

Technical White Paper

## **Susceptibility of wireless devices to denial of service attacks**

By Peter Egli, Product Manager Wireless & Networking Technologies

Netmodule AG  
Meriedweg 11  
CH-3172 Niederwangen  
[www.netmodule.com](http://www.netmodule.com)  
[peter.egli@netmodule.com](mailto:peter.egli@netmodule.com)

## Contents:

<b>Introduction</b> .....	<b>3</b>
<b>DoS in the security context</b> .....	<b>4</b>
Classification of DoS attacks .....	4
Physical layer attacks .....	4
Protocol or media level attacks .....	5
Inter-Network and transport level attacks.....	5
Application level attacks .....	5
Importance of DoS.....	5
<b>DoS attacks on WLAN (IEEE 802.11)</b> .....	<b>6</b>
802.11 media access protocol attacks .....	6
WLAN management frame attacks .....	6
WPA 802.1i attack .....	7
Flooding attacks .....	7
Something-of-death attack .....	7
<b>DoS attacks on ZigBee (IEEE 802.15.4)</b> .....	<b>7</b>
<b>Interference – the intentional and unintentional Denial of Service</b> .....	<b>8</b>
<b>Conclusion</b> .....	<b>9</b>
<b>References</b> .....	<b>9</b>

## Introduction

After years of technical debate and trials wireless technology is finally taking off. A wealth of new transmission and media access technologies vie for market supremacy and set out to enable a range of new applications and services. While WLAN (IEEE 802.11) has been a kind of trail-blazer for other technologies introducing radio technology at low cost other standards follow suit each trying to fill its niche of specific characteristics (throughput, range, power consumption).

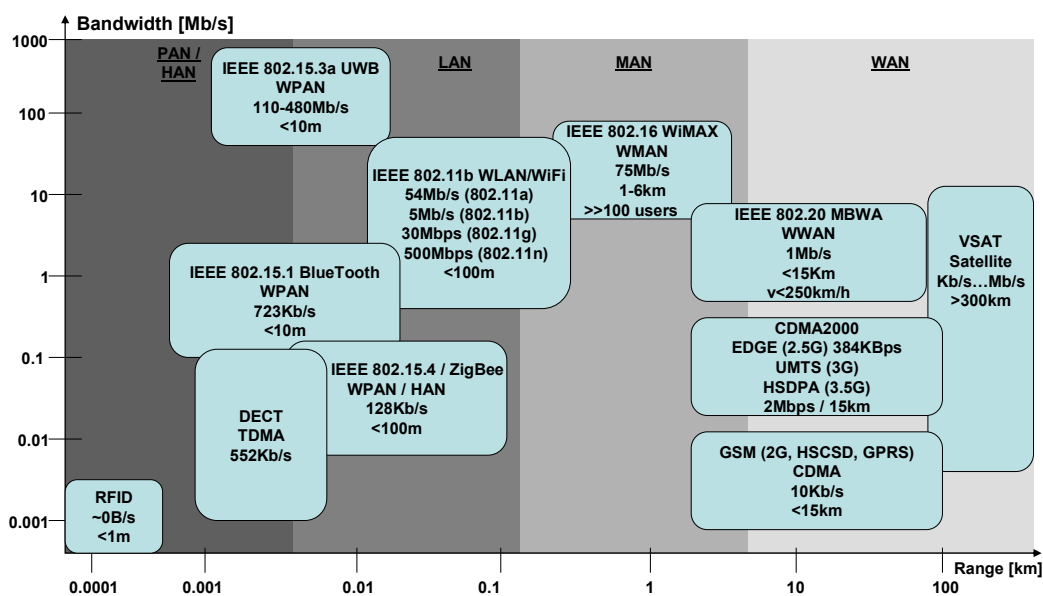


Figure 1: Wireless landscape

Wireless networks differ fundamentally from wired networks. Malicious packets can not be prevented from reaching an access point or client as opposed to wired networks where some filtering can be employed or access on a network port can be controlled (through use of 802.1X PBNAC for example). Conversely the reach of wireless networks is difficult to control thus allowing an intruder easy physical access. This means that strong security is an absolute must for wireless networks.

