ISSN 2047-3338

Analysis and Study of Denial of Service Attacks in Wireless Mobile Jammers

S.M.K .Chaitanya[1], P. Naga Raju[2], Y.N.V.L. Ayyappa[3] and Vundavalli Ravindra[4]
[1,2,3,4]Nova College of Engineering & Technology JangaReddy Gudem, West Godavari, India

***Abstract*– Nature of the medium in wireless networks makes it easy for an adversary to launch a Wireless Denial of Service (WDoS) attack. Recent studies, demonstrate that such attacks can be very easily accomplished using off-the shelf equipment. To give a simple example, a malicious node can continually transmit a radio signal in order to block any legitimate access to the medium and/or interfere with reception act is called jamming and the malicious nodes are referred to as jammers. Jamming techniques vary from simple ones based on the continual transmission of interference signals, to more sophisticated attacks that aim at exploiting vulnerabilities of the particular protocol used. In our article, we mention a detailed up-to-date discussion on the jamming attacks recorded in the literature. We also describe various techniques proposed for intrusion detecting in the presence of jammers. Finally, we survey numerous mechanisms which attempt to protect the network from jamming attacks. We final discuss better security for intrusion detection in wireless mobile jammer which is efficient to existing one.**

***Index Terms*– Wireless Networks, Intrusion, Jammers and Security**

I. INTROUDCTION

JAMMING is the radiation of electromagnetic energy in a communication channel which reduces the effective use of the electromagnetic spectrum for legitimate communication.Jamming results in a loss of link reliability, increased energy consumption, extended packet delays and disruption of end-to-end routes [1]. Jamming may be both malicious with the intention to block communication of an adversary or non-malicious in the form of unintended channel interference. In the context of embedded wireless networks for time-critical and safety critical operation such as in medical devices and industrial control networks, it is essential that mechanisms for resilience to jamming are native to the communication protocol. Resilience to jamming and its avoidance [2], collectively termed as anti-jamming, is a hard practical problem as the jammer has an unfair advantage in detecting legitimate communication activity due to the broadcast nature of the channel. The jammer can then emit a sequence of electromagnetic pulses to raise the noise floor and disrupt [3] [4] communication. Communication nodes are unable to differentiate jamming signals from legitimate transmissions or changes in communication activity due to node movement or nodes powering off without some minimum processing at the expense of local and network resources.

WLANs use the 2.4 and 5 GHz license-free spectrum for communication. This spectrum is shared by other wireless devices and protocols such as cordless phones, microwave ovens, Bluetooth devices, etc. These devices and protocols often do not coexist well together and can create mutual interference when co-located and operating concurrently. WLANs use the IEEE 802.11 protocol to avoid collisions between different devices and allow fair sharing of the medium. WLAN Denial of Service can be intentional (by an attacker in the vicinity) or unintentional (neighboring devices interfering with each other) as illustrated in Fig. 1.

WLAN devices sense the RF medium to determine if the channel is free before transmitting their own packets. The protocol is referred to as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).In CSMA, a device wishing to transmit has to first listen to the channel for a predetermined amount of time so as to check for any activity on the channel. If the channel is idle, the device is allowed to transmit. If the channel is busy, the device has to defer its transmission. Collision Avoidance schemes tend to beless "greedy" when it comes to grabbing the channel and back off transmission for random intervals if they sense activity. In essence, WLANs are designed to "play nice" on the shared communication medium. On the contrary, devices such as microwave ovens simply spew energy in the 2.4 GHz band when they are powered up. Other devices such as wireless video cameras might use a continuous wave modulation scheme where they

