A Trivial Denial of Service Attack on IEEE 802.11 Direct Sequence Spread Spectrum Wireless LANs

Chris Wullems, Kevin Tham, Jason Smith and Mark Looi
Information Security Research Centre
Queensland University of Technology
Brisbane, Australia
{c.wullems, wk.tham, j4.smith, m.looi}@qut.edu.au

Abstract

This paper describes a trivial, but highly effective denial of service attack based on commonly available IEEE 802.11 hardware and freely available software. The attack requires limited resources and is inexpensive to mount. This paper will discuss the attack, its implementation, and provide an analysis of methods to achieve optimal denial of service results. While there is currently no defense against this type of attack, the paper also discusses possibilities for attack mitigation.

1. Introduction

The IEEE 802.11 standards [1] specify the Medium Access Control (MAC) and Physical (PHY) layer requirements for Wireless Local Area Networking (WLAN). Acceptance of this standard has led to widespread adoption of WLAN technology as a supplement to, and in some cases a replacement for, wired networking infrastructure in the enterprise office environment. The success of the deployment of this technology in the enterprise environment has lead to a range of sectors that traditionally use proprietary radio technology, to consider how the affordable IEEE 802.11 based devices might be applied to their communications needs.

1.1. Emerging IEEE 802.11 Applications

The specification by the IEEE of the 802.11 wireless LAN standards has led to the emergence of a wide range of affordable, and to a large extent interoperable, technology becoming available for wireless communications. The availability of affordable wireless communications technology has not evaded the attention of a number of sectors that have traditionally relied on expensive, proprietary radio technologies to meet their communications needs. Such sectors include transportation, process control, and telecommunications.

For example Alcatel, a large provider of control technologies to the transport sector, is including 802.11 based radios in their technology strategy [2] and is reportedly using COTS based IEEE 802.11 radios for trains in Las Vegas, Hong Kong, and Korea[1]. There also appears to be interest in the industrial networking arena for using commodity 802.11 data radios in a range of applications[2]; consideration of WLAN technology for use by the military[3]; public safety; and the interworking of WLAN and 3G systems[4].

This emerging interest in adopting IEEE 802.11 technology for environments that have stringent performance and security requirements, especially in safety-critical control environments, is very concerning in lieu of the ease with which such communications can be disrupted, as described in Section 4. While attacks on the confidentiality and integrity of WLAN communications can be expected to be resolved in current and future enhancements to the standards - attacks on availability as described in this paper may not be so easily solved.

The structure of the paper is as follows. First existing confidentiality, integrity, and availability attacks against IEEE 802.11 based WLANs are summarized in Section 2. Aspects of the MAC and PHY layer protocols relevant to the newly described attack are reviewed in Section 3 and the new attack is described in Section 4. The new attack is analyzed in Section 5 and possible solutions to existing and this new attack are discussed in Section 6. Conclusions are presented in Section 7.

[1] See `http://www.tsd.org/cbtc/projects/`
[2] See `http://ethernet.industrial-networking.com/wireless.htm`
[3] See Joint Tactical Radio System `http://jitc.fhu.disa.mil/jtrs/`
[4] See IEEE Communications, Volume: 41, Issue: 11, Nov. 2003 for articles on the integration of wireless LAN and 3G wireless.

0-7803-8246-3/04/$17.00 © 2004 IEEE.

2. Existing Attacks against IEEE 802.11

Since becoming standardized and in subsequent years, a number of attacks, both theoretical and practical have been described against IEEE 802.11 networks. The attacks either focus on the confidentiality and integrity of wireless communications, or the availability of the wireless networking infrastructure.

Significant attacks against the security services provided by the Wired Equivalent Privacy (WEP) protocols are well documented [3-5]. A range of availability attacks, mainly directed at the management and MAC protocols used by IEEE 802.11 WLANs have also been identified [6, 7]. These attacks generally exploit the fact that many of the management messages in IEEE 802.11 are unauthenticated, rather they rely on correctly behaving MAC layer implementations. Some example attacks involve:

- Identity spoofing to permit deauthentication or disassociation of the victim node from the network (See Figure 1);
- Exploiting power saving features; and
- Exploiting media access protocols through such activities as modifying backoff timers, and keeping network allocation vectors (NAV) at non zero values.

