. RELATED WORKS

Most previous studies employ frequency hopping to avoid jammers. Frequency hopping, however, cannot alleviate the influence of a wideband jammer [7], [8], which can effectively jam all the available channels. In addition, recent studies have shown that a few cleverly coordinated, narrowband jammers can practically block the whole spectrum [9]. Thus, ARES does not rely on frequency hopping.

A. Studies Based on Frequency Hopping

1) Navda *et al.* [5] implement a proactive frequency-hopping protocol with pseudorandom channel switching. They compute the optimal frequency-hopping parameters, assuming that the jammer is aware of the procedure followed.
2) Xu *et al.* [6] propose two anti-jamming techniques: reactive channel surfing and spatial retreats. However, their work is on sensor networks that only support very low data rates and transmission powers.
3) Gummadi *et al.* [15] find that 802.11 devices are vulnerable to specific patterns of narrowband interference related to time recovery, dynamic range selection, and PLCP-header processing. They show that due to these limitations, an intelligent jammer with a 1000 weaker signal (than that of the legitimate transceiver) can still corrupt the reception of packets. In order to alleviate these effects, they propose a rapid frequency-hopping strategy.

B. Other Relevant Work:

1) Xu *et al.* [14] develop efficient mechanisms for jammer detection at the PHY layer (for all the four types of jammers). However, they do not propose any jamming mitigation mechanisms. In the same authors suggest that competition strategies, where transceivers adjust their transmission powers and/or error correction codes, *might* alleviate jamming effects. However, they neither propose an anti-jamming protocol nor perform evaluations to validate their suggestions.
2) Lin and Noubir present an analytical evaluation of the use of cryptographic interleavers with different coding schemes to improve the robustness of wireless LANs. In the authors show that in the absence of error-correction codes (as with 802.11) the jammer can conserve battery power by destroying only a portion of a legitimate packet.
3) Noubir also proposes the use of a combination of directional antennas and node mobility in order to alleviate jammers. ARES can easily be used in conjunction with directional antennas or with error correction codes. We would like to refer the interested reader to our literature survey on anti-jamming systems in for more details.

C. Prior Work on Rate and Power Control:

Rate and power control techniques have been proposed in the literature as means of mitigating interference. However, they do not account for a hostile jamming environment. With these schemes, nodes cooperate in order to mitigate the impact of "legitimate" interference, thereby improving the performance. As an example, Zhai and Fang [23] consider the optimal carrier sensing range for maximum spatial reuse in MANETs. All nodes are restricted to the same maximum transmission power, and their work is purely based on analysis and simulations. In this paper, we follow a purely experimental approach, and our results indicate that ARES effectively alleviates the impact of jammers that use higher transmission powers. Our scheme is specialized toward handling malicious interference of jammers, which attempt to disrupt ongoing communications.

IV. EXPERIMENTAL SETUP

A. Test-Bed Description

Our wireless test-bed consists of 37 Soekris net4826 nodes, which mount a Debian Linux distribution with kernel v2.6, over NFS. The node layout is depicted in Fig. 2. Thirty of these nodes are each equipped with two miniPCI 802.11a/g WiFi cards, an *EMP-8602 6 G* with Others chipset, and an *Intel-2915*. The other seven nodes are equipped with one *EMP-8602 6G*and one *RT2860* card that supports MIMO-based (802.11n) communications. We use the MadWifi driver for the *EMP-8602 6 G* cards. We have modified the Linux client driver of the *RT2860* to enable Space Time Block Coding (STBC) support. We use a proprietary version of the *ipw2200* access point (AP) and client driver/firmware of the *Intel-2915* card. With this version, we are able to tune the CCA threshold parameter.

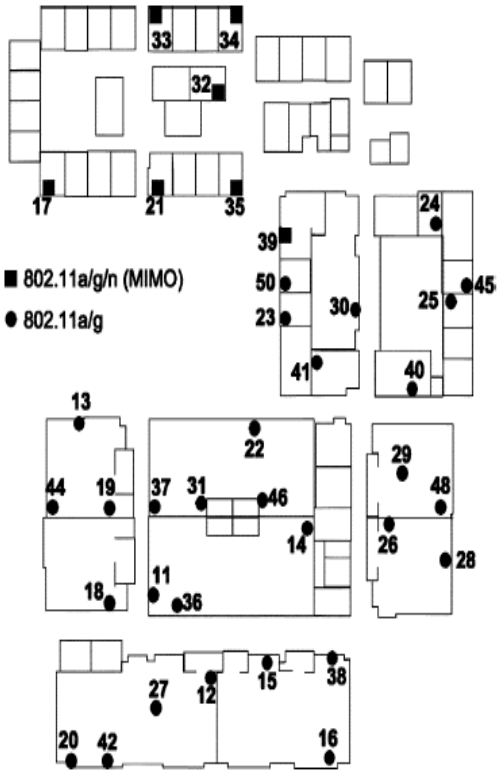

Fig.2. Deployment of our wireless test-bed.

