Protocol-Aware Radio Frequency Jamming in Wi-Fi and Commercial Wireless Networks

Abid Hussain, Nazar A. Saqib, Usman Qamar, Muhammad Zia, and Hassan Mahmood

Abstract: **Radio frequency (RF) jamming is a denial of service attack targeted at wireless networks. In resource-hungry scenarios with constant traffic demand, jamming can create connectivity problems and seriously affect communication. Therefore, the vulnerabilities of wireless networks must be studied. In this study, we investigate a particular type of RF jamming that exploits the semantics of physical (PHY) and medium access control (MAC) layer protocols. This can be extended to any wireless communication network whose protocol characteristics and operating frequencies are known to the attacker. We propose two efficient jamming techniques: A low-data-rate random jamming and a shot-noise based protocol-aware RF jamming. Both techniques use shot-noise pulses to disrupt ongoing transmission ensuring they are energy efficient, and they significantly reduce the detection probability of the jammer. Further, we derived the tight upper bound on the duration and the number of shot-noise pulses for Wi-Fi, GSM, and WiMax networks. The proposed model takes consider the channel access mechanism employed at the MAC layer, data transmission rate, PHY/MAC layer modulation and channel coding schemes. Moreover, we analyze the effect of different packet sizes on the proposed jamming methodologies. The proposed jamming attack models have been experimentally evaluated for 802.11b networks on an actual testbed environment by transmitting data packets of varying sizes. The achieved results clearly demonstrate a considerable increase in the overall jamming efficiency of the proposed protocol-aware jammer in terms of packet delivery ratio, energy expenditure and detection probabilities over contemporary jamming methods provided in the literature.**

Index Terms: **Jamming detection, network allocation vector (NAV), protocol-aware jamming, random jamming, shot-noise.**

I. INTRODUCTION

Wireless local area networks (WLANs) have attained extensive appeal owing to their expediency, efficiency and utility. Rapidly decreasing infrastructure and technology costs have made them highly effective and triggered their worldwide deployments. The global deployment of commercial wireless networks including wireless fidelity (Wi-Fi), worldwide interoperability for microwave access (WiMax), global system for mobile communications (GSM), code division multiple access (CDMA), and long term evolution (LTE) have increased significantly in the last two decades.

Despite the advancements in technology, security in wireless networks remains principal concern for deploying wireless networking solutions to business. Wireless networks are physically exposed and opportunities for intrusion are high. The broadcast nature of WLANs introduces an inherent security flaw in wireless communication [1]. Advanced hacking attempts such as sniffing, rogue access points [2], bluesnarfing, bluejacking and denial of service (DoS) attacks [3] have presented serious security challenges to wireless networking. Significant has been documented on the security of wireless networks[4]–[8]. Several security mechanisms including access control, data integrity, data confidentiality, user authentication and anonymity have been proposed in the literature [5], [7], [9], [10]. Issues of quality of service (QoS) and discontinuity of the service have also been widely addressed [11], [12].

Denial of Services (DoS) attacks on wireless networks are considered among the major attacks because of the launching ease and effectiveness of these attacks. Radio frequency (RF) jamming [6], [9], [11]–[15] provides attackers with highly efficient and easily implementable methods to launch DoS attacks against the inherently insecure wireless broadcast medium. When working working on such attack models, one question always arises, "Why propose efficient and effective mechanisms to disrupt WLAN services? Is it prudent to devise new jamming mechanisms allowing hackers to disrupt WLAN services?" Although, jamming can be malicious as an attempt to disrupt WLAN services with the ultimate loss of data connectivity and communication, it can also facilitate protecting the most important targets by jamming remotely controlled wireless devices such as, cellular jammers. Whereas, we work on weaknesses in WLAN protocols by first launching intelligent attacks to identify potential vulnerabilities associated with the protocols, we then propose possible countermeasures to avoid such attacks. In this paper, our contributions are as follows:

- Implementing a novel protocol-aware RF jamming attack that exploits vulnerabilities at the physical (PHY) and medium access control (MAC) layers of WLANs. We also demonstrate that the proposed attack model is feasible to be implemented against any network whose channel and protocol characteristics are known to an attacker.
- Achieving high jamming efficiency.
- Launching stealthy jamming attacks against 802.11b, GSM and WiMax networks at different data rates.

Our results are based on experimentation in actual testbed environment. We demonstrate a significant improvement in jamming efficiency over 802.11, GSM, and WiMax networks as compared to the similar work proposed in the literature. The re-

Manuscript received April 2, 2014.

The research in this paper is partially supported through the project titled "SecureDial" (Secure Telephone and Fax), No. 20-1688/RD/2010/11 dated June 15, 2012 by Higher Education Commission, Islamabad-Pakistan.

A. Hussain is with School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST) Islamabad, Pakistan, email: abid.hussain@seecs.edu.pk.

N. A. Saqib and U. Qamar are with College of Electrical and Mechanical Engineering, National University of Sciences and Technology (NUST) Islamabad, Pakistan, email: {nazar.abbas, usmanq }@ceme.nust.edu.pk.

M. Zia and H. Mahmood are with Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan, email: {mzia, hasan}@qau.edu.pk.

Digital object identifier 10.1109/JCN.2014.000069

mainder of this paper is organized as follows.

Section II explains RF jamming principles and the channel access mechanisms in 802.11 networks. Section III provides a summary of similar work reported in the literature. The proposed probabilistic jamming models are explained in Section IV and V. We describe our experimental environment in Section VI. A discussion on the achieved results is presented Section VII. Section VIII provides our analysis on the effect of different packet sizes on the efficiency of random jamming mechanisms. Our conclusions are made in Section IX.

II. UNDERSTANDING RF JAMMING

In this Section we discuss important concepts and terminologies required for the understanding of the remainder of this paper. We briefly explain RF jamming and channel access mechanisms in WLANs. Further details can be accessed in [1], [16].

A. RF Jamming in WLANs

RF jamming attacks work on the basis of signal-to-noise ratio (SNR). SNR can be defined as the ratio of the power level containing the meaningful information of a primary modulated signal to the intensity of the background noise. The SNR model of wireless communication suggests that it is impossible to generate meaningful information from the primary modulated signal if the power level of ambient noise or noise produced by the jammer is sufficiently higher than the power level of the primary signal [17], [18].

