Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks

Kemal Bicakci a,1, Bulent Tavli b,⁎

a TOBB University of Economics and Technology, Electrical and Electronics Engineering Department, Sogutozu Caddesi No 43, 06560 Ankara, Turkey

b TOBB University of Economics and Technology, Computer Engineering Department, Sogutozu Caddesi No 43, 06560 Ankara, Turkey

ABSTRACT

IEEE 802.11 access points deployed in shopping malls, university campuses, crowded streets, airports, and many other locations provide ubiquitous Internet access to millions of stations. However, these hot spots are vulnerable to Denial-of-Service (DoS) attacks due to the broadcast nature of wireless communication. It does not require specialized hardware or particularly high level of experience to render 802.11 networks inoperable through DoS attacks. Standard off-the-shelf equipment is sufficient for a malicious station to disrupt the service between access points and stations. In this paper we present a systematic survey of DoS attacks, which exploits MAC and physical layer vulnerabilities of 802.11 networks. Available countermeasures against DoS attacks are discussed and compared. Future research directions and open issues are also discussed.

© 2008 Elsevier B.V. All rights reserved.

Contents

1. Introduction .............................................................. 932

2. 802.11 standard ............................................................ 932

2.1. Frame types ........................................................... 932

2.2. Contention resolution ...................................................... 932

2.3. Physical Layer Convergence Protocol (PLCP) ............................................ 933

2.4. Channels ............................................................ 933

2.5. Security ............................................................ 933

3. DoS in the physical layer of 802.11 ................................................... 934

3.1. Physical layer attacks ...................................................... 934

3.1.1. Resource Unlimited Attack (RUA). ............................................. 934

3.1.2. Preamble attack. ..................................................... 934

3.1.3. SFD attack ....................................................... 935

3.1.4. Reactive attack ..................................................... 935

3.1.5. HR (Hit and Run) attack ................................................. 935

3.1.6. Symbol attack ...................................................... 935

3.1.7. Monopolizing attack ................................................... 935

3.2. Physical layer countermeasures .................................................. 935

4. DoS in MAC layer ........................................................... 936

4.1. Attacks in MAC layer. ..................................................... 936

4.1.1. Selective MAC layer attacks ..................................................... 936

4.1.2. Complete MAC layer attacks .................................................. 936

4.2. Countermeasures in MAC layer. .................................................. 936

4.2.1. MAC address spoof detection .................................................. 936

4.2.2. Cryptographically protecting management and control frames . . . . . . .................................................. 936

⁎ Corresponding author. Tel.: +90 312 292 4074; fax: +90 312 292 4180.
E-mail addresses: bicakci@etu.edu.tr (K. Bicakci), btavli@etu.edu.tr (B. Tavli).

1 Tel.: +90 312 292 4262; fax: +90 312 292 4180.
1. Introduction

The convenience and low cost of 802.11 based wireless local area networks have led to widespread deployment worldwide. Increasingly, we are accessing the Internet wirelessly. It is well-known that due to the broadcast nature of the wireless access it is open to many malicious attacks and a series of security extensions to 802.11 have already been proposed. However, these extensions primarily deal with vulnerabilities related to unauthorized access and confidentiality breaches. As our dependence on wireless access increases, it is essential to consider also the issue of availability, another important security requirement.

Denial-of-Service (DoS) attacks are attacks against availability, attempting to prevent legitimate users from accessing the network. Note that DoS attacks are different from selfish behavior motivated by possible beneficial outcome. Due to broadcast nature of wireless networks, DoS attacks are easy to conduct particularly in the wireless domain. Besides, there are many 802.11 specific DoS vulnerabilities experimentally demonstrated in the literature in recent years. A generic DoS attack scenario in a representative 802.11 network is presented in Fig. 1.

To emphasize the importance of the problem, we aim to present a holistic view on the DoS attacks in 802.11 wireless networks in this paper. Our principal objective is two-fold:

1. Systematically survey, classify and compare DoS vulnerabilities in 802.11 networks. As the top–most classification, it is natural to group the vulnerabilities according to the network layer they belong to; however, some attacks crosscut across multiple layers.

2. Classify the countermeasures and evaluate their efficacy. Our classification distinguishes between practical solutions that can be deployed relatively easier and the potential solutions that require new extensions in the standard.

The rest of the paper is organized as follows. In Section 2, we briefly outline the key properties of 802.11 standard that are most relevant to DoS issues. In Section 3, we group and analyze the DoS vulnerabilities and countermeasures in the physical layer of 802.11 networks. In Section 4, we discuss MAC layer related DoS issues. In Section 5, we discuss some additional issues related to DoS attacks and countermeasures. In Section 6, we present a summary, give future research directions and draw conclusions.

2. 802.11 standard

In this section, we highlight parts of 802.11 standard which present malicious users with opportunities to breach secure, fair, and efficient protocol operation. In this paper we consider 802.11 infrastructure mode of operation, where a Basic Service Set (BSS) is orchestrated by the Access Point (AP).

2.1. Frame types

There are three frame (packet) types in 802.11 networks: management frames, control frames, and data frames. Each frame type has its subtypes, which are listed in Table 1. Management frames are mainly used for network management and admission control. Control frames are mainly used for access control, and data frames carry data. Certain
management frames are exploited the most in DoS attacks. Therefore, we will focus on management frames among these three frame types.

All APs transmit a beacon frame at fixed intervals. Clients listen for beacon packets to identify the access points within range. Alternatively, probe request frames are generated by stations actively searching for existing wireless networks. Stations are identified through their MAC addresses. Once an AP receives a probe request frame it responds back with a probe response frame, which is very similar to beacon frame and contains necessary information on the BSS. The only difference is that probe request frames are generated by stations actively searching for existing wireless networks. Stations are identified through their MAC addresses. Once an AP receives a probe request frame it responds back with a probe response frame, which is very similar to beacon frame and contains necessary information on the BSS. The only difference is that beacon contains Traffic Indication Map (TIM) showing which stations in the sleep mode for power saving have data frames waiting for them in the AP’s buffer. After discovering an existing BSS, a station should be authenticated by the AP to be able to get more privileges. Thus, authentication request and response frames are exchanged. Even when open system authentication is replaced with the shared key based WEP (Wired Equivalent Privacy) protocol; authentication achieved in this phase is rather weak and subsequently needs to be supplemented by further steps of 802.11i. A station can be authenticated by multiple APs; however, it should be associated by only one AP at a time. After the authentication, association request and response frames are exchanged to establish the association.