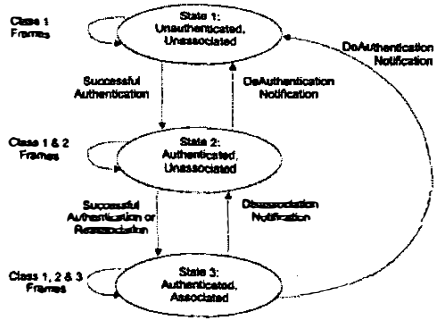

Figure 1. Authentication and association states [1]

While each of these attacks is significant to varying degrees, it is the opinion of the authors that there are likely to be solutions to these types of attacks through the judicious application of cryptographic techniques such as the authentication of messages[5].

3. Review of IEEE 802.11 Protocols

The IEEE 802.11 working group standards detail information about the physical layer (PHY) and Medium Access Control layer (MAC) protocols required for wireless local area networking (WLAN). The PHY layer is further divided into the Physical Layer Convergence Procedure (PLCP) sublayer[6] and the Physical Medium Dependent (PMD) sublayer as shown in Figure 2.

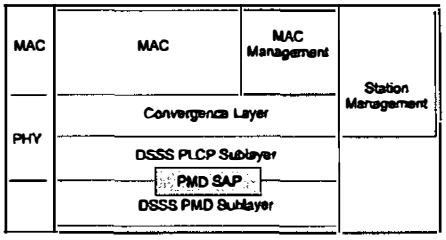

Figure 2. PHY / MAC layers [1]

The PHY layer provides the MAC layer with information about the availability of the underlying medium (carrier sense functions) and is involved with the reception and transmission of data.

To provide distributed, but coordinated access to the shared wireless medium, the IEEE 802.11 MAC protocols perform Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). This strategy minimizes the likelihood of two stations transmitting simultaneously, resulting in a collision and subsequent corruption of data, while ensuring that the available bandwidth is effectively utilized. Fundamental to the functioning of CSMA/CA in the IEEE 802.11 MAC protocols is the Clear Channel Assessment (CCA) procedure performed by the PHY layer.

3.1. Clear Channel Assessment

The Clear Channel Assessment (CCA) is used by the MAC layer to determine (1) if the channel is clear for transmitting data, and (2) for determining when there is incoming data.

[5] IEEE 802.11i will address the security issues associated with WEP, but will not currently address some of the availability attacks described.

[6] The use of this sublayer ensures that the MAC layer is not tightly coupled to a specific PMD

Evaluation of CCA is made by the PHY layer and the resulting assessment is communicated to the MAC layer via the *PHY-CCA.indicate* service primitive. This primitive can either be set to IDLE, when the channel is assessed to be clear, or BUSY when the channel is assessed to be in use[7].

The IEEE 802.11 series of standards define the following Clear Channel Assessment modes:

- **CCA Mode 1** Energy above threshold. CCA shall report a busy medium upon detection of any energy above the ED threshold.
- **CCA Mode 2** Carrier sense only. CCA shall report a busy medium only upon detection of a DSSS signal. This signal may be above or below the ED threshold.
- **CCA Mode 3** Carrier sense with energy above threshold. CCA shall report a busy medium upon detection of a DSSS signal with energy above the ED threshold.
- **CCA Mode 4** Carrier sense with timer. CCA shall start a timer whose duration is 3.65ms and report a busy medium only upon the detection of a high rate PHY signal. CCA shall report IDLE medium after the timer expires and no high rate PHY signal is detected. The 3.65ms timeout is the longest duration possible for a 5.5Mbit/s PSDU.
- **CCA Mode 5** A combination of carrier sense and energy above threshold. CCA shall report busy at least while a high rate PPDU with energy above the ED threshold is being received at the antenna.