In recent years security has become a pivotal aspect of every new technology. But security is often reduced to the "usual" privacy, authentication, integrity and non-repudiation. DoS (Denial of Service) is acknowledged as being a threat but conventional wisdom is that it is difficult to counter such attacks with pure technical means. Unfortunately countermeasures to DoS are not deemed valuable features by marketing people and almost never find their way into data sheets.

The availability of low cost hardware, open source software and the publicly available frequency bands (ISM 2.4GHz, 5.1GHz UNII band) have made it comparably easy to craft a device for launching a DoS attack on networks operating in the ISM band. IEEE 802.11 WLAN networks are appealing targets since they provide medium range connectivity (~100m), that is make it relatively easy for an attacker to go undetected, use license free bands (everybody can send traffic provided it is under the allowed maximum transmission power) and their technology readily available at low cost.

ZigBee (IEEE 802.15.4) is another candidate that could arouse the malicious interest of hackers and crackers since it too is medium range (~70m), uses license free bands (ISM) and, if the hype turns into reality, will become a ubiquitous technology.

RFID (Radio Frequency IDs) tag applications are still in their infancy even though the technology has matured in recent years. However since the proper functioning of typical RFID applications is usually critical for companies employing this technology we do not see widespread deployment yet (such as in supermarkets). It is foreseeable that these tags will first be used in controlled environments for applications like goods tracking (parcel service) as a replacement for bar code labels. Only when security issues, most notably possible DoS attacks, are solved will this technology make its way into everyday usage.

Bluetooth is only short range and thus not really interesting for attackers. Additionally Bluetooth's use has so far been restricted to personal communication applications (wireless headset, message exchange between handheld devices through Bluetooth) what makes it not really a rewarding target for DoS attacks. However this could change as Bluetooth finds widespread use in the automotive sector (on-board wireless networks for hooking up handheld devices to the car's entertainment and information system). Unless Bluetooth remains restricted to non-critical applications it could too become a target for DoS attacks.

This paper presents a selection of DoS attacks on WLAN and ZigBee, discusses the implications and possible countermeasures.

## DoS in the security context

### Classification of DoS attacks

The field of network security can be roughly organised into the functions confidentiality (protection against eavesdropping), authentication (protection against spoofing), integrity (again protection against spoofing, replay attacks) and non-repudiation (protection against denial of involvement). All these functions are well studied and understood and a range of protocols and technologies are available to implement these functions. When it comes to DoS things look differently. Even though DoS is commonly acknowledged as a security threat surprisingly little is done to actively implement countermeasures.

DoS attacks can be roughly classified according to the OSI layering model:

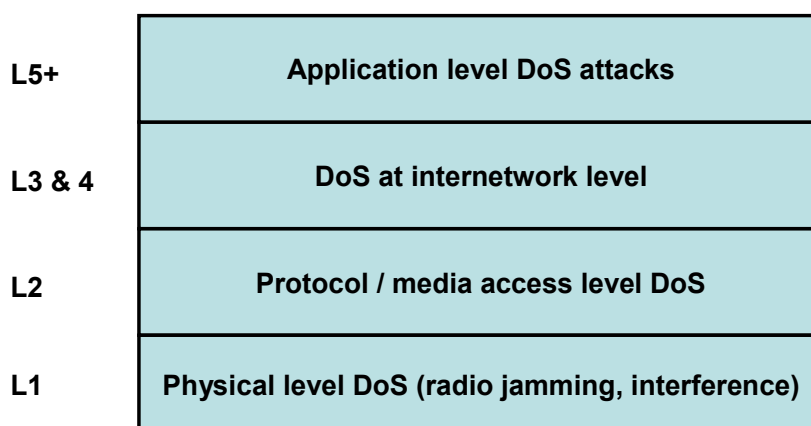


Figure 2: DoS classification

### Physical layer attacks

When thinking about DoS attacks on wireless networks physical layer attacks probably receive most attention. It is obvious that jamming a wireless network with noise signals may reduce the throughput of the network to unacceptable levels. Interference with other radio transmitters, wantonly or inadvertently, is another possibility to thrash the performance of a wireless network.