Deauthentication frames are the frames exchanged to return back to the initial unauthenticated-unassociated state. Deassociation frames are used to return to authenticated but unassociated state. The discussion is summarized in Fig. 2. Note that none of the management frames are cryptographically protected, thus, any station can send any such frame.

2.2. Contention resolution

802.11DCF (Distributed Coordination Function) is a CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance) based channel access mechanism. Normally stations are in the receive mode, however, triggered by the arrival of packets in the transmit queue, a station switches to transmit mode, selects a random backoff value bounded by the value of the station specific variable CW (Contention Window) and starts to sense the channel. CCA (Clear Channel Assessment) module is used to determine the channel status.

Once the CCA module declares the medium to be idle, the station waits for DIFS (Distributed Inter-Frame Space) amount of time, if the channel stays idle for DIFS duration, then the station (or the AP) decrements its backoff value for each time slot it senses the medium idle. Upon the expiration of the backoff counter the sender transmits a Request-To-Send (RTS) packet to capture the channel and to announce its intent to transmit to the receiver station. The receiver responds back with a Clear-To-Send (CTS) packet. Then the sender transmits the data frame and the receiver acknowledges the successful receipt of the data packet. The utilization of RTS/CTS frames is optional in 802.11 and data frames can be sent without the RTS/CTS prefix. In this exchange, both sender and receiver waits SIFS (Short Inter-Frame Space) amount of time to start a frame transmission. If transmission fails then the current value of the CW is doubled and sender tries to retransmit the packet by repeating the whole chain.

Each frame contains a duration field to indicate the duration in microseconds of the projected successful completion time of the ongoing handshake, which updates the NAV (Network Allocation Vector) on each neighbor station. Channel access is deferred until NAV expires. 802.11 channel access is illustrated in Fig. 3.

2.3. Physical Layer Convergence Protocol (PLCP)

802.11 MAC frames are encapsulated by the PLCP header. Each frame starts with a PLCP Preamble containing a SYNC field triggering the energy detection circuitry that differentiates noise and/or interference from a valid frame transmission, also used for symbol level receiver synchronization and an SFD (Start Frame delimiter) field to indicate the actual start of PLCP header. The PLPC header includes: SIGNAL, SERVICE, LENGTH, and CRC (Cyclic Redundancy Check — computed over the PLCP header) fields. The MAC frame includes a separate CRC computed over the MAC frame.

2.4. Channels

802.11 b/g uses 11 overlapping channels (only three of these channels are non-overlapping) in the 2.4 GHz ISM (Industrial, Scientific, and Medical) band in United States and Canada (there are 14 channels in Japan, 4 channels in France, 2 channels in Spain, and 13 channels in the rest of Europe).

2.5. Security

It is well-known that in wireless LANs, authenticating stations by their MAC addresses is not secure since it is easy for an attacker to learn authorized addresses and change his MAC address accordingly.

![Fig. 2. Change in the connection states upon receipt or transmission of different 802.11 management frames.](image-url)
Wired Equivalent Privacy (WEP), part of the 802.11 standard since initial ratification, provides shared key authentication. On June 2004, IEEE approved the 802.11i security standard\(^2\) that upgrades the former WEP specification, which has severe security weaknesses. Using a four-way handshake, 802.11i establishes mutual authentication and generates a fresh shared secret key to protect data frames in the subsequent communication session.

There are three parties involved in the 802.11i protocol. These are the supplicant (the station), the authenticator (AP) and the authentication server (e.g. RADIUS server). If a pre-shared key is not preconfigured or cached, the station and authentication server execute one of the mutual authentication protocols in the extensible authentication protocol (EAP) framework to generate the master session key (MSK) to be used in the four-way handshake. This protocol is usually chosen as EAP-Transport Layer Security (EAP-TLS) (successor of the well-known Secure Socket Layer (SSL) protocol). In EAP-TLS execution, AP serves as the relay and 8-bit packet identifiers are used to track requests and responses.

Four-way handshake is executed between the station and AP only after the master session key is transferred securely from authentication server to the AP. Both AP and the station first generate a secret key called the pairwise master key (PMK) from MSK and then confirm that the other party holds the same PMK with the handshaking. At the end, both parties derive a pairwise transient key (PTK) to be used in the following data session. PTK can also be generated from the pre-shared key if the station and AP are configured so. No data packet is allowed until the handshake is completed successfully. This discussion is summarized in Fig. 4. The analysis of 802.11i suggests that 802.11i is a well-designed protocol which addresses major security issues except availability. Detailed information can be found in [3].

3. DoS in the physical layer of 802.11

Physical layer DoS attacks are generally known as jamming\(^8\)–\(^10\). Jamming aims to prevent a station as well as an AP from successfully transmitting or receiving frames in the physical layer so that frames cannot be passed on to higher layers.

3.1. Physical layer attacks

Physical layer DoS attacks can be classified according to their targets (e.g., certain parts of the frame preamble or the complete frame), timings (e.g., continuous, periodic, random, or reactive), and energy budget (e.g., low or high). We present a classification of the physical layer DoS attacks based on these attributes.

3.1.1. Resource Unlimited Attack (RUA)

If the jammer has virtually unlimited sources (i.e., energy, power, and bandwidth) then it can maintain a high level of signal strength at any receiver continuously in a wide frequency range. In such jamming cases all wireless devices in the effective range and jamming bandwidth will be blocked off as long as the attack continues (examples of such jamming operations were reported at the second gulf war). However, it is possible to disrupt a receiver even if the jamming signal is much weaker than the signal strength of a legitimate frame transmission. Such attacks are described below.