B. *Experimental Settings and Methodology*

We experiment with different rate adaptation algorithms in the presence of random jammers. We also perform experiments with various transmission powers of jammers and powers/CCA thresholds of legitimate nodes. Our measurements encompass an exhaustive set of wireless links, routes of different lengths, as well as static and mobile jammers. We examine both single-input–single-output (SISO) and MIMO links. We experiment with three modes of operation: 802.11a/g/n (unless otherwise stated throughout this paper, our observations are consistent for all three modes of operation). The experiments are performed late at night in order to isolate the impact of the jammers by avoiding interference from collocated WLANs. By default, all devices (legitimate nodes and jammers) set their transmission powers to 18 dBm (for our experiments that involve only the Intel-2915 cards, the maximum power that we can use is 20 dBm).

1) Implementing a Random Jammer: Our implementation of a random jammer is based on a specific configuration dBm and a user space utility that sends broadcast packets as fast as possible. For the purposes of research, we have implemented our own random jammer on an 802.11 legacy device by setting the CCA threshold to 0 dBm. By setting the CCA threshold to such a high value, we force the device to ignore all legitimate 802.11 signals even after carrier sensing. Packets arrive at the jammer's circuitry with powers less than 0 dBm (even if the distances between the jammer and the legitimate transceivers are very small). An effective random jammer should be able to transmit packets on the medium, as fast as possible, during random *active* time intervals.

2) Traffic Characteristics: We utilize the *iperf* measurement tool to generate UDP data traffic among legitimate nodes; the packet size is 1500 B. The duration of each experiment is 1 h. For each experiment, we first enable *iperf* traffic between legitimate nodes, and subsequently, we activate the jammer(s). We consider both mesh and WLAN connectivity. We experiment with different jammer distributions, namely: 1) *frequent jammers*, which are active almost all of the time; 2) *rare jammers*, which spend most of their time sleeping; and 3) *balanced jammers* that have similar average jamming and sleeping times. We have disabled RTS/CTS message exchange throughout our experiments.

V.ARES DESIGN

ARES is composed of two main modules: 1) a Rate module that chooses between fixed or adaptive-rate assignment; and 2) a Power Control module that facilitates appropriate CCA tuning on legitimate nodes.

1.Rate Control

Rate adaptation algorithms are utilized to select an appropriate transmission rate as per the current channel conditions. As interference levels increase, lower data rates are dynamically chosen. Since legitimate nodes consider jammers as interferers, rate adaptation will reduce the transmission rate on legitimate links while jammers are active. Hence, one could potentially argue that rate control on legitimate links increases reliability by reducing rate and can thus provide throughput benefits in jamming environments. To examine the validity of this argument, we experiment with three different popular rate adaptation algorithms, Sample Rate, AMRR and One . These algorithms are already

implemented on the MadWifi driver that we use. For simplicity, we first consider a balanced random jammer, which selects the sleep duration from a uniform distribution U [1,8]and the jamming duration from U[1,5](in seconds).

1) *Fixed transmission rate (***Rf***):* This is the nominal transmission rate configured on the wireless card.

2) *Saturated rate (***Rs***):* It is the rate achieved when **R**f is chosen to be the rate on the wireless card. In order to compute **Rs** for a given **Rf ,** we consider links where the PDR 100% for the particular setting of **Rf** .We then measure the rate achieved in practice. We notice that for lower value of **Rf** , the specified rate is actually achieved on such links

TABLE 1
Saturated throughput matrix in megabits per second

Rf	6	9	12	18	24	36	48	54
Rs	6	9	12	18	24	26	27	27

.

However, for higher values of **Rf (**as an example**, Rf =54 M**b/s), the achieved data rate is much lower; this has been observed in other work, Table I contains a mapping, derived from measurements on our test-bed,between **Rf** and **Rs**.

*Application data rate (***Ra***):* This is the rate at which the application generates data. It is difficult (if not impossible) to *a priori* determine the *best* fixed rate on a link. Given this, and if we let R be the set of all possible fixed transmission rates, we set

Rf={min x:x>Ra}

which is the maximum rate that is required by the application (we discuss the implications of this choice later). Our key observations are summarized as follows.

