Journal of Information & Communication Technology
Vol. 5, No. 2, (Fall 2011) 74-79

A Theoretical Framework for Modulation Based Adaptive Jamming Technology

Ehtesham Khan *
Sumayya Meraj *
Syed Abbas Ali *
N.E.D. University of Engineering & Technology

ABSTRACT

In communication, wireless communication has the vital importance, due to its transferability, movability and instant connectivity. The cell-phone jamming technology has become a major objective of secure communication, but it also ceases the necessary GSM service. In jamming technology, to extemporize the discontinuity of necessary service, adaptive jamming has been introduced. In this paper a theoretical framework for modulation based adaptive jamming technology is proposed which is based on altered frequency band. The reliability and robustness of proposed solution is prominent due to vital experimental results of the modulation technique. The research mainly targets GSM Networks' security and proposes to enhance its confidentiality level. Here hardware is integrated with software to customize its usage and increase more features.

INSPEC Classification : B61, B62, C56, D4

Keywords : Modulation technique, Adaptive jammer, Domain interchangeability, Altered frequency, GSM band

1. INTRODUCTION

The vitality of adaptive jamming technology is still a challenging task and research is being done on it. Several experimental results based on modulation techniques are reported to improve the robustness and reliability of the wireless system(Roder 2006). In this paper, the proposed idea provides the theoretical framework of modulation based solution for adaptive jamming technology to overcome the headache of jammers. Jammers generates signals of GSM frequencies in contra direction of incoming signals thus superimpose GSM frequencies(Lin, Xiaoli and Jun 2010).

We propose to bring GSM band (coming from base tower) below the ranges of signal generated by jammer through modulation is called altered frequency band. For uplink we have to adjust a networking application programming interface (API) of smart-phone, provided by smart-phone manufacturer to operate on modulated frequency. For downlink

* The material presented by the authors does not necessarily portray the viewpoint of the editors and the management of the Institute of Business and Technology (IBT) or N.E.D. University of Engineering & Technology.

* Ehtesham Khan : ehtesham_khan@live.com
* Sumayya Meraj : sumayya_meraj@live.com
* Syed Abbas Ali : saaj.scholar@yahoo.com

we need to apply demodulation on modulated signal to transmit GSM frequency to the base tower. For authentication we have to develop a smart-phone application (software) which consist password authentication service through server. Also that smart-phone application will daily synchronize its schedule from the server to automate the connectivity of the smart-phone for an allocated time (e.g. Smart-phones of employees will be non-operable in the period of meeting).

2. METHODOLOGY

The proposed solution is a combination of hardware and software, in which only an authorized person can access its cell-phone in an allocated time. To provide the required solution, we need to develop frequency domain based on altered frequency band and altering device signal below the range of signal generated by jammer through modulation to adaptively jam the target region. This domain would be developed through the modulation technique by applying the Frequency Shift Keying (FSK) through which GSM band alter to low frequency band (by Frequency Altering Device)(Hasegawa 2010). When the frequency modulates into the altered band (i.e. below to GSM Band) it cannot be accessible by any general cell-phone. To gain access the cell-phone application (software) is used which tunes the transceiver of cell-phone onto that altered frequency band. The cell-phone transceiver is made to work with the least of 450MHz frequency band(Schmidt, Digel and Berroth 2011).

3. THEORETICAL FRAMEWORK

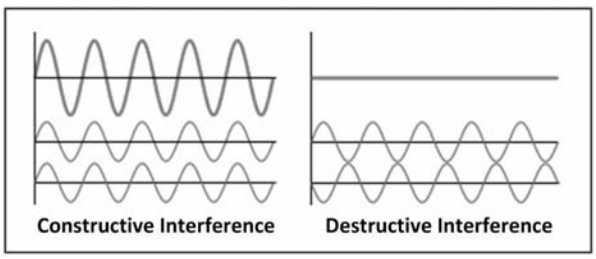
To elaborate the theoretical framework for modulation based adaptive jammer, we have divided our proposed solution into three different phases:

3.1.Frequency Band Modulation/Demodulation
3.2.GSM Band Jamming
3.3.Smart-phone (Application)

3.1. Frequency Band Modulation/Demodulation

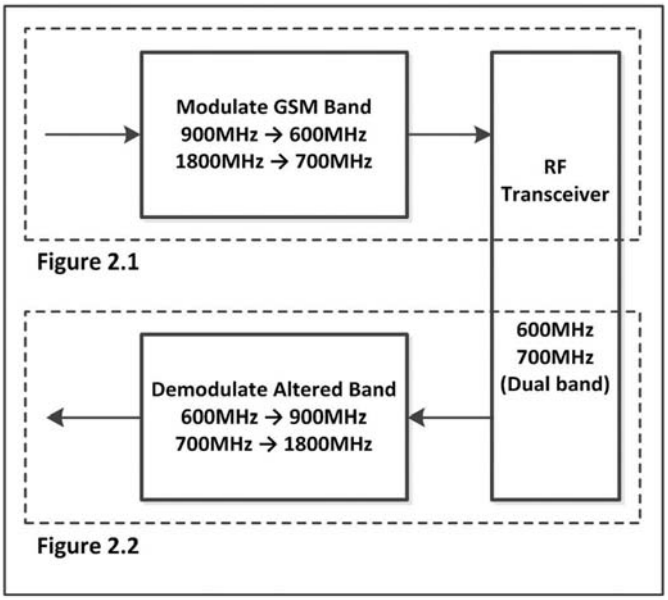
The critical part of this frequency band analysis is modulation and demodulation phase. This is the behavior of jammers that they work destructive interference which itself is based on superposition principle (Wikipedia n.d.). "When two or more waves are incident on the same point, the total displacement at that point is equal to the vector sum of the displacements of the individual waves. If a crest of a wave meets a crest of another wave of the same frequency at the same point, then the magnitude of the displacement is the sum of the individual magnitudes - this is constructive interference. If a crest of one wave meets a trough of another wave then the magnitude of the displacements is equal to the difference in the individual magnitudes this is known as destructive interference" (Feynman, Leighton and Sands 1969), as illustrated in Figure1.

Figure 1
Superposition principle



The frequency band of jammers are set according to the GSM bands used in a particular region which generates waves of same amplitude 180° out of phase with normal GSM band to jam the upcoming frequencies. In this phase of our proposed solution, we are interested to generate signal using frequency band altering device from incoming GSM frequency band (Coming from base tower) signal below the signal generated by jammers through modulation techniques. In Modulation phase we modulate using Frequency Shift Keying (FSK) the receiving frequency range of 900 MHz to 600 MHz and 1800 MHz to 700 MHz thus we can attain these altered frequencies across jammed area. The question is why we have used Modulation technique to transform our transmitted signal? The answer is reliability and lossless transformation of signal which no other techniques can perform as modulation does, see in Figure 2 (Figure 2.1). When base station receives the GSM frequency Band of 900/1800 MHz, we need to step up the transmitted frequency of 600/700 MHz back to the GSM frequency range, illustrated in Figure 2 (Figure 2.2).

Figure 2
Working mechanism of Frequency Band Modulation/Demodulation

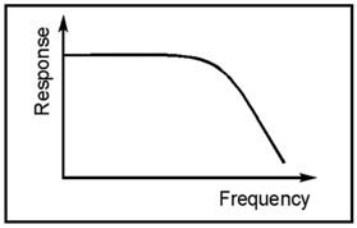


3.2. GSM Band Jamming

In this phase of our proposed solution, we deals with the discontinuity of GSM signals as default, within the area which will be adaptively jam and altered frequency band below the range of signal generated by jammer. The phenomenon of filters is used in GSM Band Jammer in order to restrict the communication like other cell-phone jammer, but due prior alteration of frequencies makes it unique. A filter is a device or process that removes unwanted component or feature from desired signal. A plethora of literatures are available to define the different types of filters(Wikipedia n.d.). In this portion, we reviewed the basic definition and concept of the filters used in GSM jammer. The graphical representation of the Low-Pass, High-Pass, Band-Pass and Band-Stop filter outputs can be seen in Figure 3 to Figure 6 respectively.