3.1.2. Preamble attack

By continuously transmitting a SYNC pattern a jammer can effectively prevent a receiver station from synchronizing to any
other station's transmissions [8]. It has been shown that such a jammer can cause significant frame losses even when its received power is three orders of magnitude less than the power of a legitimate frame transmission. Furthermore, if the preamble attack is performed in a periodic on/off fashion, the automatic gain control (AGC) unit is shown to be deceived by the jammer, which causes frame losses due to bit errors.

3.1.3. SFD attack

An SFD pattern announces the actual start of the PLCP header. If the receiver sees the SFD pattern transmitted by the jammer before it sees the SFD pattern of the transmitter, it starts to process the incoming bits following the SFD pattern with wrong ordering, which results in CRC errors both at the PLCP header and the MAC frame (i.e., the PLCP fields such as LENGTH and CRC are assembled from wrong samples) [8].

3.1.4. Reactive attack

Continuous transmission drains the jammer's energy resources. An energy-efficient jamming technique is reactive jamming. In this kind of attack a jammer passively monitors the channel until it senses a frame transmission. Upon detection of an ongoing frame transmission the jammer starts to send interfering signals to corrupt the ongoing frame transmission [10]. Alternatively, when the jammer detects the start of an ongoing DCF handshake, it can create interference signal without the need to detect an ongoing transmission. Jamming opportunity is present at all the stages of a handshake.

3.1.5. HR (Hit and Run) attack

If the jammer station continuously transmits jamming signals, then its energy consumption will be high. Furthermore, detection of such a station will be easy. However, if jamming signals are turned on and off periodically or randomly, then both the energy consumption will be less and the identification of such a node will be harder [10].

3.1.6. Symbol attack

802.11 and 802.11b frames do not include any Forward Error Correction (FEC) schemes. Thus, creating an error in a single symbol will render the whole frame useless. Similar to the reactive attack, during an ongoing transmission a jammer transmits a strong signal for the duration of a single symbol [9] and can succeed in destroying the whole frame.

3.1.7. Monopolizing attack

The attacker can try to monopolize the wireless channel by sending a short frame in every SIFS period. However, number of frames that is needed for a full disruption is huge [5] (for the SIFS period of 20 μs 50,000 packets/s are needed).

Both SFD and preamble attacks are targeted primarily against the preamble bits, but they also affect the bits following the preamble. Furthermore, both SFD and preamble attacks can be performed using any timing strategy (i.e., reactively, periodically, continuously, and randomly). On the other hand reactive, HR, symbol, and monopolizing attacks can also be performed using the SYNC or SFD patterns. Hence, due to the intertwined characteristics of the aforementioned physical layer attacks further classification of these attacks is not meaningful.

3.2. Physical layer countermeasures

The first step in countering against a physical jamming attack is to detect whether there is an attack performed by a malicious entity or not. In this section we first describe the methods of detecting the existence of physical layer jamming and then present the methods for thwarting these attacks.

Low throughput, low packet delivery ratio (PDR) and high packet latency are indicators of a jamming attack. However, these indicators are also present, when the network is congested. Thus, better metrics should be used to detect a jamming attack and differentiate it from other network conditions. Two types of jamming detection approaches are proposed in [10]: Signal strength consistency and location consistency. In signal strength consistency approach, a station is suspected to be a victim of a jammer station, if the measured PDR is low and the measured average signal strength of incoming signals is high. Signal strength level is an indicator of a high quality channel. An unexpectedly high frame loss rate in such a channel is an indication of an active jammer station. Location consistency is conceptually similar to signal strength consistency. If the PDR of a data flow between a sender and a receiver is extraordinarily low despite the fact that these stations are physically close enough (it is possible to estimate the distance between 802.11 stations by using signal strength, up to a few meters certainty) then a jammer station is suspected to be present in the surrounding area.

If the existence of an active jammer is detected or suspected then the legitimate users in the network should take actions to counter the intended actions of the jammer station (or multiple jammer stations). In case the jammer station is equipped with a narrow band transmitter, rapid frequency hopping can be a highly effective method in combating the jammer’s actions. A single station’s jamming attacks are experimentally shown to be relatively ineffective against legitimate stations rapid frequency hopping action [8]. If the number of jammer stations increases then the effectiveness of rapid frequency hopping gracefully decreases until all the channels (11 overlapping channels in North America) are jammed by at least one jammer station. Since implementing rapid frequency hopping brings extra overhead proactive utilization of such prevention methods is not very efficient if there is no ongoing DoS attack detected.

There also exists a radical solution: mobile stations can seek spatial retreat to escape from the jammer station [10]. If there are multiple spatially dispersed APs around then a mobile station can move away to a position where it can associate with another AP provided that the jammer station’s power is not high enough to jam.
the new link. Multi-hop forwarding of frames to the base station is yet another solution.

If a legitimate station is detected to be under jamming and if the station’s corrupted frame receptions is dominated by MAC CRC errors rather than PLCP CRC errors, then the jammer can be under a symbol attack. Symbol attacks can be effectively combated by strong FEC (Forward Error Correction) coding [9]. However, strong FEC means increased overhead.

4. DoS in MAC layer

4.1. Attacks in MAC layer

802.11’s MAC protocol allows an attacker to selectively or completely disrupt the network access using relatively few packets and lower power consumption.

4.1.1. Selective MAC layer attacks

By “selective” we mean the attacker targets an individual station not the whole network. Note that these DoS attacks benefit from a central basic vulnerability, which is the easiness of MAC-address spoofing. Below, we first give a list of options for this type of DoS:

4.1.1.1. Deauthentication/deassociation attack. Cryptographic protection is not implemented yet for management frames in the 802.11 standard. Therefore, by listening to the traffic and learning the MAC addresses of the station and the AP, an attacker can forge a deauthentication or a deassociation frame and transmit it either to the station or to the AP to knock the station off the network. Deauthentication attacks are more efficient than deassociation attacks because they require more work for the station to return back to the associated state. If the attack is repeated persistently, the station is kept from accessing the network indefinitely [5].