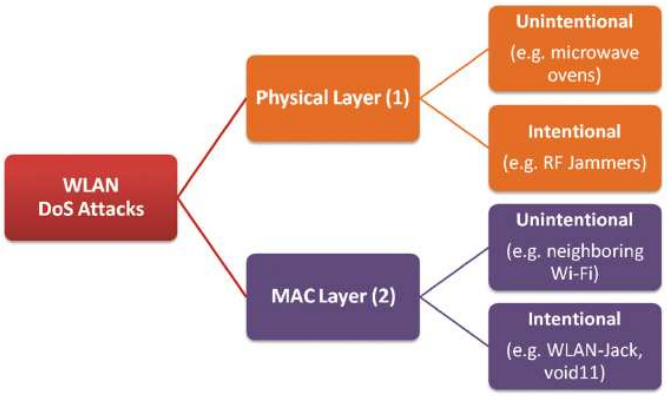

Fig. 1: Denial of Service scenarios for WLANs Physical Layer Vulnerabilities

are always radiating energy on a given RF channel. If these devices are operating in the vicinity of a WLAN, they can effectively shut down all WLAN communication because devices will defer their transmissions until they sense that the medium is idle. Malicious RF jammers are also freely available on the internet. These devices are illegal and are specifically designed to disrupt wireless communications. Figure 2 shows a handheld, quad-band, cellular and 2.4 GHz band jammer that uses a 6.0V Ni MH battery pack with an approximate battery life of one hour. The device has a total output power of 1200 mW (a typical WLAN access point normally operates at 100 mW). Such a device can effectively block WLAN communication within a 30 meter radius. Very high power jammers capable of radiating 200 W of power, effective over a 1 km, are also available in the black market.

A. MAC Layer Vulnerabilities

The 802.11 MAC is particularly vulnerable to DoS. The current standard protects only data frames and leaves various control and management frames subject to manipulation by an attacker. Since the ratification of the IEEE 802.11i standard in 2004, WLANs have been able to provide strong authentication of wireless devices and encryption of data traffic. The 802.11i standard uses the IEEE 802.1X Extensible Authentication Protocol (EAP) to guarantee that only authorized devices gain access to the wireless network and uses the Advanced Encryption Standard (AES) to guarantee confidentiality and integrity of the data communications between authenticated devices. IEEE 802.11i is the basis for the WPA2 (Wi-Fi Protected Access 2) industry standard. A major limitation in the 802.11i standard is that no protection is available for management or control frames that establish connections and, in general, affect the behavior of WLANs. Tools such as "wlan-jack", "hunter-killer" and "void11" exploit the lack of management and control frame protection to mount DoS attacks in WLANs.

II. INTRUSION DETECTION SYSTEM

Intrusion detection systems (IDS) process large amounts of monitoring data. As an example, a host-based IDS examines log files on a computer (or host) in order to detect suspicious activities. Network-based IDS, on the other hand, searches network monitoring data for harmful packets or packet flows

A. Types of Intrusion Detection System

Network –based intrusion detection system [NIDS] that tries to detect malicious activity such as denial of service attacks, port scan or even attempts to crack into computer by monitoring network traffic. NIDS does this by reading all incoming packets and trying to find number of TCP connection requests to a very large number of different ports is observed, one could assume that there is someone conducting a port scan of some or all of the computers in the network. It mostly tries to detect incoming shell codes in the same manner that an ordinary intrusion detection system does. Often inspecting valuable information about an ongoing intrusion can be learned from outgoing or local traffic and also work with other systems as well, for example update some firewalls blacklist with the IP address of computers used by suspected crackers.

Host-based intrusion detection system [HIDS] monitors parts of the dynamic behavior and the state of computer system, dynamically inspects the network packets. A HIDS could also check that appropriate regions of memory have not been modified, for example- the system-call table comes to mind for Linux and various v table structures in Microsoft windows. For each object in question usually remember its attributes (permissions, size, modifications dates) and create a checksum of some kind (an MD5, SHA1 hash or similar) for the contents, if any, this information gets stored in a secure database for later comparison (checksum-database). At installation time- whenever any of the monitored objects change legitimately- a HIDS must initialize its checksum-database by scanning the relevant objects. Persons in charge of computer security need to control this process tightly in order to prevent intruders making un-authorized changes to the database.

Protocol-based intrusion detection system [PIDS] typically installed on a web server, monitors the dynamic behavior and state of the protocol, and typically consists of system or agent that would sit at the front end of a server, monitoring the HTTP protocol stream. Because it understands the HTTP protocol relative to the web server/system it is trying to protect it can offer greater protection than less in-depth techniques such as filtering by IP address or port number alone, however this greater protection comes at the cost of increased computing on the web server and analyzing the communication between a connected device and the system it is protecting.