3.2. Medium Access Control

The IEEE 802.11 standards specify both a centralized and distributed coordination function for controlling access to the shared transmission medium in WLANs operating in infrastructure mode (BSS /ESS). These are known as the Point Coordination Function (PCF) and the Distributed Coordination Function (DCF) respectively. The DCF is also used to permit the ordered sharing of network resources in ad hoc, or IBSS based WLANs.

The PCF is centrally controlled and operates by a master (the access point) polling slaves (the stations) for any data they may have to transmit. This permits contention free access to the transmission medium and operates in a speak only when spoken to paradigm. The PCF mode of operation is not widely deployed, so is not discussed further in this paper.

The DCF as its name suggests provides distributed, but coordinated access to the shared medium. In coordinating access to shared medium there are two goals: (1) permit stations to conunence transmission with minimal delay; and (2) prevent two or more stations from transmitting simultaneously to avoid collisions and data corruption. In order to meet these goals the 802.11 standard specifies a *listen before talking* paradigm for communications medium access, such that a station can only transmit while no other station is transmitting. This achieved by having the station perform a carrier sense operation, in the form of a clear channel assessment (CCA) prior to transmitting any data. To minimize the likelihood of two stations sensing the medium idle simultaneously, the medium must be idle for a period of time known as an inter frame space (IFS)[8] before transmission. Once the medium has been idle for at least the appropriate IFS time, a random backoff procedure is performed - further reducing the likelihood of two stations transmitting simultaneously (See Figure 3). The random backoff time is calculated as a function of the number of unsuccessful attempts to transmit an MPDU, such that as the offered load to the network increases, the larger the range of possible backoff time values becomes.

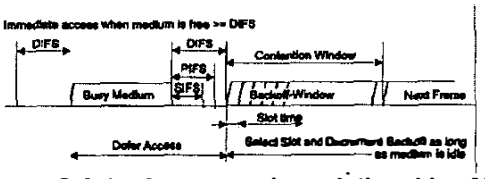

Figure 3. Inter frame spacing relationships [1]

An additional IFS value is used by the DCF when frame transmission errors are detected. This value is known as the Extended IFS (EIFS) and it is the longest IFS value of all.

3.3. Summary

The important points to note from this section, are that the CCA is used by the MAC layer to determine if the transmission medium is available for data transmission. Whenever the MAC layer receives a

[7] The specific details of how this is achieved differ with each physical layer, but the process involves the detection of energy beyond some threshold (PMD_ED.indicate), or the acquiring of a valid code lock (PMD_CS.indicate)

[8] These values are PHY specific and the use of different IFS values allows simplistic prioritization of traffic to be performed.

PHY-CCA.indicate(IDLE) it will wait for an IFS plus a random backoff time prior to transmitting. When the MAC layer receives a PHY-CCA.indicate(BUSY) service primitive from the PLCP layer it will defer from accessing the medium. The PHY layer uses energy detection, code detection, or some combination of the two to determine if the medium is busy and sets PHY-CCA.indicate accordingly.

4. A New Attack on IEEE 802.11

Here we propose a new attack on the IEEE 802.11 WLAN protocols. The attack described permits a low powered, portable device such as a Compaq IPAQ, using a commonly available wireless networking card to significantly disrupt wireless network communications over a significant range, for a significant period of time, in a manner that makes the identification and localization of the attacking node non-trivial.

The attack exploits the Clear Channel Assessment (CCA) procedure used by all standards compliant hardware and causes all stations within range, both clients and access points, to permanently defer transmission of data. This is achieved by stimulating the CCA in a manner that the channel is always assessed to be busy, thus preventing the transmission of any data over the wireless network.

Significant concerns are raised by this attack for a number of reasons, including:

- Attack can be mounted using standard hardware and commonly used drivers;
- Attack consumes limited resources on the attacking node, so is inexpensive to mount;
- Vulnerability being exploited will not be mitigated by emerging MAC layer security enhancements i.e. IEEE 802.11 TGi; and
- There is currently no defense against this type of attack for DSSS based[9] WLANs.