A malicious node can launch a jamming attack in one of the two manners. (1) It can substantially increase the background noise by generating high power radio signal in the same frequency band, causing errors in the legitimate packets. The receiver would not be able to demodulate the primary signal correctly or recover the errors and therefore would discard those packets because of cyclic redundancy checksum (CRC) failure. (2) A malicious node can transmit legitimate packets with the valid frame headers without following the access mechanism of the deployed channel to deceptively indicate to other competing nodes that a legitimate transmission is in progress. The packet headers would be valid but the long payload is useless and random. As the attacker continuously transmits these unusable packets, the communication channel becomes busy denying access to other nodes.

B. Channel Access Mechanism in WLANs

802.11 WLAN MAC uses the carrier sense multiple access with collision avoidance (CSMA-CA) protocol for granting channel access to contending nodes. In wireless networks, collision is a receiver based phenomena. CSMA-CA unlike CSMA with collision detection (CD) lacks the ability to sense collisions during an ongoing transmission. The CSMA-CA protocol grants channel access to any node using two types of carrier sensing functions: Physical carrier sensing & virtual carrier sensing.

In physical carrier sensing when a node wishes to transmit, it waits for a fixed time known as the distributed inter frame spacing (DIFS) to sense if the channel is idle. If idle, the transmission is initiated. A collision can occur if two nodes sense that the channel idle, and simultaneously begin transmissions. Physical carrier sensing does not prevent two nodes from simultaneously initiating their transmissions as they are unable to hear eachother. In case that a collision occurs, there will be a low probability that packets arriving at the receiver would pass the CRC. Hence, they will be dropped owing to MAC checksum failure. In the ALOHA-based classical CSMA protocol, physical sensing is the only collision preventive mechanism. Since transmitters cannot detect collisions at the receiver, they will keep on transmitting and hence waste of energy. The error correction of collided frames depends entirely on the error detection and correction capability of the receiving nodes.

In virtual carrier sensing when a node wishes to transmit, it waits for a DIFS time to detect if the channel is busy as with physical carrier-sensing as explained above. If a node senses that the channel is idle, it initiates its transmission assuming no other node is transmitting. To reserve the channel for a fixed period, 802.11 frames carry a duration field. When a node transmits, it calculates the transmission time of the data packet based on the data rate and place this value in its duration field. In virtual carrier sensing, each client maintains a timer mechanism known as network allocation vector (NAV). When a frame is received and decoded by the clients, the NAV value on the client side is updated with the value from the duration field if it does not exceeds the current NAV value. This is to inform other nodes that the channel will remain busy owing to its transmission for the mentioned period. This NAV value serves the purpose of virtual carrier sensing at all other nodes in the sensing range of the currently transmitting node. The CSMA/CA protocol at each node implements a time counter function that is used to count the value of the network allocation vector. On each transmission every node in the network updates its counter value according to the transmitting packet NAV value and only senses the channel if its own NAV counter reaches zero. If in the first attempt the transmitting node discovers a transmission already in progress it randomly selects a waiting time slot from its contention window (CW). The node remains silent for this randomly chosen number of time slots and senses the channel again after this time interval. If the node again finds the channel busy, it assumes that large numbers of nodes are waiting for the channel and doubles its contention window. It then repeats the process. However the NAV counter adds vulnerability to the WLANs MAC protocol by broadcasting the time duration of the transmission and can be exploited by an attacker launching an intelligent jamming attack.

III. RELATED WORK

In this section we present a brief overview of the contemporary jamming techniques discussed in the literature. We also highlight jamming detection mechanisms and discuss three essential parameters: Packet delivery ratio (PDR), energy consumption and detection probability of a jammer.

A. Existing Jamming Techniques

Many jamming attack models have been reported in the literature . These attack models employ different strategies to jam the channel. Some of the more common models are explained below.

- Constant Jammer: A constant jammer continuously transmits random data without following channel access mechanisms of deployed network [12], [14]. Therefore, whenever a legitimate node attempts to access the channel, it finds the channel busy and hence backs off. If back off occurs continuously it forces the collision avoidance function to increase its contention window rapidly such that it reaches to its maximum time limit. It is considered as the most effective jamming technique as it causes complete disconnection among the participating nodes. However, the jammer employs huge energy cost and suffers high detection probability owing to its nonstop transmission [14].
- Deceptive Jammer: A deceptive jammer continuously transmits legitimate packets with valid packet headers that include a payload with random and useless data. It deceives the other nodes by simulating a valid transmission in progress [12]. Similar to constant jamming, deceptive jamming does not follow any valid channel access mechanism and therefore consumes an excessive amount of energy [6].
- Random Jammer: A random jammer makes its transmission by alternating between active and sleep intervals. In the active phase, it transmits for a predefined number of time slots; it then enters sleep phase where it remains dormant for specific period. In this manner, the jammer can save a significant amount of energy, the amount depending upon the length of sleep interval [12]. The jamming techniques discussed do not consider the traffic patterns of the underlying network. This may result in wastage of energy because the jammers may continue transmitting even if there is no legitimate traffic on the network.
- Reactive Jammer: A reactive jammer saves energy and computational resources by transmitting when it listens traffic on the network. It suspends its transmitter and senses the channel until a legitimate node initiates its transmission. Whenever signal is sensed, it sends RF signal adding noise to the ongoing transmission. The jammer enters into sleeping phase again when the legitimate node completes its transmission [9]. This is an effective jamming technique with a relatively low detection probability. A reactive jammer can save a substantial amount of energy if the channel remains idle for long durations.

B. Jamming Detection Mechanism

The major task in jamming detection is to differentiate between network congestion and a jamming attack by an adversary. Different jamming detection mechanisms have been developed. They utilize various network characteristics to identify the jamming, such as PDR, channel access, or carrier sensing time and signal strength ratio are exploited to detect RF jamming attacks [12], [14].

B.1 Packet Delivery Ratio (PDR)

Packet delivery ratio is the ratio between the number of correctly decoded packets and the total number of packets received by a particular node. A preset threshold is maintained at all the nodes in the network that is based on long-term average of the received packets. If PDR falls significantly below this threshold value, it is assumed that the network is jammed [9]. However, it is not valid to consider low PDR as only a jamming attack. PDR is also based on a number of channel parameters including distance between sending and receiving nodes, transmission power of the sender, multipath fading, modulation scheme, and error correction capability of the receiver. Similarly, network congestion and unexpected situations due to node failure can add further confusion to jamming detection.

B.2 Carrier Sensing Time

A legitimate node in a network can track channel access time whenever it transmits. If a jammer constantly transmits denying access of the channel to other nodes it will alarm the participating nodes that the channel is constantly busy, which could be a consequence of jamming.