• Rate adaptation algorithms perform poorly on high-quality links due to the long times that they incur for converging to the appropriate high rate.

• On *lossless* links, the fixed rate **Rf** is better, while rate adaptation is beneficial on *lossy* links.

We defer defining what constitute lossless or lossy links later in this section. Conceptually, we consider lossless links to be those links that can achieve higher long-term throughput using a fixed transmission rate **Rf** rather than by applying rate adaptation.

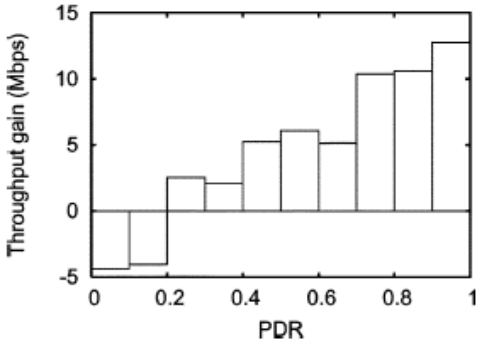

Fig.3 Throughput gain of fixed rate versus Sample Rate, for various link qualities and for application data rate of 54 Mb/s.

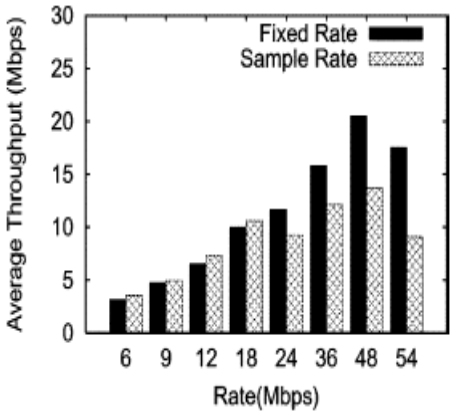

Fig.4 Performance with rare jammers is aligned with our observations for the case with balanced jammers **Ra= Rf.**

2. Power Control

Power control in 802.11 networks needs to ensure that there are no asymmetric links in the network to avoid throughput starvation of any node. To this end, two fundamental concepts are those of a contention domain and symmetry.

According to the CSMA/CA protocol of the 802.11 MAC, a node that wishes to transmit a packet needs to first measure the strength of the power received on the wireless channel, i.e. the sum of the noise and interference on its operating channel. If the received power on the channel is higher than a certain threshold referred to as the Clear Channel Assessment (CCA) threshold of node , the medium is assessed to be busy, and the transmission is deferred. Otherwise, the node transmits its packet. In this framework, we define the contention domain of a reference node as the set of nodes in the network that can generate sufficient interference to suppress the transmission of the reference node.

Power Jammers

we consider a single legitimate data link and a jammer, incrementing the transmission power on the data link should increase the signal-to-interference- plus-noise ratio (SINR) of the received data packets. Thus, one could argue that increasing the transmission power is always beneficial in jamming environments. Note here that increasing the transmission power in environments with lower power jammers can potentially increase the network-wide interference. However, as we will see in the following, ARES includes a CCA tuning mechanism that avoids starvation effects caused from legitimate interference. We vary the transmission powers of both the jammer and legitimate transceiver, as well as the CCA threshold of the latter. Note that the jammer's transmission distribution is not very relevant in this part of our study. Our expectation is that tuning the power of legitimate transceivers will provide benefits while the jammer is active. In other words, one can expect that the benefits from power control will be similar with any type of jammer.

We define the following:

- **RSSITR:** the received signal strength indicator (RSSI) of the signal of the legitimate transmitter at its receiver.
- **RSSIRT :** the RSSI of the signal in the reverse direction (the receiver is now the transmitter).
- **RSSIJT** and **RSSIJR :** the RSSI values of the jamming signal at the legitimate transmitter and receiver, respectively.
- **RSSIJ:** the minimum of{ RSSIJT , RSSIJR }
- **PL** and **CCAL:** the transmission power and the CCA threshold at legitimate transceivers.
- **PJ:** the transmission power of the jammer. Our main observations are the following.
- Mitigating jamming effects by incrementing is viable at lowdata rates. It is extremely difficult to overcome the jamming interference at high rates simply with power adaptation.
- Increasing CCAL restores (in most cases) the isolated throughput (the throughput achieved in the absence of jammers)