4.1. Attack Description

To facilitate correct MAC operation, the IEEE 802.11 standard mandates that a Station Management Entity (SME) will be present and able to interrogate layer specific status and control layer specific parameters. The two layers controlled via the SME are the MAC Layer Management Entity (MLME) and the PHY Layer Management Entity (PLME). Interactions among the management entities are depicted in Figure 4.

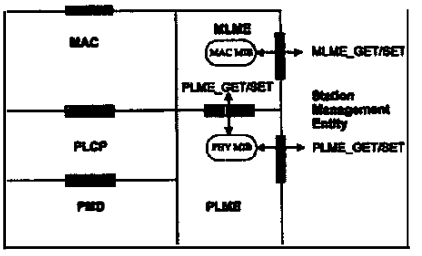

Figure 4. Station Management Entities (SME) [1]

The attack described here takes advantage of an optional PLME service primitive[10] that places the network card in a test mode of operation capable of continuously transmitting a specified bit pattern on a given channel.

Once the attacking node begins transmitting this pattern, all stations within range of the transmission, including AP's, will receive a PHY-CCA.indicate(BUSY) assessment of the channel state until the attacking node is disabled. This results in clients of the network perceiving the AP as out of range. The effect of the attack, as observed in our experimentation is almost instantaneous.

The following subsections details the affects of the attack on PLCP receive and transmit procedures based on preliminary experimentation.

4.2. Affects of attack on the PLCP receive procedure

The affect of an attack against PLCP receive procedures is relevant where the attacking station is within range of a station, but out of range of the access point the station is associated with. In this case, beacons are successfully transmitted from the access point allowing stations to be associated and synchronized. The PLCP receive procedure is affected as follows for stations within range of an attacking node.

1. **The PLCP frame is transmitted by the attacking node while the media is idle.** In this case, the CCA algorithm detects the carrier and the sync pattern is successfully detected (Figure 6). The PLCP frame sent by an attacking node is received, but fails the CRC check. Observations made during preliminary testing

[9] These are the high rate WLANs.

[10] PLME-DSSSTESTMODE.request

confirmed that PLCP frames received contained CRC errors. As the PLCP CRC test fails, CRC FAIL is returned and the state machine returns to RX_IDLE state as illustrated in Figure 6.

2. **The PLCP frame is transmitted by the attacking node while a beacon frame or a frame from another station is being transmitted.** The result of this is a collision, such that the sync pattern cannot be detected. The result is a loop where the CCA detects a carrier, sync pattern detection fails, resulting in a return to the state of RX_IDLE. Inevitably all beacon frames successfully transmitted will collide with frames transmitted by the attacker, resulting in disassociation from an access point in the attacked channel.

Observations made during preliminary testing confirm that both conditions cause the station port status to change from "Connected to IBSS" to "Out of Range (ESS)".

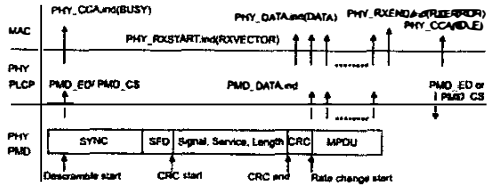

Figure 5. PLCP receive procedure [1]

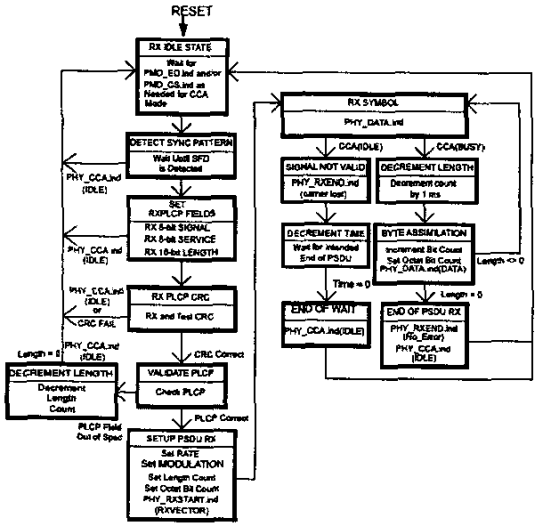

Figure 6. PLCP receive state machine [1]

4.3. Affects of attack against the PLCP transmit procedure

When using the DCF to coordinate data transmissions in either infrastructure (BSS) or ad hoc (IBSS) mode the following transmit procedure is followed by the PLCP layer (See Figure 7).