This technique is efficient in detecting constant and deceptive jammers as they constantly keep the channel busy. However, it is not effective for detecting random and reactive jammers as they do not deny channel access to other nodes rather they only introduce errors to legitimate transmissions.

B.3 Signal Strength

As jammers generate high power signals, the signal strength is adversely affected by the transmission of the jamming signal. Jamming detection techniques based on signal strength distribution have been discussed in [14]. These techniques determine the state of the channel by: (1) Comparing the average of the received signal strength to a preset threshold value and (2) sampling the received signals and classifying them based on already available trained samples.

C. Jamming Efficiency

The majority of the proposed jamming attack models consider PDR as the measure of jamming efficiency. Those techniques ignore other equally important factors such as energy expenditure and detection probability of the jammer. In [6], the authors confirm that energy consumption and the detection probability of any jamming mechanism are directly proportional to the length of a transmission. Consequently, we consider the overall efficiency of the jammer consisting of three essential parameters: The packet drop ratio, the energy expenditure, and the detection probability. In the remainder of this section, we will discuss the overall efficiency of the above mentioned jamming techniques based on these parameters.

Both constant and deceptive jammers transmit continuously. Thus they occupy the channel for the entire time resulting in a packet drop ratio of 100. However, these jammers require a huge energy budget and their detection probability is high. Similarly, reactive jammers cause all the legitimate packets to drop. They may save energy depending upon the traffic patterns of underlying network. If we assume saturated network conditions, energy consumption and the detection probability of reactive jammers increase and approach those of the constant and deceptive jammer. The random jamming technique, conversely, attempts to lower energy consumption and the detection probability by suspending its transmitter for predefined time intervals. This may result in better PDR values as a large number of packets may pass uninterruptedly during the sleep phase of the jammer.

IV. MODELING SHOT-NOISE BASED RF JAMMING IN 802.11 WI-FI, GSM AND WIMAX NETWORKS

Our proposed model for RF jamming can be viewed as an intelligent variant of pulse jamming [11]. In pulse jamming, shot-noise bursts of a few microseconds are transmitted during the course of an ongoing transmission. These bursts cause the CRC function to drop data packets owing to checksum failure. However implementing pulse jamming is not easy. Modern wireless communication protocols deploy robust CRC functions, enhanced modulation, and error detection and correction mechanisms at different layers to reduce the effect of bit errors caused by noise. Thus in environments where there is constant traffic, implementing pulse jamming into practical use requires a significant number of noise bursts. In these scenarios, the pertinent question is, "What should be the length of the noise burst transmission and how much time should elapse between two consecutive pulses?"

In this work, we propose a novel RF jamming method that corrupts a sufficient number packet bits forcing a CRC check failure. This results in a retransmission request or packet drop owing to MAC checksum failure. We have implemented and tested the performance of proposed jamming method on commercial networks such as 801.11b, GSM, and WiMax. We have derived shot-noise bounds for 802.11b networks at data rates of 2, 5.5, and 11 Mbps. In an extension to this work we have also modeled shot-noise bounds for GSM and WiMax networks at data rates of 270.833 Kbps, 812.5 Kbps, 1083 Kbps, and 1354.2 Kbps, and 5 Mbps, 7.5 Mbps, 10 Mbps, and 15.1 Mbps respectively.

A. RF Jamming in 802.11b Wi-Fi Networks

Similar to any wireless communication, 802.11 networks are prone to channel errors caused by intentional and unintentional noise sources or due to environmental conditions. To minimize the effect of these bit errors, 802.11 networks employ convolutional code redundancy at the PHY layer. We can model the RF jamming in WLANs by calculating the maximum number of bits that can be corrected through the decoding algorithms. The calculated number will provide a close estimate for the duration of shot-noise pulses that can effectively distort a sufficient number of bits in a packet that will be beyond the error correction capability of the decoder at the receiving node.

Let us assume that a wireless PHY layer is employing convolutional coding with code rate R_c, and a random generating function $T(x, y)$. A probabilistic bound for the total number of correctable errors using convolutional code can be found in [8]. Let us assume that the bit crossover probability on a memoryless binary symmetric channel is p.The maximum likelihood decoder uses the hamming distance metric for error correction. The all-zeros path will be replaced with a path containing hamming distance if and only if there are at-least $(d+1)/2$ or more transmission errors that occur at specific d positions [16]. Therefore,

$$P_k = \begin{cases} \sum\limits_{e=(k+1)/2}^{k} \binom{k}{e} p^e (1-p)^{k-e} & \text{if } k \text{ is odd} \\ \frac{1}{2}\binom{k}{k/2} p^{k/2}(1-p)^{k/2} & \\ \quad + \sum\limits_{e=(k/2)+1}^{k} \binom{k}{e} p^e (1-p)^{k-e} & \text{if } k \text{ is even} \end{cases} \tag{1}$$

where k is the Bernoulli trial and P_k is the probability of a specific k_{th} Bernoulli trial. A complete modulation symbol consisting of L bits transmitted using the convolutional coding will be distorted if it collides with a shot-noise pulse of equal or longer duration. Convolutional coders use interleaving techniques to spread data bits over multiple modulation symbols to reduce the burst errors. However, interleaving techniques are generally not preferred owing to added complexity in encoding and decoding functions. Therefore, we can safely assume that the coder at the 802.11 PHY layer does not use the interleaving function for the modulation of the data. It should be further noted that because of the linear nature of convolutional coding, data bits could span over two symbols. Thus, to ensure that two modulation symbols are unrecognizable, we must transmit a shot-noise pulse of duration equal to the transmission time of the two symbols plus the guard time between the symbols. Hence, the duration of the shot-noise pulse is: $T_N = 2 \times T_L + T_G$, where T_L is the symbol transmission time and T_G is the guard time. Moreover, we further investigate the total number of pulses required to purge the effect of error correction techniques as follows.