4.1.1.2. Duration inflation attack. If the attacker is in the radio range of its target, it can continuously defer the target’s transmission by asserting a large duration field in its RTS, CTS or other frames. Note that in the 802.11 standard each neighbor station should update its NAV according to the frame duration field value but the specification is not implemented properly in most wireless devices [5].

4.1.1.3. Attacks against 802.11i. If the attacker causes the 802.11i protocol to fail at some point (e.g. by forging negotiated security suites), the legitimate station needs to exchange extra messages to recover back. If the recovery time is large enough and in the meantime it is possible to launch the attack again, then this is an effective DoS attack to the specified station. Furthermore, one can exhaust the memory of the station by sending a burst of forged first messages in the 802.11i 4-way handshake [3].

4.1.1.4. Attacks against sleeping nodes. In 802.11 stations can enter a sleeping mode to save power. In this mode, AP buffers the frames for the station and upon receipt of a polling message from the wakeden station; it sends the frames and erases them from the buffer. By spoofing station’s polling message, an attacker can cause the AP to discard the messages destined for the station. It is also possible to spoof AP’s TIM message to convince the station that there is no pending data for it. A DoS attack can also cause the station fall out of synchronization with the AP, wake up at wrong times and therefore loose packets [5].

4.1.2. Complete MAC layer attacks

The attacks we summarize above can be generalized to block the network access to all the stations served by an AP; however, there are more efficient resource-depletion attacks for complete disruption. The attacker can simply target the AP and exhaust its finite computation and/or memory resources so that it can no longer give service to any other station.

4.1.2.1. Probe request flood. The basic idea is to send a burst of probe requests having different source MAC addresses to induce a heavy workload on the AP so that it can not give service to legitimate stations [4].

4.1.2.2. Authentication or association request flood. Similarly, the attacker can waste the AP’s resources by sending a burst of authentication or association requests. It was shown that if WEP is enabled AP has to manage a heavier load and therefore can be blocked with less traffic [4]. It is surprising to see that contrary to the specification, many APs also respond to association requests in their initial states. If 802.11i is implemented, the attacker can also exhaust the space of the EAP packet identifier, which is only 8-bits long, by association request flooding [3].

4.2. Countermeasures in MAC layer

4.2.1. MAC address spoof detection

One (non-cryptographic) method to detect MAC address spoofing is based on the sequence number field, whose value is incremented by one for each non-fragmented frame. An attacker does not have the ability to alter the value of sequence number if he can not control the firmware functionality of his wireless card [15,18]. Through the analysis of the sequence number pattern of the captured wireless traffic, detection systems were shown to be capable of detecting MAC address spoofing to identify deauthentication/deassociation attacks [15]. Alternatively, identifying wireless stations by using physical layer attributes to detect MAC address spoofing is also possible, which is discussed in Section 4.4.

4.2.2. Cryptographically protecting management and control frames

To extend security to the management traffic, IEEE started to work on a proposal at the 802.11 Task Group ‘w’. While other working groups are trying to broaden the functionality of management frames to include sensitive data, 802.11w will secure some of the management frames in an amendment expected to be announced in late 2008. The new extension will be able to provide protection against some of the MAC layer DoS attacks (e.g. deauthentication attacks), but will not surely be a solution for all DoS attacks. The final specification is yet to be publicized; however, it is known that mitigating DoS attacks is not the actual goal of the working group [14].

The cryptographic solution can work against different types of attacks but especially public key cryptography is expensive and can easily be a DoS target itself. For the sake of not opening a new DoS hole, the efficiency of the new protocol has utmost importance. Similar to 802.11i, we expect 802.11w to be comprehensively reviewed in detail after it is announced.

Using cryptography only after a DoS attack is detected can be an alternative option worth exploring further. To extend cryptographic solutions to other management frames, we need to consider additional limitations. For instance, the extension is not straightforward to implement for probe request–response frames because keying material is not available before the frame exchange unless two parties share a long term secret key.

4.2.2.1. Protocol repair. After identifying the DoS attack related to forging the first message of the handshake in 802.11i, He and Mitchell took a prompt action and the repair they proposed to the standard was adopted by the 802.11 Task Group ‘i’ in their final deliberation [3]. Another issue regarding protocol repair is the exchange in 802.11i, which is performed in the authenticated-associated state. It was shown that eliminating the association request flooding is possible by employing 802.11i before the association [2]. However, this requires a
major change in the standard [3]; therefore, we can easily say that not
all protocol repairs can be a practical solution in the short term.

4.2.2.2. Cryptographic (client) puzzles. The basic idea of client
puzzles is as follows. When a server gets a request, it distributes a
puzzle to the client. Only after verifying that the puzzle is correctly
solved by a client, the server responds to its request. The difficulty
of the puzzle can increase when the server detects that it is under a DoS
attack and as the attack becomes more severe. The 802.11 standard
can be updated to include this safeguard; however, further investiga-
tion is required to see if an effective puzzle can be constructed for
wireless networks in the sense that the puzzle is easy to solve for
legitimate stations having moderate resources, but it is difficult
enough for blocking attackers conducting a flooding attack.

4.2.2.3. Other non-cryptographic solutions. While cryptographic
solutions are promising remedies to avoid some of the most effective
DoS attacks, they need an update in the 802.11 standard. The solutions
below are more specific to a single type of attack but do not require a
standard change.

4.2.2.3.1. Delaying the effects of requests. If the effect of a
deauthentication or a deassociation request is delayed for a couple
of seconds, that request can be securely discarded when a data packet
arrives afterwards. This solution opens a new DoS vulnerability for
roaming mobile stations, not a significant limitation from a practical
point of view [5].