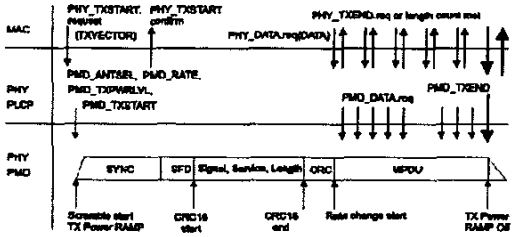

Figure 7. PLCP transmit procedure [1]

Prior to any transmission the PHY-CCA.indicate(IDLE) must be received by the MAC layer and appropriate IFS times must have elapsed. Once the channel is assessed to be clear, transmission of the PPDU is initiated by the MAC layer issuing the PHY_TXSTART.request(TXVECTOR) primitive. The PLCP layer then sets PMD parameters such as the antennae to use, transmission rate and transmission power level. Transmission of the data is then commenced via the PMD_TXSTART.request primitive. Transmission terminates when data transfer has completed, or the MAC layer issues a PHY-TXEND.request primitive.

The denial of service attack described in this paper effects the PLCP transmit procedure directly and indirectly in the following ways.

1. **The attack occurs whilst a station is transmitting a frame.** In this case the transmission was initiated successfully, but part of the transmission is corrupted due to the initiation of an attack. An acknowledgment for the transmitted frame will not be received resulting in retransmission and an increase of the contention window[11].

   Acknowledgment failure or the receipt of PHY-RXEND.indication errors will result in the deferral of transmissions for a period greater or equal to EIFS. The EIFS is used to resynchronize the station to the actual medium

[11] Backoff time is based on a random value between the minimum and maximum values ofthe contention window.

state, such that reception of an error-free frame during EIFS, results in the resumption of normal medium access procedures using the DIFS and backoff timers. Because an error-free frame is unlikely to be received, the station could remain in this state for the duration of the attack.

In the event the station is able to resynchronize, subsequent retransmissions are not able to occur, as it is unlikely the station will receive a CCA.indicate(IDLE).

2. **The attack occurs whilst the station is idle.** The continuous transmission of data onto the shared media, by the attacking node, dramatically reduces the likelihood that any station will receive a CCA.indicate(IDLE) that is a prerequisite for any PLCP transmission to commence.

   As the media is sensed as busy during a backoff slot, the backoff procedure is suspended and the media must be sensed as idle for a period of time equal to the appropriate IFS[12].

   Even if a station was able to assess CCA.indicate(IDLE), any transmissions from a station are likely to collide with those of the attacker resulting in the MAC layer backoff procedures being activated.

The affect of the attack on PLCP transmission procedure is illustrated in Figure 8.

4.4. Attack Implementation

The attack was implemented on a laptop running Linux Fedora Core 1 and a Compaq iPAQ running Familiar Linux. Both implementations used the *linux-wlan-ng* [8] drivers and PRISM based wireless network interface cards.

The goal of the linux-wlan project is to develop a complete, standards based, wireless LAN system using the GNU/Linux operating system that provides a convenient interface to low level functionality of the PRISM based network cards. Low level configuration of the device is made possible via the user level application, *wlanctl-ng p2req_low_level* series of commands. These permit the manipulation of the management entities described in Section 4.1.

[12] DIFS if no errors have been detected, EIFS if errors have been detected.

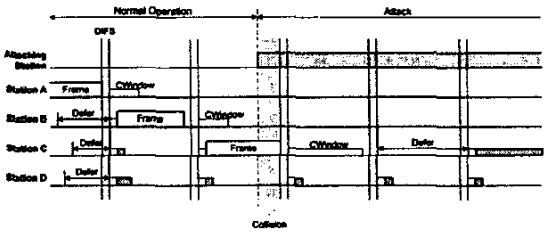

Figure 8. Backoff procedure during attack

5. Analysis

The following subsections detail the procedures used to create the attack, and how the attack was tested.

