Security Vulnerabilities in Hybrid Flow-specific Traffic-adaptive Medium Access Control

T. Owens Walker III
Department of Electrical and Computer Engineering
United States Naval Academy
Annapolis, Maryland, USA
owalker@usna.edu

Murali Tummala and John McEachen
Department of Electrical and Computer Engineering
Naval Postgraduate School
Monterey, California, USA
{mtummala, mceachen}@nps.edu

Abstract

Wireless network security is a daunting challenge as researchers analyze the vulnerabilities of wireless medium access control schemes such as IEEE 802.11, Bluetooth, and IEEE 802.16. While these wireless protocols employ traditional contention and non-contention approaches, recent work has identified the delay and throughput performance advantages of a flow-specific medium access hybrid solution for wireless networks such as the traffic-adaptive Cooperative Wireless Sensor Medium Access Control (CWS-MAC) protocol. Accordingly, this paper addresses the security of wireless networks employing these hybrid, flow-specific schemes by analyzing the vulnerabilities in traffic-adaptive CWS-MAC, many of which are applicable to hybrid medium access schemes in general. Critical vulnerabilities are identified that expose the protocol to denial of service, energy exhaustion and “greedy” attacks. The effects of attacks exploiting these vulnerabilities are shown to include decreased throughput and increased delay in both the contention and non-contention modes as well as increased per node energy consumption.

1. Introduction

Within the last ten years, wireless networks have been employed in wide ranging applications including sensitive industrial control and inventory tracking [1], confidential medical monitoring [2], and covert military operations [3]. With the proliferation of these wireless networks comes a “proliferation of wireless threats” [4] and it has been well-established that security remains a daunting challenge [5].

Significant work has been done in investigating the security vulnerabilities in both established and proposed medium access protocols. While “systems level” security has been provided for the widely deployed IEEE 802.11 wireless networks in the form of the IEEE 802.11i standard [6], unique vulnerabilities such as the contention-mode back-off mechanism [7] and the Request-to-Send/Clear-to-Send handshake [8] continue to be the focus of researchers in an effort to “secure” the protocol. Similarly, newer technologies such as Bluetooth [9] and Mobile WiMax [4] have come under increased scrutiny. The security of wireless sensor networks have also been the focus of ongoing efforts [10],[11] including a detailed analysis of the S-MAC protocol and its vulnerabilities to denial of service attacks [12].

While these well-studied wireless medium access solutions employ traditional contention and non-contention approaches, recent work has identified the delay and throughput performance advantages of a flow-specific medium access solution for wireless networks [13]. A hybrid approach capable of concurrently providing different medium access service to different traffic flows and dynamically switching flows between medium access service types to respond to traffic variations, flow-specific medium access is able to achieve the delay performance of contention-based approaches at low demand and the throughput performance of scheduled approaches at high demand on a per flow basis. The traffic-adaptive Cooperative Wireless Sensor Medium Access Control (CWS-MAC) protocol [13] and its companion low-power energy-efficient version [14] have been shown to outperform contention, non-contention and hybrid medium access solutions [13].

Along the lines of the security work found in other wireless network solutions, the main contribution of this paper, then, is the identification and analysis of the security vulnerabilities that reside within this flow-specific medium access scheme.

This paper is organized as follows. In Section 2 we put this work in context by providing an overview...
of security concepts as they apply to the medium access layer. Section 3 provides background on the traffic-adaptive CWS-MAC protocol while we investigate vulnerabilities within the protocol in Section 4.