Let us assume that there are S modulation symbols in a MAC layer frame and there are no channel-induced errors. Let X represent the number of unrecognizable symbols resulting from the transmission of one shot-noise pulse, R denotes the total redundancy bits appended in a MAC frame and Y is the number of symbols that can be corrected based on R bits. Then, at least $Y+1$ symbol errors are required to successfully make the checksum failure and hence the packet drop at MAC layer. Let us further assume that, to induce at least $Y + 1$ symbol errors in a frame we require M number of shot-noise pulses. Then we have $XM \geq Y + 1$. Therefore,

$$M \geq \frac{Y+1}{X}. \tag{2}$$

Given M number of pulses per frame of S symbols and

Probability(Pr) {One pulse deforms one symbol} = P, then

Pr {0 symbol distorted in M pulses}

$$= \binom{M}{0} P^0 (1-P)^M, \tag{3}$$

Pr {1 symbols distorted in M shot-noise pulses}

$$= \binom{M}{1} P^1 (1-P)^{M-1}, \tag{4}$$

...

Pr {up to Y symbols distorted in M shot-noise pulses}

$$= \sum_{i=0}^{Y} \left(\begin{array}{c} M \\ i \end{array} \right) p^i (1-p)^{M-i}, \tag{5}$$

Pr {M pulses cause ≥Y+1 symbol errors }

$$1 - \sum_{i=0}^{Y} \binom{M}{i} p^i (1-p)^{M-i}. \tag{6}$$

B. RF Jamming in GSM and WiMax Networks

The model for RF jamming 802.11 Wi-Fi networks described in the previous section can be further extended to GSM and WiMax networks. Based on PHY and MAC layer characteristics of these networks, the length of shot-noise pulses can be calculated to effectively implement jamming on those networks.

GSM and WiMax networks use a frequency hopping spread spectrum (FHSS) technique at the PHY layer to avoid channel-induced errors resulting from noise. A typical GSM network uses 64 different frequencies between 890–960 MHz in the GSM 900 band. Similarly a typical WiMax networks uses 100 frequencies in the 2.4 GHz frequency range. We have spread the jamming signal on those 64 and 100 frequencies for GSM and WiMax networks respectively to avoid synchronization overhead and simplify the jamming process. Since GSM and WiMax networks use maximum distance separable (MDS) block code at MAC layer for further strengthening the error correction capability of convolutional coding at the PHY layer, the number of shot-noise pulses required to force a failed error correction on those networks can be computed as follows.

Let us assume that there are k total bits (data + redundancy) in a MAC frame. The data bits are modulated in n data symbols and $k - n$ redundancy bits are modulated into R parity symbols. If we assume that R parity symbols can correct K symbols successfully, it requires at least $K + J$ symbol errors to cause checksum failure, where J ranges from $1, \cdots, N$. The probability that a transmitted pulse will distort $> K + J$ symbols follow the exponential random variable given as:

$$P[S_e = K] = (1 - p_e)^{k-1} p \tag{7}$$

$$P[S_e = K] = \frac{1}{2}(e)^{\frac{R}{2W}} \tag{8}$$

where S_e is the symbol error, R is the average power in the signal, and P is the total noise induced by the jamming signal. If a shot-noise pulse can distort b symbol errors and MDS block code can correct $\frac{n-k}{2}$ symbol errors; then $N_s \geq [r/2 + 1]$ shot-noise pulses are required to purge the effect of the MDS code beyond recovery. Solving for b yields:

$$bN_s \geq \frac{n-k}{2} + 1, \tag{9}$$

$$N_s \geq \frac{1}{2b}(n - k + 2). \tag{10}$$

Because we are transmitting jamming signals on on every frequency channel, we must consider the average power per channel of the jamming signal. The capacity loss of a channel by a jamming signal can be calculated as follows.

Let us assume that B_s is the bandwidth of the transmission signal, P_s is the average power of this signal and P_T is the total power of the jamming signal, that is, $P_T = B_s(N_o + J_o)$ then the capacity of the channel will be

$$C = B_s \log_2(1 + \frac{P_s}{P_T}). \tag{11}$$

V. PROPOSED PROTOCOL-AWARE RF JAMMING ARCHITECTURES

For verification of probabilistic models presented in Section IV, we propose two shot-noise based RF jamming algorithms, that are: Shot-noise based random jammer and data-rate adaptive protocol aware jammer.

A. Shot-Noise based Random Jammer

In most practical scenarios the jammer is not aware of the transmission parameters of the underlying network. The proposed shot-noise based random jammer specifically deals with these situations. The proposed jamming algorithm substantially boost the jamming efficiency by fine tuning its transmission parameters. The Jammer works as follows.

The jammer maintains one of two states at any given time. It is either in sleeping state or in active state. In sleeping state the jammer is dormant while in active state it transmits shot-noise pulses.

If we assume that an 802.11 network requires 2,100 μs to transmit its longest data packet [1] we customize the jammer to remain in sleeping state for a fixed duration of 2,100 μs and then transmits shot-noise pulses of fixed lengths. Thus a jammer emits a trains of noise pulses with a gap of 2,100 μs. The process of transition between active and sleeping states continues for J seconds depending on how long the jamming is to execute. After J seconds, we calculate the PDR through our own deployed packet capturing node. If the calculated PDR is above the threshold value we lower the sleeping time interval by 300 μs (the smallest amount of time to transmit one complete packet at the highest rate in 802.11b). The proposed algorithm for the shot-noise based random jammer is presented in Algorithm 1.

Algorithm 1 shot-noise based random jammer algorithm

```
1:  procedure RANDOM JAMMER
2:      T_i ← 2100μs
3:      T_j ← GetJammingPulseDuration
4:      while T_j do
5:          Wait(T_i)
6:          JammingPulse(T_j)
7:      end while
8:      if PDR_j < PDR_thresh then
9:          Decrement T_i by 300μs
10:         GoTo4
11:     end if
12:     return T_i
13: end procedure
```

In this method, the jammer generates shot-noise pulses of 1 μs after each predefined fixed time interval at a data rate of 11

Mbps. In this manner 11 bits are transmitted each time. This significantly reduces the energy consumption as well as the detection probability of the jammer.

B. Data-Rate Adaptive Protocol-Aware jammer

In 802.11 wireless networks, different data rates are used for transmission by the stations. The selection of a specific data rate is a function of the channel characteristics and environmental conditions. The channel characteristics that determine the transmission rate include ambient noise in transmission channel, PDR, bit error rate, and total transmission load on an access point (AP). The nodes in 802.11 network dynamically alter their data rates during a communication based on the PDR and buffer space of the receiver. These dynamic changes in data rates trigger change in the modulation scheme, symbol transmission rate, and time. Moreover, channel sensing and data transmission or receiving cannot be accomplished simultaneously by a wireless node [1], [16]. Thus, determining the time interval for data transmission of a legitimate node is not possible if the jammer is continuously transmitting noise signals. If a jammer is able to determine the traffic pattern and transmission duration of a node it can significantly increase its overall efficiency.