Physical layer security threats (jamming, interference) are deemed very difficult to counter. In fact there is little to do against physical layer attacks apart from electromagnetic shielding of buildings and use of homing tools to pinpoint and identify the culprit and, if possible, take it out (provided it is on one's own premises). Fortunately physical layer attacks are also difficult to execute since the power of a signal loses 6dB when doubling the distance between sender and receiver. This means that the signal quickly drops to low levels with growing distance and in turn means that for being a real threat the attacker must be close to the target or use excessive levels of transmission power.

## Protocol or media level attacks

As opposed to physical layer DoS attacks protocol layer attacks take place on layer 2 (media access layer) and are far more easy to mount. This kind of attacks exploits weaknesses of the wireless protocol and can not be countered by upgrading the affected devices with new software unless the protocol itself is modified to foil future attacks. Interestingly MAC layer DoS attacks receive too little attention by implementers, standard bodies and customers alike.

A variant of this kind of attack is the brute-force hogging of radio capacity thus rendering the wireless network virtually inaccessible to legitimate clients.

Wireless networks are particularly vulnerable to MAC level attacks since they use a shared medium and thus an attacker quickly gains information on all network participants.

Similar to physical layer attacks there is little a network administrator can do against protocol exploits. Administrators have to resort to monitoring / logging of suspicious activity and try to isolate the attacking device and take it out of service.

## Inter-Network and transport level attacks

At this level the distinction between wired and wireless networks vanishes and wireless networks can take advantage of the availability of a wide range of solutions against such attacks.

Possible attacks are ping-of-death (specially crafted ping packet that aims at crashing the receiving device), land attack (TCP SYN segment with source IP forged to destination IP thus causing an ACK war at the receiver), smurf (ping packet flood) and TCP SYN flood (overwhelm receiver with SYN segments each allocating a new data structure for the new connection) to name a few. As this kind of attack is well-studied and understood there are also various solutions available such as packet filtering, hardened network stacks, intrusion detection, traffic shaping and access control lists (both on MAC and IP level).

Nevertheless vendors of wireless equipment should make sure that their equipment provides the means to protect itself and other legitimate network devices from malicious devices.

## Application level attacks

Here the attacker attempts to exploit a weakness of an application protocol like DNS (cache poisoning), HTTP (stack and buffer overflow) or otherwise sends malicious code in the form of a virus, worm or Trojan horse which then unfolds its detrimental effect on the affected device.

Like inter-network level attacks application level attacks have been around for a long time and correspondingly there are very effective means to protect a device against such attacks (hardened protocol stacks, authentication and firewalls).

## Importance of DoS

Naturally DoS issues are of paramount importance for mission critical applications like health care, aviation and automotive. As wireless technology starts to penetrate into more and more markets and applications it is evident that sooner or later DoS will become a huge issue. Legislative bodies in the U.S. have already started to address security issues in company networks (Sarbanes Oxley Act on Corporate Governance including IT, HIPAA for health care) whereas the EU is not that far yet but will probably follow suit with their own legislation.

If CIOs are to take security seriously they are well advised to address DoS issues proactively.