4.2.2.3.2. Define a new interpretation of the duration field. The four
key frame types that contain duration values are ACK, Data, RTS and
CTS. Since fragmentation is almost never used in 802.11 networks,
duration fields of Data and ACK frames not followed by a fragment can
easily be ignored. For the RTS frame, similar to previous solution we
can delay the effect of the duration field and discard its effect if a
subsequent data packet is not seen. The biggest challenge is the CTS
frames for which the solution we use for RTS is not directly applicable
because of the hidden terminal problem. An imperfect solution is to
give isolated CTS packets for some portion of time [5].

4.2.2.3.3. Decreasing the retry limit. When a high retry limit for
unacknowledged frames (e.g. probe reply message) is set, flooding
attacks become more harmful. A solution is to change the retry limit
by a smaller value upon detection of a DoS attack, however it is
reported that this solution is difficult to be implemented above the
firmware level [4].

4.3. DoS attacks to 802.11 networks including MAC and higher layers

For the sake of completeness, in this section we briefly mention
DoS implications of the protocols working above the MAC layer in
802.11 networks.

Address Resolution Protocol (ARP) is a stateless protocol used to
determine the mapping between IP and MAC addresses. Since no
source authentication is present in ARP, an attacker can poison
another station’s ARP cache by sending a wrong ARP reply when they
are in the same broadcast domain. This problem has been reasonably
mitigated in wired networks; however, in the context of wireless
networks, we need to revisit the problem because broadcast domain is
enlarged by the presence of APs and includes both the wireless and
wired networks [1].

Other upper layer DoS attacks are also possible due to the
bandwidth limitations of wireless networks as compared to wired
networks. For instance, one can perform ICMP ping flooding or TCP
sync flooding from a wired network to deplete the wireless
bandwidth.

4.3.1. Countermeasures

The classical defense against these upper layer attacks are filtering
(for prevention) and intrusion detection systems (for detection).

4.3.1.1. Filtering. The risk of both ARP poisoning and flooding attacks
can be mitigated by implementing packet filters. A firewall between
the switch connecting APs and the wired network can filter the traffic
and prevent ARP attacks originated from the wired network.

4.3.1.2. Intrusion detection systems. Detection is the only defense
option when prevention is not possible. It is also needed to assure
that the prevention measures are really working [1]. Intrusion detecting
systems may be able to detect ARP poisoning attacks by detecting the
excessive number of unsolicited ARP replies as well as others that
exploit the deficiencies in the network protocols. However, detection
without reaction usually makes little sense. We will elaborate more on
this crucial issue in Section 4.4.

4.4. MAC layer countermeasures by using physical layer

Most DoS attacks are possible just because an attacker can
masquerade himself by using forged MAC addresses. Physical layer
properties like signal strength or transmitter characteristics can be
used to create rather reliable and hard to forge fingerprints of a station
for identification [11,12].

4.4.1. Identifying stations through signal characteristics

The position of a station can be identified with a level of ambiguity
(due to the inherent standard deviation of propagating RF signals
around a mean value) through RSSI (Receive Signal Strength
Indicator) measurements of its transmitted frames by multiple APs.
RSSI measurements of a certain station by each AP are combined into a
signalprint at a central entity. RSSI has certain properties enabling its
use as a reliable metric:

1. It is hard to spoof RSSI characteristics.
2. RSSI is strongly correlated with the physical location of a station.
3. A stationary station’s RSSI is relatively stationary.

It is reported that RSSI-based signalprints can be reliably used to
identify a station’s relative position and to physically discriminate
distinct nodes provided that the nodes are not in close proximity [11].

This has the potential to be used as two countermeasures:

1. To identify and drop the subset of the frames that originates from
the same station to avoid resource depletion attacks
2. To identify attacks by comparing the fingerprints of the conflicting
requests (authentication vs. deauthentication).

The specific utilization of station identification through signal
characteristics is presented in Table 3. Note that here the goal is not to
determine the physical location of the stations but to distinguish it
from others. This technique has the capability to give the correct
reaction of discarding the frames originated from the attacking
station only. Other detection methods based on traffic trace analysis
cannot react to the attack properly if the attacker uses forged MAC
addresses and any other identification mechanism is not in place. For
instance, while being very powerful against greedy behavior of
legitimate users cryptographically authenticated by the AP and
therefore cannot change their MAC addresses, DOMINO software [6]
if used alone cannot identify and penalize an attacker who is
interested in DoS only.

We think that location detection techniques proposed for wireless
networks that depend on other kinds of measurements (e.g. TDOA
time difference of arrival) [7]) can also be used against DoS attacks.
Alternatively, the RF fingerprint of the transmitter can be used for
identification. In [12] a complete system for identification of 802.11
stations based on RF signal characteristics are demonstrated. In 802.11
radios, the signal received at the antenna is referred to as RF signal
which is first demodulated to an IF (Intermediate Frequency) for
necessary signal processing at this frequency and then the IF signal is
demodulated to baseband for final processing. The system takes the IF
output of the incoming RF waveform, the IF signal is down-converted to baseband, signal startup time (a period of time between the signal rising from the noise floor and reaching its steady-state level) is determined and the signal samples following the startup are used as the feature vector (a set of characteristics sufficiently describing the particular measurement) for the signal.

4.4.2. Key generation from signal envelopes

Cryptography can be an effective solution against some of the most devastating DoS attacks. However, to employ cryptographic solutions there is another difficulty besides the need for updating the standard; establishing the shared secret key. EAP-TLS solves this problem using public-key cryptography but it is not reasonable to assume that stations hold a public key certificate in all wireless applications. Therefore, it is worth to explore alternative methods for computing a shared secret.