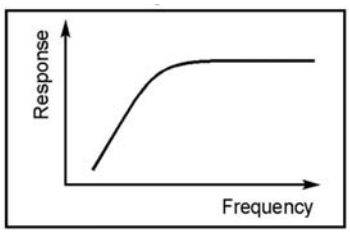
i. **Low-Pass Filter:**"A low-pass filter (LPF) is a filter that passes low-frequency signals but attenuates (reduces the amplitude of) signals with frequencies higher than the cut-off frequency."

Figure 3



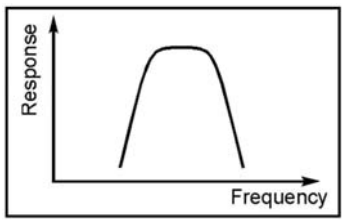
ii. **High-Pass Filter:**"A high-pass filter (HPF) is a filter that passes high frequencies and attenuates (reduces the amplitude of) signals with frequencies lower than its cut-off frequency."

Figure 4



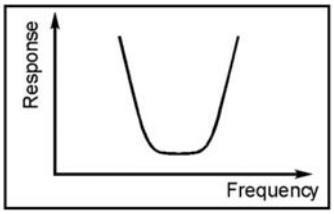
iii. **Band-Pass Filter:**"A band-pass filter is a filter that passes frequencies within a certain range and rejects (attenuates) frequencies outside that range."

Figure 5



iv. **Band-Stop Filter:**"A band-stop filter is a filter that passes most frequencies unaltered, but attenuates those in a specific range to very low levels. It is the opposite of a band-pass filter."

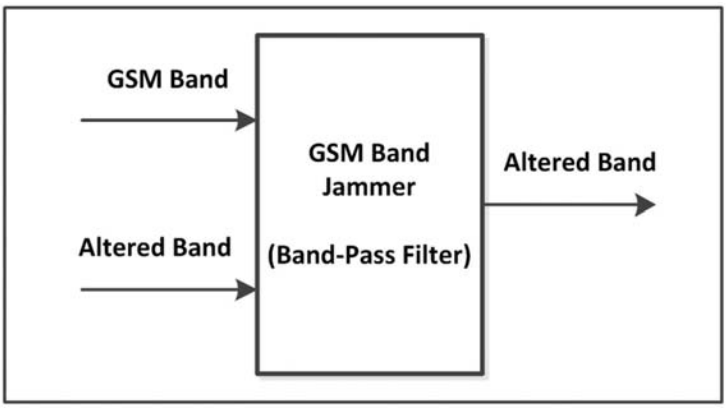
Figure 6



When the GSM Frequency Band superimposed with GSM Jamming signals it discontinues

the GSM signals or GSM frequencies as default in the premises. While the Altered Frequency Band will pass as traditionally assuming that band-pass filter allow or pass the altered frequency band, illustrated in Figure 7.

Figure 7
Working mechanism of GSM Band Jamming



3.3. Smart-Phone

Wireless communication devices like mobiles have a built-in radio frequency (RF) transceiver which is programmed to manipulate with incoming signals normally 900/1800MHz frequencies. That is why, to make them operable on 600/700MHz we need to configure the RF transceiver of mobile phone so as to adopt altered frequency band as illustrated in Figure 2. Normally mobile phones manufactured world-wide can work on 900/1800MHz that is the GSM range. We have to configure RF transceiver of mobile phone through API provided by mobile phone manufacturers. By that API the smart-phone application (software) will be develop which will configure the RF transceiver, also limit the misuse of the solution through server authentication and various other features. This limitation could be handled and demonstrated by using FM frequencies.