Application protocol based intrusion detection system [APIDS] will monitor the dynamic behavior and state of the protocol and typically consists of a system or agent that would sit between a process, or group of servers, monitoring and analyzing the application protocol between two connected devices.

B. Categories of Intrusion Detection System

Intrusion detection is classified into two types: 1) Misuse detection and, 2) Anomaly detection. Misuse detection uses well-defined patterns of the attack that exploit weakness in system and application software to identify the intrusions (Kumar and Spafford, 1995). These patterns are encoded in advance and used to match against user behavior to detect intrusions. Anomaly detection identifies deviations from the normal usage behavior patterns to identify the intrusion. The normal usage patterns are constructed from the statically measures of the system features, for example the CPU and I/O activities by a particular user or program. The behavior of the user is observed and any deviation from the constructed normal behavior is detected as intrusion.

C. What is Anomaly?

Anomaly detection refers to detecting patterns in a given data set that do not conform to an established normal behavior. The patterns thus detected are called anomalies and translate to critical and actionable information in several application

domains. Anomalies are also referred to as outlier, surprise deviation etc.

Most anomaly detection algorithms require a set of purely normal data to train the model and they implicitly assume that anomalies can be treated as patterns not observed before. Since an outlier may be defined as a data point which is very different from the rest of the data, based on some measure, we employ several detection schemes in order to see how efficiently these schemes may deal with the problem of anomaly detection. The statistics community has studied the concept of outliers quite extensively. In these techniques, the data points are modeled using a stochastic distribution and points are determined to be outliers depending upon their relationship with this model. However with increasing dimensionality, it becomes increasingly difficult and inaccurate to estimate the multidimensional distributions of the data points. However recent outlier detection algorithms that we utilize in this study are based on computing the full dimensional distances of the points from one another as well as on computing the densities of local neighborhoods.

The deviation measure is our extension of the traditional method of discrepancy detection. As in discrepancy detection, comparisons are made between predicted and actual sensor values, and differences are interpreted to be indications of anomalies. This raw discrepancy is entered into a normalization process identical to that used for the value change score, and it is this representation of relative discrepancy which is reported. The deviation score for a sensor is minimum if there is no discrepancy and maximum if the discrepancy between predicted and actual is the greatest seen to date on that sensor. Deviation requires that a simulation be available in any form for generating sensor value predictions. However the remaining sensitivity and cascading alarms measures require the ability to simulate and reason with a causal model of the system being monitored. Sensitivity and cascading Alarms

An appealing way to assess whether current behavior is anomalous or not is via comparison to past behavior. This is the essence of the surprise measure. It is designed to highlight a sensor which behaves other than it has historically. Specifically, surprise uses the historical frequency distribution for the sensor in two ways. It is those sensors and to examine the relative likelihoods of different values of the sensor. It is those sensors which display unlikely values when other values of the sensor are more likely which get a high surprise scores. Surprise is not high if the only reason a sensor's value is unlikely is that there are many possible values for the sensor, all equally unlikely.

III. SURVEY ON JAMMERS

To understand the inherent tradeoff between energy efficient link protocols with well-defined schedules and their susceptibility to jamming attacks, we first describe the different types of jammers and their impact on various types of link layer protocols. We then highlight a particular class of statistical jammers and their impact on energy-efficient sensor network link protocols.

A. Comparison of Jamming Models

Xu et al. [7], [8] introduce four common types of jammers: constant, random, reactive and deceptive. Constant jammers continually emit a jamming signal and achieve the highest censorship of packets corrupted to total packets transmitted. The constant jammer, however, is not energy-efficient and can be easily detected and localized. The random jammer is similar to the constant jammer but operates at a lower duty cycle with intervals of sleep. A random jammer transmits a jamming signal at instances derived from a uniform distribution with a known minimum and maximum interval. The censorship ratio of the random jammer is constant and invariant to channel utilization. At low duty cycles, the random jammer is difficult to detect and avoid.