In wireless communication the signal envelope changes significantly with small variations in the propagation environment between the transmitter and the receiver. Nevertheless, for a limited time window (channel coherence time) a stationary transmitter/receiver pair experiences similar channel characteristics. The signal envelopes they receive from each other are shown to exhibit strongly correlated characteristics (e.g., deep valleys in the waveforms at similar locations). In [13] a key generation method based on mutual-information utilization is presented. A pair of stations (or the station and AP) exchange frames in a Time Division Duplex fashion. The waveforms received in both stations will have deep valleys approximately at the same positions. Each station creates a bit-string by comparing the signal amplitude with a commonly established threshold at each time slot — if the signal value is higher than the threshold the output bit is one. Generated bit strings will not be identical but will have discrepancies only in certain positions. The sender transmits a partial statistical description of its bit-string and the receiver corrects its bit-string according to this information. Since only the sender and receiver have enough mutual information on the bit-string the partial statistical description can be utilized efficiently — the computational complexity of reconstructing the bit-string by an adversary is not feasible. Hence, both the receiver and sender have a bit string, which can be used to create a common secret key.

Although, the physical layer countermeasures presented in this section are quite effective and do not require an update in the standard, they usually require significant hardware and firmware changes in standard 802.11 products.

5. Discussion

We summarize the DoS attack types and countermeasures in Tables 2 and 3, respectively. This section addresses some additional issues related to DoS attacks and countermeasures.

In one sense it is true to say that flooding attacks are the most harmful DoS problem today since they directly target limited computational and memory capabilities of APs and do require only commodity hardware and software. On the other hand, deauthentication/deassociation attacks are superior to flooding attacks at least in one aspect. While flooding attacks can be mitigated by more aggressive system management techniques (e.g., by decreasing the retry limit), deauthentication attacks can be successfully conducted even against a system having infinite resources.

Addressing the central vulnerability of MAC address spoofing, identifying stations through RSSI measurements is a practical and effective defense against both attacks mentioned above [11]. However this defense can not be used if there is only one AP serving all the wireless stations. In addition, RSSI measurements are not able to distinguish two physically close devices and are not capable of identifying stations using multiple antennas. These drawbacks can be mitigated by collecting not only RSSI values but also additional physical layer measurements (e.g. TDOA, RF signal samples, etc.). Sequence number-based MAC address spoof detection systems are also valuable until reverse-engineered “attack cards” allowing frames with arbitrary sequence numbers become commonplace [15].

Attacks 9 and 11 in Table 2 have limited applicability as far as DoS attacks are of concern. However selfish stations who only compete to access the channel with their neighbors can easily obtain an unfair share by several MAC layer misbehaviors which constitute a superset of these attacks [19].

If DoS attacks are a headache, then distributed DoS attacks (DDoS) can certainly be called a nightmare. A coordinated distributed DoS attack relying upon zombie stations that have been infected by malware can bring an AP to its knees easily by flooding. Most countermeasures are simply useless against DDoS hence stations should say no to zombie recruitment by all means. The effects of malware-driven ICMP ping flood and TCP SYN flood attacks in 802.11 networks were analyzed in a recent study and it was demonstrated that even a single infected station can have a dramatic impact on the performance [20].

It is clear that standardization of cryptographic countermeasures will improve the security of 802.11 networks against DoS attacks.

### Table 2

Summary of DoS attacks in 802.11 networks.

<table>
<thead>
<tr>
<th>No</th>
<th>Attack name</th>
<th>Easiness</th>
<th>Experimenterally demonstrated</th>
<th>Selectivity property</th>
<th>Countermeasures (Table 2 no)</th>
<th>Energy consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Resource Unlimited Attack</td>
<td>L</td>
<td>Y</td>
<td>N</td>
<td>–</td>
<td>High</td>
</tr>
<tr>
<td>A2</td>
<td>Preamble attack</td>
<td>M</td>
<td>Y</td>
<td>N</td>
<td>C1, C2, C3</td>
<td>High</td>
</tr>
<tr>
<td>A3</td>
<td>SF2 attack</td>
<td>M</td>
<td>Y</td>
<td>N</td>
<td>C1, C2, C3</td>
<td>High</td>
</tr>
<tr>
<td>A4</td>
<td>Reactive attack</td>
<td>M</td>
<td>Y</td>
<td>Y</td>
<td>C1, C2, C3</td>
<td>Medium</td>
</tr>
<tr>
<td>A5</td>
<td>HR attack</td>
<td>M</td>
<td>Y</td>
<td>N</td>
<td>C1, C2, C3</td>
<td>Low</td>
</tr>
<tr>
<td>A6</td>
<td>Symbol attack</td>
<td>L</td>
<td>N</td>
<td>N</td>
<td>C1, C2, C3, C4</td>
<td>Low</td>
</tr>
<tr>
<td>A7</td>
<td>Monopolizing attack</td>
<td>L</td>
<td>N</td>
<td>N</td>
<td>C1, C2, C3</td>
<td>High</td>
</tr>
<tr>
<td>A8</td>
<td>Deauthentication/deassociation</td>
<td>H</td>
<td>Y</td>
<td>Y</td>
<td>C5, C8, C10, C11, C14, C15</td>
<td>Low</td>
</tr>
<tr>
<td>A9</td>
<td>Duration inflation</td>
<td>M</td>
<td>N</td>
<td>Y</td>
<td>C5, C10, C11, C12</td>
<td>Low</td>
</tr>
<tr>
<td>A10</td>
<td>Attacks against 802.11i</td>
<td>M</td>
<td>N</td>
<td>Y</td>
<td>C5, C8, C10</td>
<td>Low</td>
</tr>
<tr>
<td>A11</td>
<td>Attacks against sleeping nodes</td>
<td>M</td>
<td>N</td>
<td>N</td>
<td>C5, C8, C10, C14, C15</td>
<td>Low</td>
</tr>
<tr>
<td>A12</td>
<td>Probe request flood</td>
<td>H</td>
<td>Y</td>
<td>N</td>
<td>C5, C7, C10, C13, C14, C15</td>
<td>Medium</td>
</tr>
<tr>
<td>A13</td>
<td>Authentication/association request flood</td>
<td>H</td>
<td>Y</td>
<td>N</td>
<td>C5, C6, C7, C10, C13, C14, C15</td>
<td>Medium</td>
</tr>
<tr>
<td>A14</td>
<td>ARP poisoning</td>
<td>H</td>
<td>Y</td>
<td>N</td>
<td>C5, C9, C10</td>
<td>Low</td>
</tr>
<tr>
<td>A15</td>
<td>ICMP ping flood</td>
<td>H</td>
<td>Y</td>
<td>N</td>
<td>C9, C10</td>
<td>Medium</td>
</tr>
</tbody>
</table>

**Easiness**
- High: Automated tools are available.
- Medium: With standard equipment (no automated tools).
- Low: Require extra hardware.