5.1. Accessing PLME-DSSSTESTMODE

As discussed in Section 4, the attack described in this paper depends on being able to access the test mode of operation via the PLME. Our testing revealed that this service primitive is implemented in a range of Prism2 based WLAN cards from Intersil and can be accessed programmatically via the wlan-ng drivers available for the Linux operating system. The network cards and drivers were tested on both desktop / laptop Intel PCs and a Compaq iPAQ 3750 running Familiar Linux.

5.2. Setting up the Attack

The following procedure is based on specific implementations of PHY sublayer functionality available through the wlan-ng driver for PRISM-based WLAN cards.

1. **Lock station to a given channel:** The station mode is set to WDS (specifies a repeater function in a wireless network), such that the channel is not changed back to an available channel it can associate to an AP.
2. **Set transmission channel:** PHY services are used to change the current channel to the specified channel for the attack.
3. **Launch Attack:** The station's continuous transmit test mode is activated, such that the station radio is put in a continuous transmission state. MPDUs containing a test data pattern are continually transmitted until the test is stopped.

Preliminary testing was conducted on a limited number of PRISM, Orinoco and Aironet-based WLAN cards. The tests were successful in both indoor and outdoor environments. In particular, attacks on infrastructure mode wireless LANs were highly effective, resulting in total denial of service for all wireless stations associated on the channel being attacked. The tests conducted made use of a PCMCIA wireless LAN card with a transmission power of 23mW. The attack range could be significantly improved through the increase of transmission power and high-gain antennas. The maximum transmission power, as licensed by the Australian Communications Authority, for DSSS on the ISM band (2.4Ghz) is limited at 4 Watts EIRP [9].

Experimentation confirmed that attacks performed near an access point significantly improve DOS results, as all associated stations are denied service. Attacks performed at long range from an access point are less successful at total denial of service, rather they are only successful at denying service to stations with range of the attacker. Ad hoc networks are more resilient to attack than infrastructure networks as they are only affected by attackers within range. An attacker is able to use open source tools such as "Airfart"[13] to locate access points to optimize the attack.

This tool and others such as "Ethereal"[14] are able to detect attackers and their approximate location. Experimentation indicated that the jamming attack disables these tools.

6. Solutions

The IEEE WLAN standards are dynamically evolving with new features and capabilities constantly under consideration. This section of the paper considers the impact that these evolving features and capabilities are likely to have on the existing attacks against WLAN's described in Section 2 and the new availability attack described in Section 4.

6.1. Existing Attacks

The attacks described in Section 2 result from poorly designed security protocols and the inability of stations to distinguish between authentic or forged management frames. Significant efforts have been undertaken by the IEEE 802.11 TGi to rectify the security issues that plagued WEP and they have specified a comprehensive security framework for providing significant security improvements to existing and future wireless LAN standards. The key management framework detailed by IEEE 802.11i can be used to ensure that management frames are authenticated and reduce the risk that the attacks described can be successfully mounted.

6.2. New Attack

Unfortunately, while the security efforts of IEEE 802.11i are capable of mitigating the security risks presented by existing attacks against 802.11 based WLANs, they will not have any impact on the new attack described in this paper. Primarily because the 802.11i solutions are applicable at the MAC layer and the attack described in this paper operates at the PHY (PMD and PLCP) layer.

It is worth noting that the attack described in this paper is dependent on the following: (1) access to an exposed low level interface capable of placing the attacking network card in DSSSTESTMODE; (2) the dependency of DSSSTESTMODE on the use of a DSSS PHY layer; and (3) the use of shared communications channel. The capability of mounting this attack using next generation WLAN cards based on the IEEE 802.11a specification is uncertain. Firstly, these cards operate with a different PHY layer, based on Orthogonal Frequency Division Multiplexing (OFDM) and there may not be access to a DSSSTESTMODE equivalent function in cards based on this standard.