2. Security at the Medium Access Layer

The principles of information assurance can be used as a framework to understand security both at the MAC layer and across the entire network stack. These principles include [15] message related services such as confidentiality, integrity, authentication, and non-repudiation as well as entity authentication which seeks to limit access to network resources to a set of authorized entities. These principles can also help place the contribution of this work in context. Information assurance can be thought of as a “systems level view” of security. Many of the concepts of information assurance can be applied at multiple layers throughout the stack and are certainly not MAC layer specific. For example, while the IEEE 802.11i standard [6] addresses and implements confidentially, authentication, and the supporting key management functions, these can all be applied (and often are) at higher layers as well. In contrast, this work specifically addresses the vulnerabilities that are unique to the medium access control layer. We use the term vulnerabilities to indicate a legitimate mechanism within the scope of a protocol that could be used by an attacker to compromise the performance of the protocol. It should be noted that in this context, an attacker can be defined as any non-cooperative node to include a hostile node with the intent to degrade over all network performance or a “greedy” node that simply seeks to make use of an unfair proportion of the network resources.

The medium access layer is designed to “mediate access” thus most attacks at this layer can be seen as either denial of service (i.e., denial of availability) attacks or energy exhaustion attacks in which sleep mechanisms built into the protocol to conserve energy are inhibited. The latter can also be thought of as a type of denial of service where the attacker seeks to reduce the operating lifetime of the node. This can be seen in [10] which surveys a number of potential attacks on a wireless sensor network. Of these, the majority are related to routing functionality (including wormhole, black hole (and variations), etc.) and only energy exhaustion (denoted as sleep deprivation torture in [10]) and denial of service can be directly tied to the medium access layer. This is also consistent with [15] which adds unfairness.

An interesting countermeasure approach to mitigate DoS attacks that can be applied to the medium access layer is a technique known as selective verification [16]. It is based on a “shared channel model” in which the attacker transmissions share the medium with the transmissions of legitimate sending nodes. The underlying idea is that if the attacker’s bandwidth is constrained, the effect of the attack can be mitigated at the receiver by dropping received transmissions with some non-zero probability. This has the effect of introducing additional loss in the channel and the legitimate senders would compensate by increasing their transmissions to achieve a desired probability of reception.

In the following, we examine the vulnerabilities of the traffic-adaptive CWS-MAC flow-specific medium access scheme. Similar to [7]-[12], we identify the vulnerabilities, discuss the performance impact of associated attacks, and offer potential solutions to mitigate this impact.

3. Traffic-adaptive CWS-MAC

The frame structure of the energy-efficient, traffic-adaptive CWS-MAC protocol [13],[14] is shown in Figure 1. The underlying non-contention scheme is developed around a TDMA frame while the contention mode is based on a slotted ALOHA approach. The contention mode is overlaid on top of the non-contention frame through the use of a contention beacon of duration $t_b$. Prior to transmitting their non-contention packets, slot owners sample for this beacon at a time $t_{sS}$ (relative to the slot boundary) while the remaining nodes will sample for the beacon with some probability $p_s$. A value of $p_s = 1$ represents the case where the node samples every transmission slot. When a contention beacon is detected, the slot is redesignated by the node as a contention slot. Upon detection of the beacon, slot owners defer and the non-contention slot is effectively “seized” as a contention slot. A frame destination bitmap of duration $t_m$ is included at the beginning of each frame as shown in Figure 2. This map is used to identify the designated receivers in each non-contention transmission slot. A minislot destination bitmap of duration $t_{ms}$ is included at the beginning of each minislot within the contention slot as shown in Figure 3. This map is used to designate the receiver(s) for the subsequent contention packet transmission in that minislot.

The traffic-adaptive mechanism in traffic-adaptive CWS-MAC utilizes flow-specific queue size
statistics to respond to changes in flow load, overall network contention and channel quality. Each flow (or each set of flows if we group a set of flows with similar characteristics together) has its own queue at each node and when the queue size reaches a predetermined threshold the flow is switched from one access mode to another.

Nodes are permitted to enter a low-power sleep state if they are neither the sender nor a receiver of the current transmission. This is accomplished as follows. Nodes wake up at the beginning of each transmission frame to receive the frame destination map. This map is created by the individual nodes who broadcast their transmission slot maps. For a given node, this individual slot map identifies the receiver(s) for the upcoming transmission in the node’s slot within the current transmission frame. In the non-contention mode, nodes enter the sleep state for the duration of transmission slots in which they are neither an intended receiver or the slot owner with traffic to transmit.