Algorithm 2 Algorithm for protocol-aware intelligent jammer

1: **procedure** PROTOCOL AWARE JAMMER
2: $T_{\text{NAV}} = GetPacketNAV$
3: $T_{\text{mid}} = T_{NAV}/2$
4: **while** $T_{\text{NAV}} > 0$ **do**
5: **if** $T_{\text{NAV}} = T_{\text{mid}}$ **then**
6: $JammingPulse(T_{\text{pulse}})$
7: **end if**
8: Decrement T_i by 300μs
9: $GoTo4$
10: **end while**
11: **end procedure**

Based on this principle, we have investigated the MAC layer protocol and formulated a strategy to determine the start of the transmission and the time to complete the transmission by a particular node. The proposed jamming mechanism makes use of the NAV and works as follows.

As explained in Section II, when an 802.11 enabled wireless node initiates its transmission, it updates the duration field of the frame with the time it expects to occupy the channel for the data transmission. All the stations on the network use this time value to update their NAV.

In this proposed technique, the jammer sniffs an ongoing transmission by a legitimate node to capture the NAV value of the packet. Based on this value the jammer is able to determine the duration of transmission and data transmission rate of this communication. This calculation provides the jammer with the suitable time to transmit. The jammer does not make its transmission during the entire period of the legitimate communication rather it emits shot-noise pulses for some T_1 μs and rests for further T_2 μs.

The T_1 and T_2 time durations are determined based on the NAV values, the data rate at which this particular node is transmitting, and data encoding scheme in use. From our experiments, we have found that the data rate has a significant impact on the jammer's efficiency. The PDR of a particular node increases if it is operating at a lower data transmission rate. Considering the effect of the data rate and increasing the jamming efficiency at lower data rates, we have implemented a data rate adaptive jamming as presented in Algorithm 2.

Based on NAV values we can determine the transmission data rate of a particular node if we transmit packets of equal size. To implement this particular jamming technique, we set three threshold values based on NAV. All these NAV values are calculated for a MAC frame size of 2,312 bytes. The threshold values determine the behavior of the jammer and change the pulse duration in the following manner.

- If the sniffed NAV value ranges from zero to 1,700 μs, we can safely assume that this particular transmitting node is a using data rate of 11 Mbps. Calculating the number of symbols per microsecond we derive to 1.375 symbols in 1 μs. This ipmlies that if the jammer transmits for 1 μs it will ideally deform 1.375 symbols. However, this is not actually the case. BPSK, QPSK and other modulation schemes used by 802.11 networks apply spaces between two consecutive symbols. This is referred to as the inter-symbol space. This space avoids overlapping of two consecutive symbols during the propagation of signals on the air and minimizes the effect of inter-symbol interference (ISI). Further, owing to the linear nature of binary convolutional codes, data bits are spread over two or more symbols. It could occur that the shot-noise pulse overlaps the inter symbol space and does not completely distort it or data bits are present in two symbols and the decoder demodulates the data correctly. This method requires relatively longer shot-noise pulses to avoid this situation. For this reason, we use shot-noise pulses of 2 μs in our experiments.
- The data rate of 5.5 Mbps is used when the received NAV value is greater than 1,899 μs and less than 3,400 μs. A shot-noise pulse of 2 μs is sufficient to eliminate the effect of error correction redundancy and consequently packet drop will occur owing to MAC checksum failure.
- A NAV value greater than 9,000 μs implies that it means that data transmission is at the 2 Mbps data rate. We require longer shot-noise pulse of 3 μs to effectively diminish the effect of error correction redundancy beyond recovery.

VI. EXPERIMENTAL SETUP

For experimental evaluation of the proposed jamming methodologies, we used two sets of different transmission/reception apparatus. We employed a D-Link DWL 650 PCMCIA wireless Network Interface Card (NIC) as a jamming device to transmit fixed length shot-noise pulses to validate the proposed jamming methods on the Wi-Fi networks. We deployed an indoor network of two wireless transceivers equipped with standard 2.4 GHz 802.11 NICs on Linux OS, and standard D-Link 2.4 GHz Wireless Router. Both NIC and wireless router use open source device drivers given at [19]. The standard channel access mechanism of the NIC was modified according to the requirements of our proposed jamming methodology as discussed in the previous section.