A reactive jammer keeps its receiver always on and listens for channel activity. If a known preamble pattern is detected, the reactive jammer quickly emits a jamming signal to corrupt the current transmission. Reactive jammers, while effective in corrupting a large proportion of legitimate packets, are not energy efficient as the receiver is always on. Another type of reactive jammer uses a simple physical layer energy detector as sensing and wake-up radios. These agile jammers wait until channel activity is detected and then jam. Although energy to 'listen' is lower, this behavior is also energy in efficient since any kind of channel activity triggers a transmission of a jamming pulse. Due to physical layer delays these jammers are effective in jamming the fraction of packets that are greater than a certain threshold length. A deceptive or protocol-aware jammer is one that has knowledge of the link protocol being used and the dependencies between packet types. Such a jammer exploits temporal and sequential patterns of the protocol and is very effective.

In [9], a statistical jamming model is described where the jammer first observes temporal patterns in channel activity, extracts a histogram of inter-arrival times between transmissions and schedules jamming pulses based on the observed distribution. This results in a very effective jammer that is not protocol-aware and is also difficult to detect. A statistical jammer chooses its transmission interval to coincide with the peak inter arrival times and is thus able to maximize its censorship ratio with relatively little effort. Fig. 2(a) illustrates the relative censorship ratio and the energy-efficiency of the different jammers. Fig. 2(b) illustrates the relative stealth or difficulty in detection. We observe that the statistical jammer has a high censorship ratio with both energy-efficient and stealthy operation and hence focus on combating such jamming.

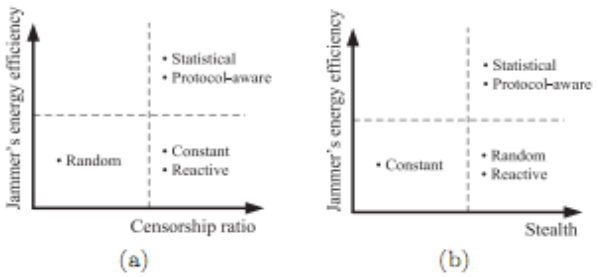

Fig. 2: Jammer's Energy efficiency vs. : (a) Censorship ratio, (b) Stealth

B. Techniques for Robust Transmission

The traditional defenses against jamming include spread spectrum techniques [10] and frequency hopping at the physical layer. While these techniques are important physical layer mechanisms for combating jamming, additional protection is required at the packet-level. As in the case of standard wireless protocols such as IEEE 802.11 and Bluetooth, the jammer may know the pseudorandom noise code or frequency hopping sequence. There have been several effort to make communication in sensor networks more robust in the presence of a jammer. In [11], Wood et al. described DEEJAM, a link layer protocol that includes several schemes for robust IEEE 802.15.4 based communication for reactive and random jammers. While mechanisms such as coding and fragmentation are proposed, the jammer still has a competitive advantage in that it may increase the power of its jamming signal and a single jamming signal is capable of jamming multiple links in the vicinity. The authors assume that reactive jammers can be considered energy-efficient.

Current radio transceivers with the IEEE 802.15.4 physical layer of communication use almost the same, if not greater, energy for receiving as they do for transmission [12]. In cases where resilience to jamming is not possible, it is useful to detect and estimate the extent to which the jammer has influence over the network. A jammed area mapping protocol is described in [13] which can be used to delineate regions affected by a jammer. Such information can ultimately be used for network routing. One of the requirements of the protocol is that every node knows its own position along with positions of all its neighbors. WisperNet does not require such position and direction information and directly computes routes with the highest end-to-end packet delivery rate.

C. Impact of Jamming on MAC Protocols

We now investigate the characteristics of different classes of sensor network link protocols and the impact of a jammer on each class.

1). Energy-Efficient MAC Protocols: Several MAC protocols have been proposed for low power operation for multi-hop wireless mesh networks. Such protocols may be categorized by their use of time synchronization as asynchronous [14], loosely synchronous [15], [16] and fully synchronized protocols [17], [18]. In general, with a greater degree of synchronization between nodes, packet delivery is more energy-efficient due to the minimization of idle listening when there is no communication, better collision avoidance and elimination of overhearing of neighbor conversations.