While this paper has focused on the effect of the new attack on networks using contention based MAC protocols such as DCF, the contention free MAC protocols such as PCF will be vulnerable too as they depend on the same CCA procedure as DCF.[15]

A fundamental factor contributing to the effectiveness of this attack is the use of a shared communications channel. One strategy for making the attack more complex to mount would be to discard the shared communications paradigm in favor of dedicated communications channels based on dynamically negotiated spreading sequences. This would result in an attacker having to jam each channel independently or jam an entire frequency, increasing the power requirements to mount the attack and the risk of being detected and localized.

[13] See `http://airfart.sourceforge.net`

[14] See `http://www.ethereal.com`

[15] The PCF is not widely implemented, so extensive testing using this mode of operation has not been performed.

7. Conclusions and Future Work

This paper has presented a highly effective denial of service attack that can be mounted against IEEE 802.11 WLANs using a DSSS PHY layer. The attack is significant as it can be achieved using only commodity based hardware and software; has low power requirements; and can be executed with minimal chance of detection and localization.

A critical observation that can be made from this work is that the presence of engineering modes of operation, such as the DSSSTESTMODE interface exploited by this attack, in production hardware can present significant security concerns. These concerns are most pronounced in network environments that rely on the correct behavior of participating nodes for continued operation.

Future work will consider attack optimization strategies such as fine tuning the attacking node parameters, the use of external high gain antennae, and the use of increased power.[16] The ability of dynamically generated spreading sequences to increase resilience to the type of attack described in the paper will also be examined.

Until adequate strategies are in place to mitigate the significant threat of denial of service in current IEEE 802,11 DSSS WLAN technology, the application of this technology should be precluded from use in safety-critical environments which typically have stringent availability requirements.

8. Acronyms

AP	Access Point
BSS	Basic Service Set
CCA	Clear Channel Assessment
CFP	Contention Free Period
CSMA	Carrier Sense Multiple Access
CA	Collision Avoidance
DCF	Distributed Coordination Function
DIFS	DCF IFS
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended IFS
ESS	Extended Service Set
FHSS	Frequency Hopping Spread Spectrum
IBSS	Independent Basic Service Set
IFS	Inter Frame Space
MAC	Medium Access Control
MLME	MAC Layer Management Entity
PC	Point Coordinator
PCF	Point Coordination Function
PDU	Protocol Data Unit
PHY	Physical layer
PIFS	PCF IFS
PLCP	Physical Layer Convergence Procedure
PLME	PHY Layer Management Entity
PMD	Physical Media Dependent
PPDU	PLCP PDU
SIFS	Short IFS
STA	Station
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy

[16] ACA permits transmission at up to 4 Watts EIRP.

9. References

[1] IEEE-SA Standards Board, "IEEE Std 802.11-1999 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 1999.

[2] F. Whitwam, "Integration of Wireless Network Technology with Signaling in the Rail Transit Industry," *Alcatel Telecommunications Review*, pp. 1-7, 2003.

[3] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," presented at The Seventh Annual International Conference on Mobile Computing and Networking (MOBICOM-01), New York, 2001.

[4] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," presented at 8th Annual Workshop on Selected Areas in Cryptography, Toronto, Canada, 2001.

[5] A. Stubblefield, J. Ioannidis, and A. D. Rubin, "Using the Fluhrer, Mantin, and Shamir attack to break WEP," presented at The Symposium on Network and Distributed Systems Security (NDSS 2002), San Diego, CA, 2002.

[6] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," presented at 11th USENIX Security Symposium, 2003.

[7] D. B. Faria and D. R. Cheriton, "DoS and authentication in wireless public access networks," presented at The ACM Workshop on Wireless Security (WiSe-02), New York, 2002.

[8] Absolute Value Systems, "linux-wlan-ng," vol. 2003, 2003.

[9] Australian Communications Authority, "Radiocommunications (spread spectrum devices) class licence 2002," Australian Communications Authority, 2002.