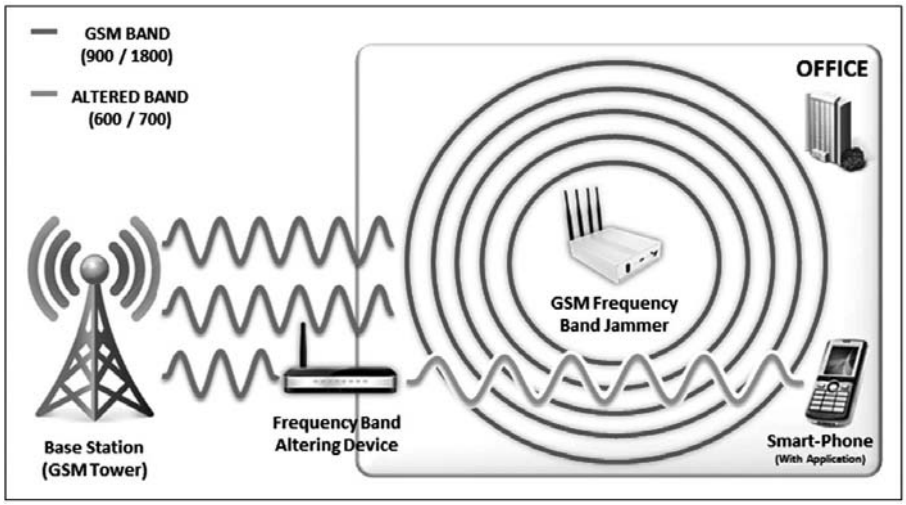
Figure 8 illustrates the proposed solution. GSM Frequency (i.e. 900/1800 MHz) which is coming from the base station is converted into the Altered Frequency (i.e. 600/700 MHz) through Frequency Altering Device. Then GSM Frequency Band Jammer allows only the Altered Frequency within the premises and blocks all the other frequencies. Then smart-phone with the application (software) which has configured to transmit or receive the message on the Altered Frequency could be able to communicate within the jammed area after authenticating its identity through server authentication, while the visitors or unauthenticated cell-phones remains disconnected from GSM service.

4. CONCLUSIONS

Adaptive jamming is an ideal solution for secure communication and proposed idea of wireless communication under jammed circumstances through modulation makes it unique of its kind. The reason using modulation techniques is that the probability of signal attenuation and information loss is minimal in modulation and original message can be easily obtained with the demodulation using a wireless modem. The altered frequency band solution is for an organization premise, where the user transmits or receives message in modulated frequency of 600MHz which is actually ideal for wireless communication because lower range frequencies have least chances of attenuation. To the best of the

author's knowledge, no direct implementation of the proposed framework has been done for adaptive jamming technology so far. The proposed theoretical framework is supported by the different implementation phases discussed in section 3. Using modulation based solution for adaptive jamming technology; we have an expectation of achieving the goal of adaptively in providing secure communication.
?

Figure 8
Diagrammatic Illustration of proposed solution



5. REFERENCES

Feynman, Richard P, Robert B Leighton, and Matthew L Sands, 1969. *Lectures on Physics, Book 1. Reading*, Mass, Addison-Wesley Pub. Co.

Hasegawa, K., 2010. "High-selectivity tunable bandpass filters with low insertion loss." *Microwave Conference Proceedings (APMC), 2010 Asia-Pacific*. Yokohama, 1130-1133.

Li, Lin, Xiaoli Xi, and Jun Wang., 2010. "Research on GPS anti-jamming algorithm based on adaptive antennas." *Signals Systems and Electronics (ISSSE), 2010 International Symposium*. Nanjing, 1-4.

Roder, H., 2006. "Amplitude, Phase, and Frequency Modulation." *Proceedings of the Institute of Radio Engineers*, August 2006: 2145-2176.

Schmidt, M., J. Digel, and M. Berroth., 2011. "Class-S power amplifier concept for mobile communications in rural areas with concurrent transmission at 450 MHz and 900 MHz." *Microwaves, Communications, Antennas and Electronics Systems (COMCAS), 2011 IEEE International Conference*. Tel Aviv, 1-4.

Wikipedia. n.d. http://www.wikipedia.org/wiki/Destructive_interference

Wikipedia. n.d. http://www.wikipedia.org/wiki/Filter_(signal_processing)