2). Asynchronous protocols: Asynchronous protocols such as Carrier Sense Multiple Access (CSMA) are susceptible to jamming both at the transmitter (busy channel indication) and at the receiver (energy drain). The Berkeley MAC (B-MAC) [8] protocol performs excellent in terms of energy conservation and simplicity in design. B-MAC supports CSMA with low power listening (LPL) where each node periodically wakes up after a sample interval and checks the channel for activity for a short duration of 0.25ms. If the channel is found to be active, the node stays awake to receive the payload following an extended preamble. Using this scheme, nodes may efficiently check for neighbor activity while maintaining no explicit schedule which a statistical jammer may exploit.

3). Loosely-Synchronous: Loosely-synchronous protocols such as S-MAC [9] and T-MAC [18] employ local sleep-wake schedules know as virtual clustering between node pairs to coordinate packet exchanges while reducing idle operation. Both schemes exchange synchronizing packets to inform their neighbors of the interval until their next activity and use CSMA prior to transmissions. S-MAC results in clustering of channel activity and is hence vulnerable to a statistical jammer.

4). Synchronous protocols: Synchronous protocols such as RT-Link [12], utilize hardware based time synchronization to precisely and periodically schedule activity in well-defined TDMA slots. RT-Link utilizes an out-of-band synchronization mechanism using an AM broadcast pulse. Each node is equipped with two radios, an AM receiver for time synchronization and an 802.15.4 transceiver for data communication. A central synchronization unit periodically transmits a 50µs AM sync pulse. Each node wakes up just before the expected pulse epoch and synchronizes the operating system upon detecting the pulse.

As the out-of-band sync pulse is a high-power (30W) signal with no encoded data, it is not easily jammed by a malicious sensor node.

In general, RT-Link outperforms B-MAC which in turn out-performs S-MAC in terms of battery life across all event intervals [12]. Fig. 2 shows the relative node lifetimes for 2AA batteries and similar transmission duty cycles. Here node

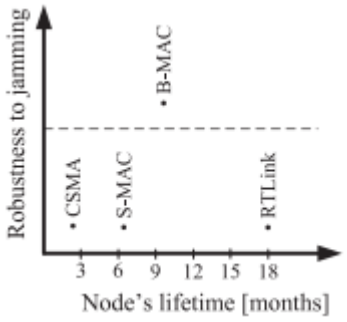

Fig. 3: Comparison of robustness to jamming and energy efficiency of sensor MAC protocols

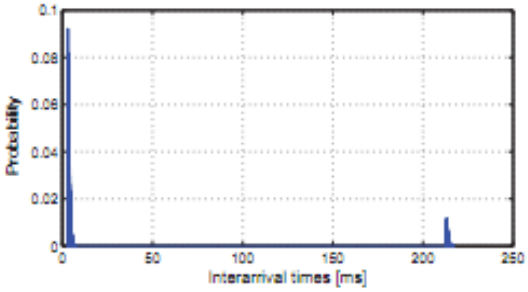

Fig. 4: SMAC PDF for 15% utilization

lifetimes for CSMA, S-MAC, B-MAC, and RT-link are 0.19, 0.54, 0.78 and 1.5 years respectively for a network of 10 nodes with a 10s event sample period (based on measurement values from [12], [9]). While RT-Link nodes communicate in periodic and well defined fixed-size time slots, a statistical jammer is able to easily determine the channel activity schedule and duration of each scheduled transmission. An attacker can glean the channel activity pattern by scanning the channel and schedule a jamming signal to coincide with the packet preamble at the start of a time slot.

5). Statistical Jamming: We focus on the statistical jammer's performance with S-MAC and RT-Link as both results in explicit patterns in packet inter-arrival times. We do not consider BMAC as we aim to leverage the more energy-efficient RT-Link as a base synchronized link-layer mechanism for WisperNet. We simulated a network of 10 nodes in each case, with a 3ms average transmission duration. In the case of S-MAC, we observe that all nodes quickly converge on one major activity period of 215ms. In Fig. 3, we also notice a spike close to 2ms. This is the interval between the transmission of control packets and data packets at the start of an activity period. In the case of RT-Link, we simulated four flows with different rates and hence observe 4 distinct spikes in Fig. 4. The other spikes with lower intensity are harmonics due to multiples of 32 slots in a frame. In both cases we observe distinct inter-arrival patterns which enable a statistical jammer to efficiently attack both protocols.