---

## DoS attacks on WLAN (IEEE 802.11)

---

As WLAN (802.11 protocol family) is well established a number of security attacks are known and published by the wireless community. Linux and other open source projects are a good choice for manufacturers of WLAN products to master the complexity of a typical access point. The availability of source code makes it also easy for wily attackers to craft their own WLAN device to mount an attack. Along with publicly available attacker tools (available in source and executable) attackers have all tools at hand to mount an attack. Open source projects such as “airjack” even allow injecting arbitrary frames into a wireless LAN network.

### 802.11 media access protocol attacks

As opposed to the physical layer attacks it is comparably easy to exploit vulnerabilities in the MAC protocol. The 802.11 MAC protocol is based on the premises of cooperation among all network participants. If only one participant does not heed the procedures set forth in the standard network availability and performance can degrade dramatically.

One of the most prominent DoS attack on the WLAN protocol is the vulnerability uncovered by the Queensland University of Technology and published by AusCERT<sup>1</sup>. This attack is based on a MAC protocol flaw in 802.11b where the CCA (Clear Channel Assessment) can be used to simulate a busy network to all WLAN clients. The newer 802.11g and 802.11n (MIMO) use different modulation schemes (OFDM) and are thus not affected by this flaw.

A very simple way to thrash the performance of the wireless medium is to constantly cause collisions by sending arbitrary data during the legitimate transmission of other clients; this leads to excessive retransmissions thus further exacerbating the problem. The collision periods need not be long; in fact a single bit error in the CRC32 protected data section suffices to corrupt a frame. However the longer the collision periods are the higher are the chances that there is indeed a collision at the receiver. At first blush this attack may exhibit the same symptoms as simple radio interference (which it actually is) so it is important for network administrators to constantly monitor the network and be able to correctly interpret the traffic patterns.

Since the wireless medium is a shared one by nature many procedures are necessary to arbitrate access among a multitude of contenders for the medium. Clients have to know as much as possible about forthcoming transmissions in order to hold back with their own transmissions to avoid collisions from the outset. For example the duration field in 802.11 frames is there to indicate to devices within range how long the current transmission will be in order to defer own media access by this amount of time. DoS attacks of course can take advantage of this procedure by injecting frames with unduly large duration values (without the need to actually send such large frames). Provided that they are properly implemented all devices within range will remain silent for that period. A possible countermeasure for devices is to ignore duration values that exceed a certain threshold (e.g. the time for transmitting 1500 bytes).

### WLAN management frame attacks

802.11 devices use management frames for the discovery, authentication and association of WLAN clients to an access point. Unfortunately several of these management frame types are not authenticated and thus amenable to DoS attacks. For example an attacker could send de-authentication frames with forged source MAC addresses to the access point thus rendering the client device inaccessible. Luckily there is a possible solution to that kind of attack by modifying access points such that they still allow traffic from and to a de-authenticated client for some time after de-authentication. Only when there is absolutely no traffic from or to the client is the de-authentication eventually effected. The “real” authentication is anyway a function that should be covered by IEEE 802.1X access control.

## WPA 802.11i attack

Even WPA and 802.11i which are aimed at securing a WLAN network may be used to launch an attack. As a protection measure the standard mandates that if a WLAN AP or station receives more than 1 message with an invalid MIC checksum the session is to be shut down for 1 minute and then a new session key has to be generated (which is meant to be a protection against security breaches). It is evident that this behavior can be misused to launch a DoS attack virtually disabling the wireless service by repeatedly sending messages with forged MIC checksums. Access points have to be modified such that they do not honor the 1 minute shut-down requirement in case of invalid MIC values.

## Flooding attacks

Flooding attacks attempt to bring down the network or critical components by overwhelming it with excessive traffic. In particular it is important that an AP (and to a lesser extent clients too) protect themselves against unduly high amounts of certain types of traffic. Access points should protect themselves by limiting the number of specific management frames per time unit in order not to fall prey to such attacks.