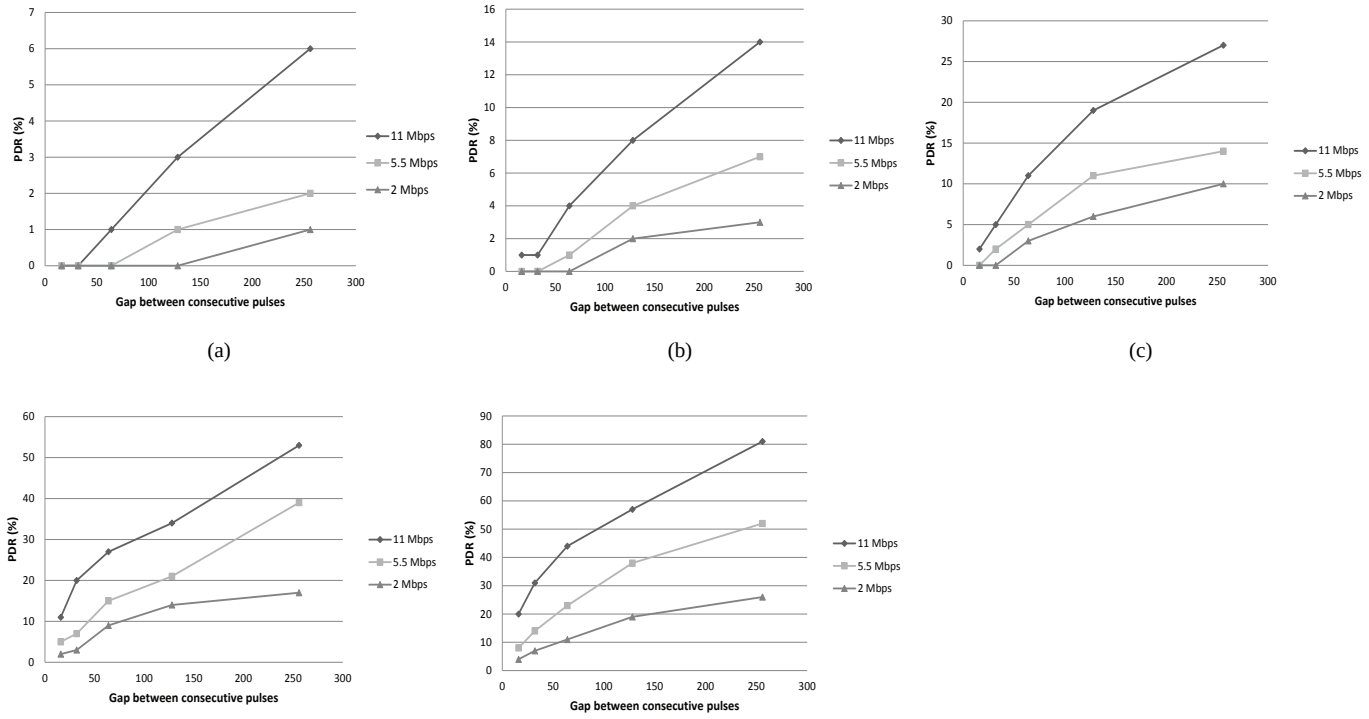


Fig. 1. Shot-noise based random jamming on Wi-Fi networks, jamming pulse of duration: (a)16 μs, (b)32 μs, (c)64 μs, (d)128 μs, and (e)256 μs.

Table 1. Packet delivery ratio of protocol aware jammer for Wi-Fi networks.

Data rate adaptive jammer			
Packet sent ratio	Packet delivery ratio		
	11 Mbps	5.5 Mbps	2.0 Mbps
100	0.0	1.0	1.6

For evaluating the proposed data rate adaptive jamming in the Wi-Fi, GSM, and WiMax networks, we employrd real testbed comprising of Universal Software Radio Peripheral kits [20] mounted with daughter cards for GSM, Wi-Fi, and WiMax networks operating at 900 MHz, 2.4 GHz, and 5 GHz Respectively. GNU radio software was configured over laptops connected with USRP kits. Wireshark packet sniffers was deployed at a separate node for collection packet traces transmitted by every node.

VII. PERFORMANCE RESULTS AND DISCUSSIONS

The results of the proposed shot-noise based random jamming attack model on Wi-Fi networks are presented in Fig. 1. PDR has been calculated by transmitting different length jamming pulses. From the obtained PDR, it is observed that when employing a sleeping time interval below 900 μs, the PDR is low and the variation in data rate has no effect. Increasing the sleeping time interval results in an increase in PDR to approximately 50% at a sleeping time interval of 2,100 μs.

The elevated PDR is a consequence of long sleeping time intervals between consecutive shot-noise pulses. Because there is no jamming activity in this time interval, many packets pass uninterruptedly, resulting in a higher PDR. A second factor behind this high PDR is the data rate. The proposed jamming model addresses all the transmissions at all the data rates. At the lower data rate of 2.0 Mbps the number of symbols per second is significantly lower than at the data rate of 11 Mbps. Hence, fewer bits are affected by the jammer pulses and they can be recovered more effectively by the error correction mechanisms at the MAC layer on the receiving nodes.

Figs. 2 and 3 present the results of the shot-noise based random jammer for the WiMax and GSM networks. We have used different shot-noise jamming pulse widths to evaluate the effect of jamming on these networks. It has been observed that frequency hopping spread spectrum (FHSS) significantly reduces the effect of jamming in these networks. In FHSS, a data signal is transmitted over many hopping frequencies and the probability of a jammer being able to synchronize with these hopping frequencies is substantially reduced. Furthermore, both WiMax and GSM deploy forward error correction (FEC) at the MAC layer in addition to physical layer redundancy that considerably improves the error correction capability of these networks.

The experimental results of the proposed data rate adaptive shot noise based protocol aware jammer are presented in Table 1. Results indicate that data rate has a minor effect on the jamming efficiency. As with the previous results, this is because at the data rate of 2 Mbps, a relatively fewer number of bits are being affected by the jamming compared to at the higher data rates of 5.5 and 11 Mbps. The results also indicate that the pro-

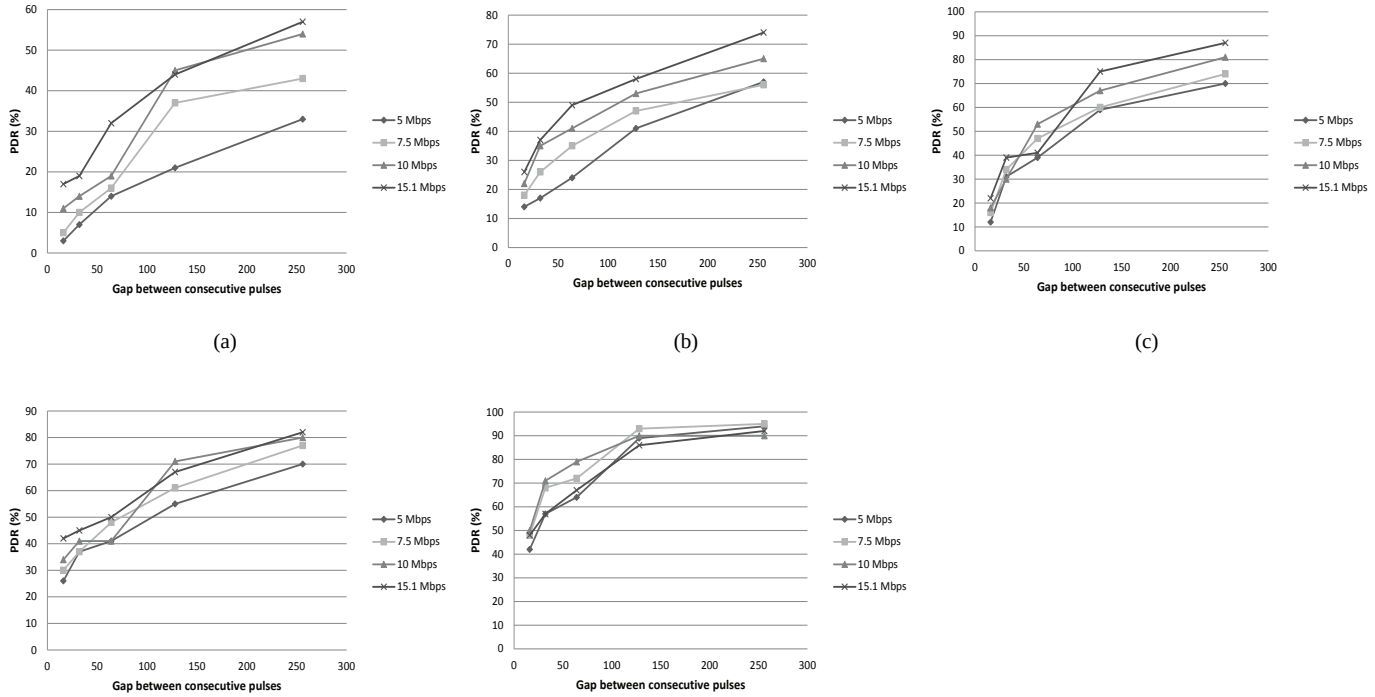


Fig. 2. Shot-noise based random jamming on WiMax networks, jamming pulse of duration: (a)16 μs, (b)32 μs, (c)64 μs, (d)128 μs, and (e)256 μs.