For a contention slot, a node will wakeup at the beginning of each minislot to receive the minislot destination bitmap to determine whether or not it is an intended receiver for the subsequent contention traffic transmission in that minislot. This minislot destination bitmap is broadcast by a node that intends to attempt transmission in that minislot. A node will stay awake for the subsequent contention packet transmission if it is designated as an intended receiver. A node is allowed to enter the sleep state until the next minislot if it is not the intended receiver or if the bitmap is unreadable as a result of a collision due to multiple attempted transmissions in the minislot. Upon termination of the final minislot, a node will remain in the sleep state unless it was the designated receiver (or transmitter) of non-contention packets in the original non-contention slot that was “seized” in which case the node will wake up to receive (or transmit) non-contention packets during the non-contention period reserved at the end of the contention slot.

Further details on flow-specific medium access and the operation of energy-efficient, traffic-adaptive CWS-MAC can be found in [13],[14].

4. Vulnerabilities within Traffic-adaptive CWS-MAC

Traffic-adaptive CWS-MAC is designed to respond to changes in contention levels on the medium. If an attacker can artificially change the perceived contention levels, then the protocol can be made to respond in specific desired ways. Defense against these attacks, then, requires the ability to differentiate between actual or artificial (i.e., introduced by the attacker) contention levels. The set of vulnerabilities within traffic-adaptive CWS-MAC are thus tied to the mechanisms designed to observe and respond to contention levels on the medium.

We now discuss the primary vulnerabilities within the traffic-adaptive CWS-MAC medium access scheme. With the notable exception of a brief portion
of the closing discussion of jamming, we make the assumption that the attacker is operating within the scope of the protocol. An attack outside of the scope of the protocol, such as “brute force” jamming [11] in which the attacker transmits without regard to the protocol constraints, can be viewed as an attack at lower layer, specifically the physical layer.

4.1. Contention Beacon

In a contention beacon attack, an attacking node can transmit a contention beacon at the beginning of every non-contention slot. If this beacon is detected by a node, the node will recharacterize the slot as a contention slot and will remain awake for potential contention mode traffic. In addition, the non-contention slot owner will defer to the contention traffic and transmit the queued non-contention traffic during the shorter non-contention portion following the contention portion of the slot. The result of this attack, then, is an increase in energy consumption at the individual nodes and a reduction in maximum achievable non-contention mode throughput (along with a commensurate increase in mean delay for the non-contention mode). This attack is partially mitigated by the presence of the preamble sampling parameter. A value less than one will mean that there is a non-zero probability that a node will not be awake to detect the attacker’s contention beacon. This can be seen to be similar to the selective verification technique of [16]. Here, the act of sleeping through the contention beacon period is essentially equivalent to “dropping” the contention beacon transmission. Legitimate nodes with contention traffic to transmit will need to compensate for this artificial increase in the loss of the shared channel by increasing their contention beacon transmissions.

In the following, by assuming that the preamble sampling probability is one, we examine the worst case upper bound on the performance impact of this type of attack.

We begin with the reduction in non-contention mode throughput caused by a contention beacon attack. It can be shown [13] that the maximum normalized throughput in the non-contention mode of traffic-adaptive CWS-MAC is

\[
S_{\text{max}}^{nc} = \frac{M(t_c + p_c(t_{IFS} - t_b - kt_{aw}))}{t_f}
\]

(1)

where \( M \) is the number of slots in a frame and \( p_c \) is the probability of a contention slot. If we assume that the preamble sampling probability is one, it can be shown [13] that the probability of a contention slot when no attacker is present is

\[
\Pr[\text{cont. slot}] = 1 - e^{-\Lambda_c}
\]