IV. PROPOSED SYSTEM DESCRIPTION

Problem statement of wireless network is a portable cell phone jammer featured by universal and hand held design, could blocking worldwide cell phone networks within 0.5-10 meters, including GSM900MHz, GSM1800MHz, GSM850MHz /CDMA800MHz and also 3G networks (UMTS /W-CDMA).

A mobile phone jammer is an instrument used to prevent cellular phones from receiving signals from or transmitting signals to base stations. When used, the jammer effectively disables cellular phones. These devices can be used in practically any location, but are found primarily in places where a phone call would be particularly disruptive because silence is expected.

A. Operation

As with other radio jamming, cell phone jammers block cell phone use by sending out radio waves along the same frequencies that cellular phones use. This causes enough interference with the communication between cell phones and towers to render the phones unusable. On most retail phones, the network would simply appear out of range. Most cell phones use different bands to send and receive communications from towers (called full-duplexing). Jammers can work by either disrupting phone to tower frequencies or tower to phone frequencies. Smaller handheld models block all bands from 800MHz to 1900MHz within a 30-foot range (9 meters). Small devices tend to use the former method, while larger more expensive models may interfere directly with the tower. The radius of cell phone jammers can range from a dozen feet for pocket models to kilometers for more dedicated units. The TRJ-89 jammer can block cellular communications for a 5-mile (8 km) radius.

Actually it needs less energy to disrupt signal from tower to mobile phone, than the signal from mobile phone to the tower (also called base station), because base station is located at larger distance from the jammer than the mobile phone and that is why the signal from the tower is not so strong.

Older jammers sometimes were limited to working on phones using only analog or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America. The jammer's effect can vary widely based on factors such as proximity to towers, indoor and outdoor settings, presence of buildings and landscape, even temperature and humidity play a role. There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers. However, like cell phones, most of the devices in common use operate at low enough power output (<1W) to avoid causing any problems.

B. Intrusion Detection for Better Wireless Network Security

A good design and development cooperation between the wireless equipment provider and network infrastructure provider has the best chance of providing security features to the user. Government regulations may impose restrictions but good improvement can still be made.

Good security should be an added feature in existing wireless communication devices. Users that don't need it should not have to pay for it. On the other hand, users that want very secure communication devices should have that option available to them at an acceptable cost. For example,

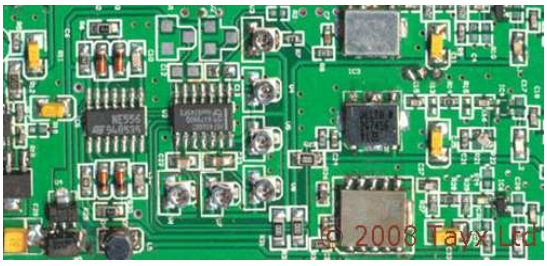

Fig. 5: Example of mobile jammer

Fig. 6: TRJ-89 Jammer

users could be offered the use of compatible but specialized user equipment when better security is needed. This is already being done in some cellular systems for large-scale emergency communications where public safety officials are issued special cell phones that have good interference immunity and priority access to the cell tower.

The best security will be achieved when security features are added at each networking layer and each physical entity of the network. It is not enough to simply encrypt the source data or provide simple spread spectrum at the physical layer. However, well-designed spread-spectrum should be an essential feature of new designs.

Wireless air links must employ highly adaptive error detection and correction algorithms if the raw data throughput is to be efficiently preserved. This means that the algorithm must recognize the basic error rate of the air link and adjust its robustness and efficiency accordingly. For example, a simple CRC code may be used when errors are very low while a long Reed-Solomon code with interleaving may be used when the errors are high. Intrusion detection is essential. Zhang and Lee [20] have outlined the intrusion issues for wireless ad-hoc networks and conclude that an intrusion detection agent (IDS) for all nodes is a key architecture. They also point out that detection must be both node-local and node cooperative in that collective statistics can be gathered so the network as a whole can make a decision about intrusion.