CCA=min(RSSITR,RSSIRT) - △

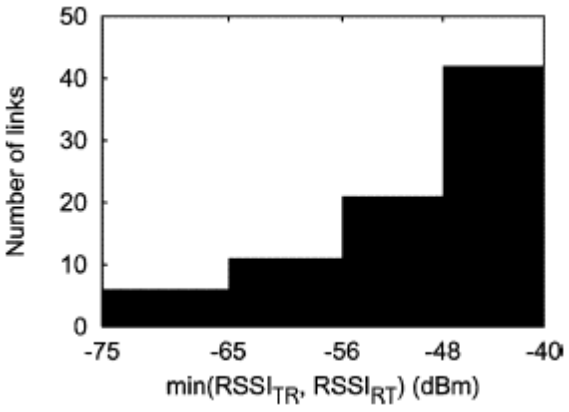

Fig. 5 Histogram with **RSSITR** and **RSSIRT** values on legitimate links.

VI. PARAMETERS AND SIMULATION RESULTS

We first evaluate ARES by examining its performance in three different networks: a MIMO-based WLAN, an 802.11 mesh network in the presence of mobile jammers, and an 802.11Awlan setting where uplink TCP traffic is considered. ARES boosts the throughput of our MIMO WLAN under jamming by as much as 100%. Our objective here is twofold. First, we seek to observe and understand the behavior of MIMO networks in the presence of jamming. Second, we wish to measure the effectiveness of ARES in such settings. Toward this, we deploy a set of seven nodes equipped with *Ralink RT2860* mini PCI cards.

TABLE 2
Simulation parameters for frequency hopping technique

Number of nodes	15
Packet size	512bytes
Terrain area	2000x1000
Number of nodes packet transmission	5

In existing method we have used the frequency hopping technique for the packet tranmission for the different source to destination. Packet losses is very low in one source to one destination packet transmission time. Packet losses will be increasin for the number of source and destination increasing time.

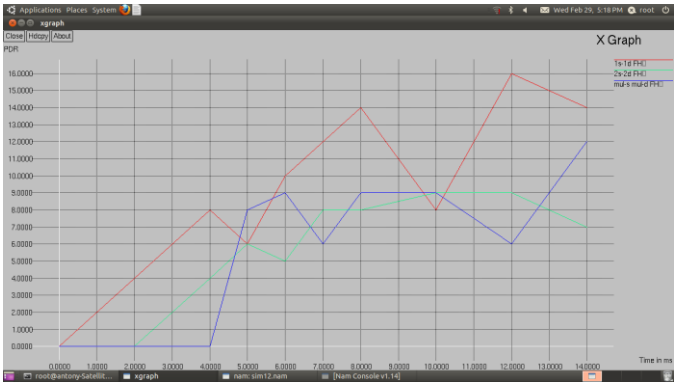

Fig. 6 Increasing the packet loss using FH method used.

TABLE 3
Simulation parameters for ARES method

Number of nodes	45
Packet size	512bytes
Terrain area	2000x1000
Number of nodes packet transmission	15

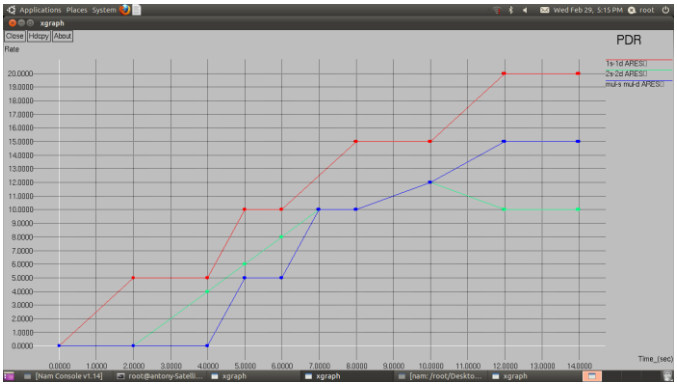

Fig.7 Reduced the packet loss when using the ARES method.