(2)

where \( \Lambda_c \) is the aggregate contention packet arrival rate. To account for the presence of an attacker, we need to modify (2) to reflect the effect of the contention beacon attack. If the attacker transmits a contention beacon in every slot with some probability \( p_A \) then the probability of a contention slot becomes

\[
\Pr[\text{cont. slot}] = 1 - e^{-\Lambda_c} + \left[1 - \left(1 - e^{-\Lambda_c}ight)\right] p_A
\]

(3)

which reduces to
\[
\Pr[\text{cont. slot}] = p_c = 1 - e^{-\lambda T_{cont}} + (e^{-\lambda T_{cont}}) \lambda_A.
\]  
(4)

We plot the probability of a contention slot as a function of the aggregate contention packet arrival rate and the probability of an attack in Figure 4. As expected, the probability of a contention slot increases as both the packet arrival rate increases and the probability of the attack increases. This probability is one when the probability of an attack is one since, in this case, the attacker transmits a contention beacon during every non-contention slot and the slots are all redesignated as contention slots (i.e., in (4), \( p_c = 1 \) thus \( p_c = 1 \)).

Substituting (4) into (1), we arrive at the maximum normalized non-contention throughput as a function of both the aggregate contention arrival rate and the probability of an attack as

\[
S_{\text{nc}}^{\text{max}} = \frac{M}{t_f} \left[ t_{nc} + \left( 1 - e^{-\lambda T_{cont}} + (e^{-\lambda T_{cont}}) \lambda_A \right) (t_{IFS} - t_b - k t_{ms}) \right].
\]  
(5)

We plot this result in Figure 5. Note that while the mean non-contention throughput decreases as the probability of the attack increases, it is bounded by a constant value that represents the non-contention portion of the contention slot in Figure 1. This inherent degree of immunity is thus tied to the minimum bandwidth allocated to the non-contention traffic. This minimum bandwidth is insulated from a contention beacon attack and can be seen from (5) to be

\[
\min \left( S_{\text{nc}}^{\text{max}} \right) = \frac{M}{t_f} \left[ t_{nc} + t_{IFS} - t_b - k t_{ms} \right].
\]  
(6)

which represents the “degree” of immunity against this type of attack in terms of the non-contention throughput.

Figure 4. Probability of a contention slot as a function of the aggregate contention packet arrival rate and the probability of a contention beacon attack.

In a manner similar to the throughput analysis, we can also modify the non-contention mode mean delay derivation of [13] to account for (4). The square of the coefficient of variation can be shown to be

\[
\frac{\text{VAR}[T_{nc}]}{(T_{nc})^2} = \frac{p_c}{(1-p_c)^2} \left\{ \left(p_c \right)^{2 \kappa} + \left( \left( \kappa - 1 \right)^2 - 1 \right) \left(p_c \right)^\kappa - 2 \kappa^2 - 2 \kappa - 1 \right\} \left(p_c \right)^{\kappa - 1} + \kappa^2 \left( 1 - (1-p_c)^2 \right) \left(p_c \right)^{\kappa - 2} - 1,
\]  
(7)

where \( \kappa = \left\lceil t_{nc} \right\rceil \) and \( f(x) = \left\lceil x \right\rceil \) is the ceiling operator. From this, we can develop the mean total delay in the non-contention mode to be

\[
\overline{D}_{nc} = \frac{t_f}{2} + \frac{\lambda_{nc} \left( 1 - (p_c)^{\kappa} \right)^2}{2 \left( 1 - p_c \right) \left( 1 - \left( \frac{\lambda_{nc}}{\lambda_{cont}} \right) \right)} \left( \text{VAR}[T_{nc}] \right) \left( \overline{T}_{nc} \right) + \left[ t_f - t_{nc} \right] \left( \frac{\lambda_{nc} \left( p_c \right)^{\kappa} - (\kappa + 1) (p_c)^{\kappa} + 1}{1 - p_c} \right)
\]  
(8)