## Something-of-death attack

While protocols serve a specific purpose there is always the danger that bad implementations open yet another door for DoS attacks where a malicious attacker sends forged and mal-formed frames with the intention of crashing the AP under attack. Fitted with some programming knowledge it is not too difficult to guess places in a protocol where a naïve implementation might get into trouble or melt down altogether. While it is true that drivers and protocol stacks mature over time and are continuously hardened against such attacks, vendors and developers should take DoS attacks into account from the outset. Vendors should make sure that software stacks and frameworks are hardened against the publicly known attacks (e.g. EAP-of-death attack).

## DoS attacks on ZigBee (IEEE 802.15.4)

---

ZigBee has the potential to become the technology of choice for networks with large numbers of (wireless) nodes interconnected by star or mesh topologies. Bluetooth was once believed to achieve that goal but never lived up to its promise. In theory and if one believes the marketing gibberish we will soon be surrounded by ZigBee nodes for appliances and devices like lights, fridges, temperature sensors etc.

ZigBee also knows the concept of network association and disassociation whereby a ZigBee router learns of nearby end devices and adds these to its internal routing table. Even though the ZigBee standard devotes some 50 pages to security there is no mention of DoS and possible counter measures. Fortunately the standard allows applying security (encryption and authentication) to all ZigBee frames thus thwarting the kind of disassociation attack possible on WLAN networks.

ZigBee end devices (sensors, actuators and the like) often run on batteries and have a very low duty cycle (ratio of active radio time compared to the silent period). Running networks in beacon-mode with predefined wake-up intervals is essential for saving battery life but also opens the door for specific DoS attacks. An attacker could repeatedly jam the medium during both the contention access period (CAP) and the contention free period (CFP, dedicated time slots for devices for transmission). Repeated disturbance of transmission may get the device under attack into an endless loop trying to deliver its data ultimately leading to battery exhaustion or greatly reducing battery life. This kind of attack can be countered by monitoring the network with scanners and intrusion detection systems of the kind available for WLAN networks.

Alternatively the ZigBee end devices could be operated in non-beacon mode where the end device actively polls the network coordinator if there is data available (beaconless mode). End devices could still go deep sleep during inactivity periods and only occasionally wake up for data transfers thus saving battery capacity. Provided that the wake up occurs at irregular intervals attackers would find it more difficult to guess the point in time when data transfer takes place.

A possible strategy for ZigBee vendors is not to use ZigBee altogether but to base their products on the underlying IEEE 802.15.4 MAC standard and augment it with their own proprietary functionality. Statically programmed random wake-up intervals for end devices break the regularity and thus predictability of the waking up of devices and thus may help foil DoS attacks. Usage of the feature “wake-on-radio” available from certain chip vendors may also help to make it difficult for an attacker to guess the activity period on the network.

## Interference – the intentional and unintentional Denial of Service

The ISM frequency band at 2.4GHz becomes more and more crowded by wireless technologies (802.11b WLAN, 802.15.1 Bluetooth, 802.15.3a UWB, 802.15.4 ZigBee). This means that network availability can suffer when other wireless devices legitimately use the same frequencies at the same location.

As can be derived from the following table interference is a possible source of performance degradation. But with careful network planning it is possible to accommodate different technologies in the same area.

From \ To	802.11b WLAN	802.15.1 Bluetooth	802.15.4 ZigBee
802.11b WLAN	n/a	<ul style="list-style-type: none"> <li>Limited freq. overlap.</li> <li>Acceptable degradation.</li> </ul>	<ul style="list-style-type: none"> <li>Considerable interference → Needs careful channel planning.</li> </ul>
802.15.1 Bluetooth	<ul style="list-style-type: none"> <li>Graceful degradation as a function of distance between BT and WLAN.</li> <li>Overall interference at acceptable levels.</li> </ul>	n/a	<ul style="list-style-type: none"> <li>Only low SIR required (2dB) for low interference.</li> <li>BT is usually low range.</li> </ul>
802.15.4 ZigBee	<ul style="list-style-type: none"> <li>ED helps reduce collisions.</li> <li>Duty cycle typically low so little effect.</li> <li>ZigBee is low power.</li> </ul>	<ul style="list-style-type: none"> <li>ED helps reduce collisions.</li> <li>Duty cycle typically low so little effect.</li> <li>ZigBee is low power.</li> </ul>	n/a