**Selectivity property**
- Y: Shown with physical experiments.
- N: Attack cannot target a specific station; all stations within range are affected.
- M: Simulation, analysis, or no proof-of-concept.

**Countermeasures**
- C1, C2, C3: Commercial solutions.
- C5, C7, C10: Commodities.
- C9, C10: Medium scale.
- C11, C12, C13, C14, C15: High scale.

**Energy consumption**
- High: Requires significant energy.
- Medium: Requires moderate energy.
- Low: Requires minimal energy.
### Table 3

<table>
<thead>
<tr>
<th>No.</th>
<th>Countermeasure name</th>
<th>Prevent/detect/</th>
<th>Attacks against</th>
<th>Shown with physical experiments</th>
<th>Effectiveness</th>
<th>Drawback</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Rapid frequency hopping</td>
<td>P+R</td>
<td>Physical layer</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Changes in the location are highly inconvenient. It may not be possible to change the location of the victim's AP. Jammer may be mobile too.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>Spatial retreat</td>
<td>R</td>
<td>Physical layer</td>
<td>Medium</td>
<td>Medium-Low</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Changes in the location are highly inconvenient. It may not be possible to change the location of the victim's AP. Jammer may be mobile too.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>Security protocol repair</td>
<td>P</td>
<td>Logical layer</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Identifying with signal strength information</td>
<td>D+R</td>
<td>Logical layer</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Jammer can create interfering signals, which might be used to deflect the intended signal.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td>Client Puzzle</td>
<td>R</td>
<td>Logical layer</td>
<td>Medium</td>
<td>Medium-Low</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Can't give effective reaction if MAC spoofing is done. False positives may result.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C5</td>
<td>Identifying through RF parameters</td>
<td>D</td>
<td>Logical layer</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Jammer can create interfering signals, which might be used to deflect the intended signal.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C6</td>
<td>Identifying through signal strength information</td>
<td>D+R</td>
<td>Logical layer</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Jammer can create interfering signals, which might be used to deflect the intended signal.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C7</td>
<td>MAC Address spoof detection</td>
<td>D+R</td>
<td>Logical layer</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Can't give effective reaction if MAC spoofing is done. False positives may result.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C8</td>
<td>Filtering</td>
<td>P</td>
<td>Physical layer</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Changes in the location are highly inconvenient. It may not be possible to change the location of the victim's AP. Jammer may be mobile too.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C9</td>
<td>Delaying the effects</td>
<td>P</td>
<td>Physical layer</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Changes in the location are highly inconvenient. It may not be possible to change the location of the victim's AP. Jammer may be mobile too.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C10</td>
<td>New interpretation of duration</td>
<td>P+R</td>
<td>Logical layer</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Changes in the location are highly inconvenient. It may not be possible to change the location of the victim's AP. Jammer may be mobile too.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C11</td>
<td>Decreasing the retry limit</td>
<td>R</td>
<td>Physical layer</td>
<td>Medium</td>
<td>Medium-Low</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Changes in the location are highly inconvenient. It may not be possible to change the location of the victim's AP. Jammer may be mobile too.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C12</td>
<td>Identifying with signal strength information</td>
<td>D+R</td>
<td>Logical layer</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Jammer can create interfering signals, which might be used to deflect the intended signal.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C13</td>
<td>Identifying through signal strength information</td>
<td>D+R</td>
<td>Logical layer</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Jammer can create interfering signals, which might be used to deflect the intended signal.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C14</td>
<td>Identifying through signal strength information</td>
<td>D+R</td>
<td>Logical layer</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Jammer can create interfering signals, which might be used to deflect the intended signal.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C15</td>
<td>Identifying through signal strength information</td>
<td>D+R</td>
<td>Logical layer</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Jammer can create interfering signals, which might be used to deflect the intended signal.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

However, network security has become an arms race and an attacker has to find only one DoS weakness to be successful. He can simply pass to the next item in his attack list after seeing that his current attack does not work for a new target. Besides, standardization efforts take time and not all legacy hardware will have sufficient CPU capacity to implement them as a software update [5]. This is why system-level defenses when applicable are recommended to victims seeking immediate solutions.

Items 5, 6 and 7 in Table 3 are not independent solutions and should be considered together in a future IEEE standard addressing DoS attacks. On this line of argument, since backward compatibility is a practical necessity for any network protocol, repairing a protocol efficiently without defecting compatibility is a real challenge for any new standardization effort. The need to protect servers running a cryptographic protocol with a client puzzle is well-understood and this combination has already been adopted by several developing Internet standards e.g. [16]. In the context of wireless networks hosting highly heterogeneous clients these previous standards should be carefully examined but it is evident that more research on client puzzles is needed before incorporating them into prospective wireless standards specifying cryptographic protection. Puzzles are one of the active research areas in wireless networking. Recently a new mechanism utilizing peculiarities of wireless environment instead of computational resources of stations was introduced [17]. The proposed puzzle questions the client for information regarding its neighbors in the close proximity. The client requires monitoring the channel to respond with a correct solution of such a puzzle.

Rapid frequency hopping is one of the few possibilities for combating against physical layer DoS attacks. IEEE 802.11b includes mechanisms for avoiding interference; however, the mechanism for channel hopping in IEEE 802.11b are coarse grained and therefore are not effective against a malicious user, who can create interference rapidly. Hence, to combat adversaries with rapid frequency hopping capabilities, fine grained frequency hopping should be incorporated into future IEEE 802.11 standards. Both the AP and the stations connected to it must use a channel hopping sequence known by the legitimate users. In [8] an MD5 hash chain to decide the next channel in the hopping sequence is used to increase the resistance against attackers. Such prevention methods should also be standardized in future IEEE 802.11 versions. Furthermore, increasing the number of channels (there are 11 non-orthogonal channels in IEEE 802.11b) will definitely increase the effectiveness of rapid channel hopping techniques.