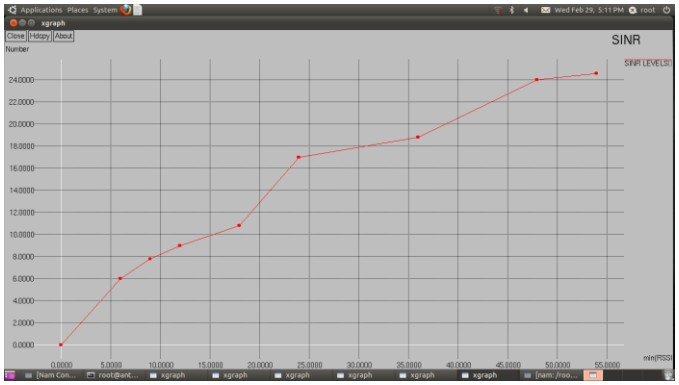

Fig.8 SINR graph for using ARES method

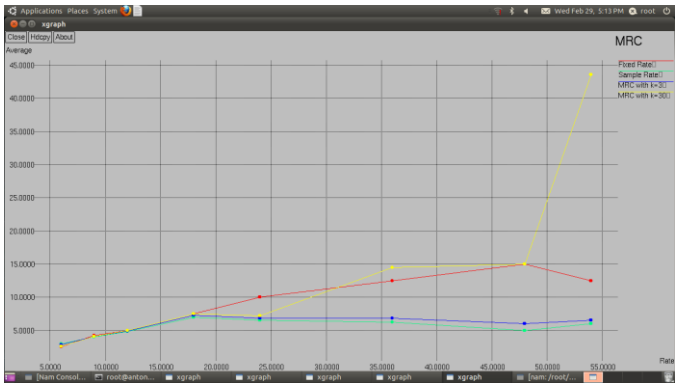

Fig.9 MRC graph for usig ARES method

VII. CONCLUSION

In this paper the Evaluation and measurement driven prototype system that uses the Rate control and Power control technique which efficiently fights against the jammers. The jammers can be avoided using Frequency hopping technique. The fixed Rate assignment can be beneficial in jammed environment. Power level tuning helps only at low rates and low power jammer. Tuning the CCA threshold enables: (i) The transmitter to ignore jamming signals. (ii) The receivers capture desired packets. In our future work is to prevent the packet losses and increasing the throughput using ARES method. We will demonstrate the effectiveness of ARES in three different deployments are: (i) an 802.11n-based MIMO in WLAN; (ii) an 802.11a/g network infested with mobile jammers; (iii) an 802.11a WLAN with uplink TCP traffic. We also introduce a network security model to prevent the jammer attacks.

REFERENCES

[1] "SESP jammers," SESP [Online]. Available: http://www.sesp.com/

[2] "Wireless noise hampers DefCon; Impact of non-Wi-Fi interference surprises observers at hacker conference," *BNET.com* 2005[Online].Available: http://findarticles.com/p/articles/mi_m0EIN/ is_2005_August_2/ai_n14841565

[3] "Techworld news," [Online]. Available: http://www.techworld.com/mobility/news/index.cfm?newsid=10941

[4] "RF jamming attack," ZOHO Corporation, Pleasanton, CA, 2010 [Online]. Available: http://manageengine.adventnet.com/products/wifi manager/rfjamming-attack.html

[5] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to Jamming attacks," in *Proc. IEEE INFOCOM*, 2007, pp. 2526–2530.

[6] W. Hu, T.Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *Proc. ACM WiSe*, 2004, pp. 80–89.

[7] "ISM wide-band jammers," [Online]. Available: http://69.6.206.229/ecommerce- solutions-catalog1.0.4.html

[8] D. Caro, "[ISN] Users fear wireless networks for control," 2007 [Online]. Available: http://lists.jammed.com/ISN/2007/05/0122.html

[9] K. Pelechrinis, C. Koufogiannakis, and S. V. Krishnamurthy, "Gaming the jammer: Is frequency hopping effective?," in *Proc. WiOpt*, Jun. 2009, pp. 187 196.

[10] V. Mhatre, K. Papagiannaki, and F. Baccelli, "Interference mitigation through power control in high density 802.11 WLANs," in *Proc. IEEE INFOCOM*, 2007, pp. 535–543.

[11] J. Bicket, "Bit-rate selection in wireless networks," M.S. thesis, Dept. Elect. Eng. Comput. Sci., MIT, Cambridge, MA, 2005.

[12] "Onoe rate control," [Online]. Available: http://madwifi.org/browser/ trunk/ath_rate/onoe

[13] S. Pal, S. R. Kundu, K. Basu, and S. K. Das, "IEEE 802.11 rate control algorithms: Experimentation and performance evaluation in infrastructure mode," in *Proc. PAM*, 2006.

[14] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting Jamming attacks in wireless networks," in *Proc. ACM MobiHoc*, 2005, pp. 46–57.

[15] R. Gummadi, D. Wetheral, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of RF interference on 802.11 networks," in *Proc. ACM SIGCOMM*, 2007, pp. 385–396.