Table 1: Interference of ISM radios <sup>2</sup>

Since 802.15.3a UWB is a wide-spectrum technology “smearing” the frequencies at very low transmission levels across several GHz (also in licensed frequency bands) it is pretty immune against interference from narrower band technologies like Bluetooth, WLAN and ZigBee. Conversely UWB does not interfere with these since the transmission levels are very low (a total of 0.5mW across the entire UWB spectrum).

Of particular concern is the interference of 802.11b on 802.15.4 networks. It is possible to run 802.15.4 and 802.11b side by side through assigning 802.15.4 channels such that they fit nicely between 802.11b channels. Even though there will still be some interference caused by inter-modulation frequencies 802.15.4 performance can be greatly improved in presence of 802.11b radios.

It is clear that this fact can be exploited by an attacker who intentionally runs an 802.11b access point in the vicinity of ZigBee nodes. In this case the network administrator would have to resort to electromagnetic shielding.

## Conclusion

---

DoS is a real threat for wireless technologies and could become a show-stopper in some critical applications. In future standards more attention must be paid to DoS issues. Security should be firmly defined in standards and as little as possible should be left to the interpretation of the developer in order to ensure interoperability and thus wide adoption. There are countermeasures, none of which are a panacea but all of which help minimise and mitigate the problem. While DoS will never be impossible the effort to mount an attack can be made a serious obstacle for an attacker.

Vendors must become more aware of the problem and implement counter-measures. Customers should urge vendors to implement or retrofit DoS mitigation functionality to their products. CIOs should make sure that they have a plan B in place so that in case of unavailability of the wireless network, either through attack or due a network failure, operations do not come to a shutdown. This can mean to have a wired network in place (part of the distribution system) that can be used as backup network.

Regular network audits to identify and eliminate trouble spots become a crucial activity of network operations. As is already the case today with regular hosts (virus scanning, software updates and the like) also wireless network components will have to undergo regular vulnerability tests and the ensuing update of software.

Whether or not and to what extent a DoS attack presents a problem is also a matter of judgment. Taking out an access point serving a guest WLAN zone may be a nuisance but does not pose a serious problem. On the other hand attacks on mission critical systems may pose a real economic risk and put machine or even personnel at risk. Think of a goods tracking system that becomes unavailable and thus may wreak havoc on the operations of a company. If risk mitigation is critical to the application the portions of the network where wireless technologies are employed should be reduced to the minimum possible or hooked up with wired access only.

Electromagnetic shielding may be advisable for tightening the security and increasing the inaccessibility of wireless networks in mission critical environments such as industrial plants and health care.

If interoperability with other vendors is not required proprietary solutions (Phy and MAC level) may be entertained thus making it difficult for an attacker to exploit the protocol since it is unknown to the public ("security by obscurity"). Most rewarding in terms of DoS protection would be the usage of different and varying frequencies, possibly based on a frequency hopping scheme with random frequency changes (of course synchronized between sender and receiver). However such solutions are definitely more expensive since vendors can not take advantage of economy of scale effects with standard radio ICs. Additionally proprietary solutions run the risk of re-inventing the wheel and also introducing the same flaws and deficiencies as standard protocols.

## References

---

- 1 <http://www.auscert.org.au/render.html?it=4091>
- 2 <http://www.eurescom.de/~pub-deliverables/P1100-series/P1118/D3/BLTandWLAN.html>
- 2 [http://www.stzedn.de/docu/stz\\_zigbee\\_coexistence.pdf](http://www.stzedn.de/docu/stz_zigbee_coexistence.pdf)