It is best to avoid ad-hoc networks except where its benefits outweigh the security risks. A robust medium access control (MAC) designed for mobility and security is another essential need for wireless. Frequency hopping is a superior anti-interference design when its data latency can be tolerated. All systems should have two-way authentication and user equipment should allow several levels of user intervention to protect against intrusion. At a minimum, the user should be able to ask for re-authentication of the access point or an entire ad-hoc network if needed. Newer, somewhat novel ideas such as IP hopping should be considered and field tested for a wireless mobile environment and interference avoidance capability is always a good alternative.

V. CONCLUSION

The paper presents a LPC2148 based mobile signal jammer is used to block the signal in all the network i.e., 3G, CDMA networks. By implementing this problem we can block the signals simultaneously in all the networks using time limit if any attack will occur in the jammer our analysis help to detect the intrusion which provides better security. In our work we discuss on security issues on wireless mobile jammers, types of intrusion in current process how to avoid finally the proposed system mode of operation and the better security presents effective compare to existing one.

REFERENCES

[1] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In ACM MobiHoc, 2005.

[2] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service. In ACM WiSe, pages 80–89, 2004.

[3] Y. W. Law et al. Energy-efficient link-layer jamming attacks. In ACM SASN, 2005.

[4] A. J. Viterbi. Spread Spectrum Communications: Myths and Realities. In IEEE Comm. Magazine, 2002.

[5] A. D. Wood, J. A. Stankovic, and G. Zhou. DEEJAM: Defeating Energy-Efficient Jamming. IEEE SECON, 2007.

[6] Texas Instruments Inc. Chipcon CC2420 Data Sheet, 2003.

[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In ACM MobiHoc, 2005.

[8] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service. In ACM WiSe, pages 80–89, 2004.

[9] Y. W. Law et al. Energy-efficient link-layer jamming attacks. In ACM SASN, 2005.

[10] A. J. Viterbi. Spread Spectrum Communications: Myths and Realities. In IEEE Comm. Magazine, 2002.

[11] A. D. Wood, J. A. Stankovic, and G. Zhou. DEEJAM: Defeating Energy-Efficient Jamming. IEEE SECON, 2007.

[12] A. D. Wood, J. A. Stankovic, and S. H. Son. JAM: A Jammed Area Mapping for Sensor Networks. In IEEE RTSS, 2003.

[13] J. Polastre, J. Hill, and D. Culler. Versatile Low Power Media Access for Wireless Sensor Networks. SenSys, November 2005.

[14] W. Ye, J. Heidemann, and D. Estrin. An energy-efficient MAC protocol for wireless sensor networks. IEEE INFOCOM, 2002.

[15] A. El-Hoiydi and J. Decotignie. WiseMac: An Ultra Low Power MAC Protocol. ISCC, 2004.

[16] L.F.W. van Hoesel and P.J.M. Havinga. A lightweight medium access protocol for wireless sensor networks. INSS, 2004.

[17] A. Rowe, R. Mangharam, and R. Rajkumar. RT-Link: A Time-Synchronized Link Protocol for Energy Constrained Multi-hop Wireless Networks. IEEE SECON, 2006.

[18] T. Dam and K. Langendoen. An adaptive energy-efficient mac protocol for wireless sensor networks. SenSys, November 2003.

[19] Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad-Hoc Networks”, Proceedings of the sixth arinual International Corlfererice on Mobile computing and Nefit,orking (MobiCom 2000), Boston, Massachusetts, Aug 6-1 1, 2000.

S.M.K. Chaitanya pursuing M. Tech in Electronics & Communication Engineering at Nova College of Engg & Tech JangaReddy Gudem, West Godavari. His area of interest includes Embedd systems and Wireless Communication.

Y.N.V.L. Ayyappa pursuing M. Tech in Electronics & Communication Engineering at Nova College of Engg & Tech JangaReddy Gudem, West Godavari. His areas of interest include Embedd Systems and Wireless Communication.

P. Naga Raju, Asst. Prof. Electronics & Communication Engineering at Nova College of Engg & Tech JangaReddy Gudem, West Godavari. His area of interest includes Embedd Systems and Wireless Communication.

Vundavalli Ravindra, with the Electronics & Communication Engineering Klce Kunchinapalli, Guntur.