posed protocol-aware RF jamming is highly effective in all perspectives of jamming. This attack model is cost effective in terms of energy expenditure and has a significantly reduced probability of detection.

When the channel is jammed by shot-noise pulses the size of packets become an important consideration. In our extended work, we have also evaluated the effect of packet sizes on jamming.

VIII. EFFECT OF PACKET SIZE ON JAMMING

802.11 networks provide support for exchanging packets of different sizes. Furthermore, longer packets can also be fragmented at the MAC layer in error prone and noisy environments. The fragmentation of packets is usually used to avoid longer retransmissions. The fragmentation of longer packets at the MAC layer considerably improves PDR in error prone network environments. However, the fragmentation of packets require additional headers that are necessarily required to reassemble those packets before forwarding to upper layers. The extra overhead of frame headers substantially decreases the overall throughput of the network. For this reason, it is not frequently used in normal network conditions. To evaluate the effect of different packet sizes on the proposed jamming techniques we transmitted packets of varying sizes ranging from 128 Kbps to 1024 Kbps at different data rates. We present the results in Table 2.

The results presented in Table 2 indicate shows that the proposed jamming method is extremely efficient for all packet sizes. The rationale behind this high jamming efficiency is that the proposed technique processes all packets equally without considering size, nature or time it takes to transmit.

Table 2. Effect of packet size on data rate adaptive jammer.

Effect of packet size on data rate adaptive jammer				
Packet size (Bytes)	Packet send Ratio (%)	Packet delivery ratio (%)		
		11 Mbps	5.5 Mbps	2.0 Mbps
128	100	1.0	0.9	0
256	100	0.7	0.5	0
384	100	0.9	0.0	0
512	100	0.5	0.0	0
640	100	0.0	0.0	0
768	100	0.0	0.0	0
896	100	0.0	0.0	0
1023	100	0.0	0.0	0

IX. CONCLUSION

In this work, we proposed two efficient jamming techniques: A low data rate random jamming and shot-noise based protocol-aware jamming. Both proposed jamming methodologies utilize shot-noise pulses to induce sufficient number of errors in the transmitted packets to cause MAC checksum failures resulting in repeated retransmission. The benefit of using shot-noise pulses is twofold: Jammers are energy efficient and their detection probability is significantly reduced. Both of these features are highly desired because of their deployment in hostile environments. Further, we evaluated the effect of different packet

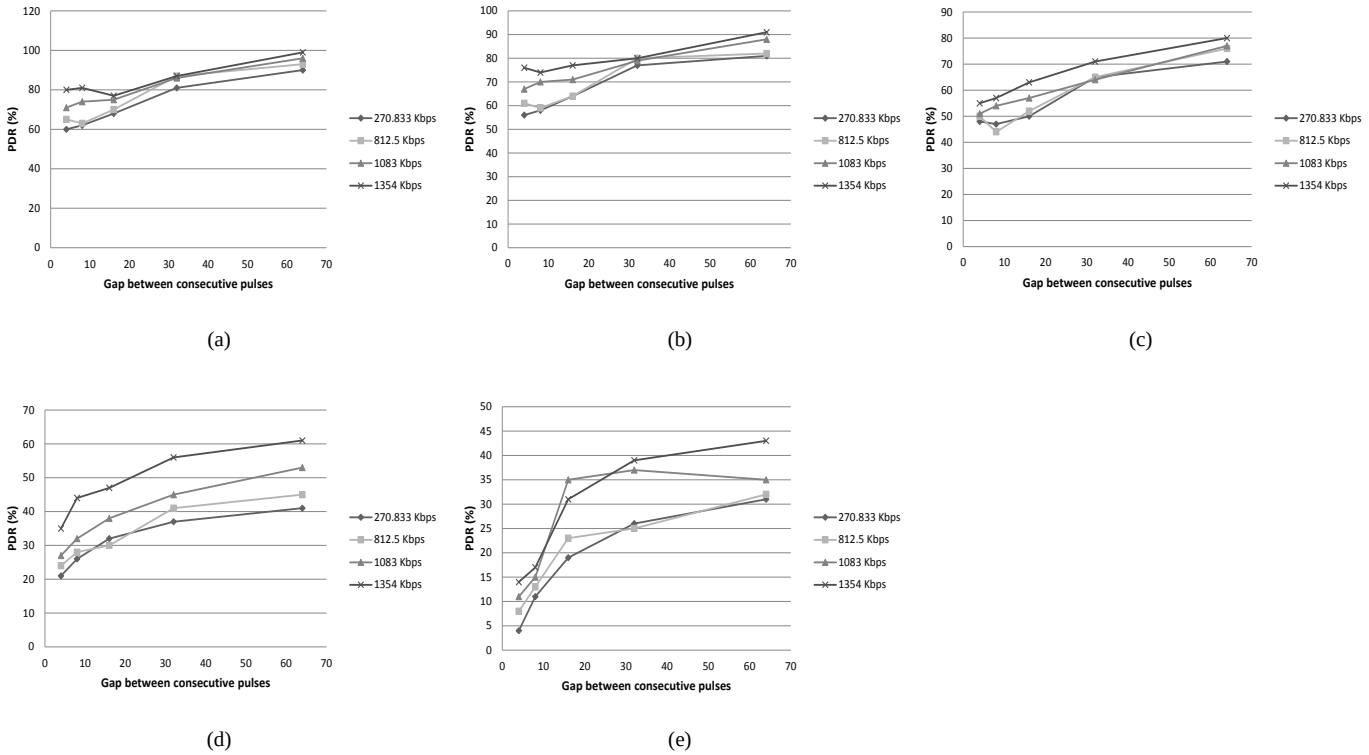


Fig. 3. Shot-noise based random jamming on GSM networks, jamming pulse of duration: (a)16 μs, (b)32 μs, (c)64 μs, (d)128 μs, and (e)256 μs.

sizes on the proposed jamming methodologies as an extension yo our work. Considering the overall efficiency of these techniques, it is suggested that necessary modifications must be implemented in MAC layer protocols to avoid jamming attacks in wireless networks.