Neither IEEE 802.11 nor IEEE 802.11b uses any error-correction scheme in the physical layer. Thus, it is easy to destroy any frame by causing a single bit error. Interleaving and Forward Error Correction techniques can significantly increase the resilience of physical layer frames. In future IEEE 802.11 standards stronger Forward Error Correction techniques should be used. Low Density Parity Check codes are shown to be a promising coding technique for binary modulation and long data frames [9]. However, if the communicating nodes are always using excessive error correction codes, then they will waste bandwidth. Thus, strong error correction codes should be used adaptively (i.e., whenever the existence of an ongoing jamming operation is detected the stations should switch to the strong error-correction mode).

Although there are several countermeasures against physical layer DoS attacks, implementing these methods incurs extra overhead and if there is no ongoing jamming operations then the system resources will be wasted. Hence, detecting the existence of any ongoing DoS attack has utmost importance for keeping the overhead of countering the possible attacks. Currently, none of the IEEE 802.11 standards include any mechanisms to identify the existence of ongoing DoS attacks. Thus, DoS detection is the very first step in DoS defense and mechanisms for DoS detection should be incorporated into future IEEE 802.11 standards (such as the mechanisms described in Section 3.2).
To increase the effectiveness of countering DoS attacks and complementing the previously proposed IEEE 802.11 standards for security enhancements we propose a security model which is shown in Fig. 5. This model is synthesized from the building blocks devised in separate research and development efforts to reflect the lessons learned on IEEE 802.11 DoS. In the model the central entity is the security extension central module, which orchestrates the security countermeasures against DoS attacks. Security extension central module is positioned in between the MAC and PHY layers. DoS detection module is the most important module for the efficient operation of the standard as a whole, which continuously monitors the data coming from other modules and decides whether an attack is in progress or not. Location and signal fingerprint modules are used for determination of the positions and signal fingerprints of neighboring nodes and the data coming from these modules are merged in a central entity called the fingerprint and location database. MAC address spoofing based attacks can be identified more robustly by using the data kept in this database (e.g., a MAC address, associated signal fingerprint vector and associated location information constitutes a robust identification for a station). Client puzzle and cryptographic protection module communicates with the central module to parameterize DoS countermeasures in the MAC layer. Rapid channel hopping and adaptive FEC modules are used as a countermeasure when an ongoing jamming operation is detected. The coordination necessary for the channel hopping of the stations and APs is provided by the channel hopping synchronization and distribution module.

6. Conclusions and open problems

In this paper, we investigate the issue of denial of service in 802.11 wireless networks which has received attention in the literature only in recent years. We discuss and compare the DoS vulnerabilities as well as available and potential countermeasures. Furthermore, we propose a security model to be used in prospective IEEE 802.11 standards for countering DoS attacks.

The most important research questions we identify for a more dependable wireless access are as follows:

- Which 802.11 frames should be cryptographically protected? Can we design efficient authentication protocols so that they will not be a DoS target themselves? Can we design effective cryptographic puzzles for wireless networks?
- At which level is it more appropriate to implement the countermeasures; at the hardware level, firmware level, or above firmware? For instance, if the source address field in 802.11 frames is protected to be modified, then it would be impossible for a malicious user to spoof MAC addresses. Although this would require major revisions in the networking hardware and firmware, the attackers cannot utilize any attacks based on MAC address spoofing.
- What kind of development tools should vendors provide to implement countermeasures above the firmware level? What kind of additional functionalities are needed for the networking equipment manufactured in order to combat DoS attacks more effectively?
- Which physical layer attributes are the best ones to be used for robust station identification? Which technique can achieve the smallest probability of false positives and false negatives?

We think today the most important DoS vulnerability is flooding attacks (authentication request or probe request floods) because these can be conducted with very little effort but can have a huge impact. In our research, we even encounter videos posted on the Internet showing how some of these DoS attacks work. We expect that carrying out a wireless DoS attack will be an easier task as more automated tools become available in public domain. As the first step towards establishing dependable Internet access through wireless technology, administrators should be aware of the great risk of ignoring DoS vulnerabilities and utilize the available short-term countermeasures immediately. In this regard, identifying and isolating the source of DoS attacks is a very promising defense but unfortunately there is a lack of user-friendly tools publicly available to network administrators.

Short-term countermeasures which require neither special equipment nor modification in the standard can provide only a partial solution. In the context of wireless local area networks, guaranteed immunity against DoS attacks can never be possible due to the openness of the channel to high-power jamming signals.

References


941

K. Bicakci is an Assistant Professor at the Department of Electrical and Electronics Engineering, TOBB (The Union of Chambers and Commodity Exchanges of Turkey) University of Economics and Technology. He has obtained his PhD degree from Middle East Technical University, Ankara, Turkey in 2003. Between 2004 and 2006, he was a postdoc researcher in Vrije Universiteit Amsterdam working with Prof. Tanenbaum in EU FP6 project named SecurE-Justice. His previous research experience includes several NSF funded security projects in which he participated as a research assistant during his MS studies in University of Southern California, Los Angeles, USA. His research interests include information security, applied cryptography, wireless and sensor networks and medical informatics.

Bulent Tavli is an Assistant Professor in the Department of Computer Engineering at the TOBB University of Economics and Technology, Ankara, Turkey. He received the B.S. degree in Electrical and Electronics Engineering in 1996 from the Middle East Technical University, Ankara, Turkey. He received the M.S. and Ph.D. degrees in Electrical and Computer Engineering in 2001 and 2005 from the University of Rochester, Rochester, NY, USA. His research interests lie in the area of telecommunications, networking, and signal processing.