Future work includes determining modifications to wireless MAC protocols to prevent jamming and to investigate efficient detection mechanisms that can differentiate between packet losses due to congestion and packet losses due to jamming.

REFERENCES

[1] *IEEE Standard for Wireless LAN-Medium Access Control and Physical Layer Specification*, IEEE Standard P802.11, 1999.

[2] D. Kotz and K. Essien. *Analysis of a Campus-Wide Wireless Network* [Online]. Available: http://dx.doi.org/10.1007/s11276-004-4750-0

[3] G. Legg. (2005) *The bluejacking, bluesnarfing, bluebugging blues: Bluetooth faces perception of vulnerability* [Online]. Available: http://www.wirelessnetdesignline.com/showArticle.jhtml

[4] P. Kyasanur and N. H. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks," in *Proc. IEEE DSN*, 2003, pp. 173–182.

[5] A. A. Cárdenas, S. Radosavac, and J. S. Baras, "Detection and prevention of MAC layer misbehavior in ad hoc networks" in *Proc. ACM SASN*, 2004, pp. 17–22.

[6] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, pp. 41–47, May 2006.

[7] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," *ACM SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, pp. 29–30, July 2003.

[8] T. X. Brown J. E. James, and A. Sethi, "Jamming and sensing of encrypted wireless ad hoc networks," in *Proc. ACM MobiHoc*, 2006, pp. 120–130.

[9] W. Xu, W. Trappe, and Y. Zhang, "Anti-jamming timing channels for wireless networks," in *Proc. ACM WiSec*, 2008, pp. 203–213.

[10] Y. Zhang and Wenke Lee, "Intrusion detection in wireless ad-hoc networks," in *Proc. ACM MobiCom*, 2000, pp. 275–283.

[11] D. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proc. IEEE MILCOM*, Oct. 2006, pp. 1075–1081.

[12] G. Alnifie and Robert Simon, "A multi-channel defense against jamming attacks in wireless sensor networks," in *Proc. ACM Q2SWinet*, 2007, pp. 1075–1081.

[13] A. Hussain and N. A. Saqib, "Protocol aware shot-noise based radio frequency jamming method in 802.11 networks," in *Proc. IEEE WOCN*, 2011, pp. 1–6.

[14] W. Xu *et al.*, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM MobiHoc*, 2005, pp. 46–57.

[15] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in *Proc. IEEE SECON*, 2007, pp. 60–69.

[16] *IEEE Standard for Information Technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and physical layer (PHY) specifications*, IEEE Standard, 2007.

[17] Y. W. Law *et al.*, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," in *Proc. ACM SASN*, 2005, pp. 76–88.

[18] Y. W. Law *et al.*, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," *ACM Trans. Sen. Netw.*, vol. 5, no. 1, pp. 6:1–38, Feb. 2009.

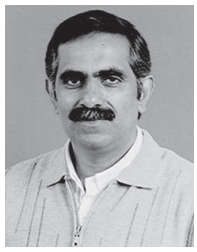
[19] *The Specifications of PCMCIA 650 NIC* [Online]. Available: http://www.dlink.com/products/?pid=23

[20] *The Universal Software Radio Peripheral* [Online]. Available: https://www.ettus.com/

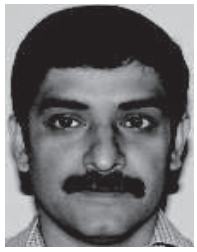
Abid Hussain received his M.S. degree in Information Technology in 2010 from School of Electrical engineering and Computer Science (SEECS), National University of Science and Technology (NUST) and is currently a Ph.D. candidate at SEECS-NUST, Islamabad Pakistan. His research interests include Wireless channel band adaptation, physical and MAC layer attacks in wireless networks and stochastic modelling of physical and MAC layer behaviour of wireless networks.

Nazar Abbas Saqib recieved his M.Sc. and M.Phil degrees in Electronics from Quaid-i-Azam University Islamabad in 1993. He received his Ph.D. degree in Electrical Engineering from CINVESTAV-IPN, Mexico. He is currently working as Associate Professor at Department of Computer Engineering, NUST College of Electrical and Mechanical Engineering, Islamabad-Pakistan. His research interests include computer and communication security, cryptographic hardware and FPGA based system design. Nazar has also co-authored a book titled 'Cryptographic Algorithms on Reconfigurable Hardware' with Springer New York in 2005.

Usman Qamar is currently an Assistant Professor at Department of Computer Engineering, College of Electrical and Mechanical Engineering, NUST, Islamabad, Pakistan. He is heading the "Data and Text Mining" Centre of the Department of Computer Engineering, College of Electrical and Mechanical Engineering, NUST, Islamabad, Pakistan. He has over 5 years of experience in data mining and data engineering both in academic and industry. His M.Phil and Ph.D. degrees are in the field of Data Mining from University of Manchester, UK. During his Post-Doc also from Manchester he was involved in various data mining projects for the industry.



Muhammad Zia received M.Sc. degree in 1991 and M.Phil degree in 1999, both from Department of Electronics at Quaid-e-Azam University, Islamabad, Pakistan. He received Ph.D. degree from the Department of Electrical and Computer Engineering at the University of California, Davis in 2010. His research interests are in the area of wireless communications and signal processing, with current emphasis on the wireless security, compressive sensing, bandwidth efficient transceiver design and blind and semi-blind detection of Space-Time Block Codes. Dr. Zia is with Department of Electronics at Quaid-i-Azam University, Islamabad.



Hasan Mahmood received the M.Sc. degree in Electronics from Quaid-i-Azam University, Islamabad in 1991, M.S degree in Electrical Engineering from University of Ulm in 2002. From 1994 to 2000, he was with the Department of Electronics, Quaid-i-Azam University, Islamabad as a Faculty Member. He received the Ph.D. degree from Stevens Institute of Technology in 2007. He is currently with the department of Electronics, Quaid-i-Azam University, Pakistan as an Assistant Professor.