where \( t_{nc} = t_{nc} + t_{IFS} - t_b - k t_{ms} \) and \( \lambda_{nc} \) is the per node non-contention packet arrival rate. For the case in which the contention packet arrival rate is zero, we plot the mean delay as a function of both the
aggregate contention arrival rate and the probability of an attack in Figure 6. Again, as in the case of the throughput, we note that while the mean delay is an increasing function of the probability of an attack, a bound is provided due to the non-contention portion of the contention slot. This can be developed from (8) using L’Hôpital’s rule to be

\[
D_{nc}^* = \frac{t_s + \frac{\lambda_{nc} (\kappa t_f)^2}{2(1 - \lambda_{nc} \kappa t_f)}}{2} + t_b + k t_{ms} + t_{nc} - (\kappa - 1) t_{nc2}.
\]

Finally, we can examine the effect of an attack on per node mean energy consumption utilizing the radio energy model of [14] and shown in Figure 7. In the following, the power consumption (and time) associated with the Sleep, Receive and Transmit states is \( P_s \), \( P_{Rx} \), and \( P_{Tx} \) (\( T_s \), \( T_{Rx} \), and \( T_{Tx} \)), respectively. The power consumption (and time) associated with the transient states are indicated as \( P_{exiting\_state-entering\_state} \) (\( T_{exiting\_state-entering\_state} \)).

For example, the power consumption (and time) associated with the Sleep to Receive transient state is

\[
P_{exiting\_sleep-entering\_receive} = (1 - p_{ms}) (1 - p_{rs}) P_s
\]

where

\[
p_{ms} = \left(1 - e^{-\lambda_{ms} t_f}\right) \left(\frac{1}{n}\right) \quad \text{and} \quad p_{rs} = \left(1 - e^{-\lambda_{rs} t_f}\right) \left(\frac{n-1}{n^2}\right).
\]

Here, we have made the assumption that transmissions are unicast and that it is equally likely that any one node will be the destination for the transmission.

Examining the non-contention slot, we treat the transmission and reception cases individually. The energy consumption parameters for the transmission case are

\[
E_{\text{Xmt\_non\_cont\_slot}} = t_{ns} P_{Tx} + T_{z-Rx} P_{z-Rx} + T_{Rx} P_{Rx-Z} (13)
\]

and

\[
Pr\left[ E_{\text{Xmt\_non\_cont\_slot}} \right] = (1 - p_s) P_{in}
\]

while the expressions for the reception case are

\[
E_{\text{Recv\_non\_cont\_slot}} = t_{ns} P_{Rx} + T_{z-Rx} P_{z-Rx} + T_{Rx} P_{Rx-Z} (15)
\]

and

\[
Pr\left[ E_{\text{Recv\_non\_cont\_slot}} \right] = (1 - p_s) P_{rec}
\]

where \( t_{ns} = t_s - t_{RS} - (t_{prop} + t_{guard}) \). For the latter case, we have again made the assumption that
transmissions are unicast and that it is equally likely that any one node will be the destination for the transmission.

For a contention slot, we must consider not only the transmission and reception cases individually, we must also consider the contention and non-contention portions of the contention slot. We start with the contention portion of the slot and find the accompanying expressions for transmission to be

\[
E_{\text{Xmt cont slot}} = t_s P_{tx} + T_{z-rx} P_{z-rx} + T_{t-tz} P_{t-tz} + e^G (t_m P_{tx} + T_{r-rx} P_{r-rx} + T_{t-rx} P_{t-rx}) \]

\[
+ (k - e^G) (t_m P_{rx} + T_{z-rx} P_{z-rx} + T_{r-rx} P_{r-rx}) \] (17)

and

\[
\text{Pr}[E_{\text{Xmt cont slot}}] = p_c (1 - e^{-\lambda c}) \] (18)

where \( G \) is the offered load for the Slotted ALOHA scheme. For reception in the contention portion of a contention slot we have

\[
E_{\text{Rcv cont slot}} = k t_s P_{rx} + T_{z-rx} P_{z-rx} + T_{r-rx} P_{r-rx} \]

and

\[
\text{Pr}[E_{\text{Rcv cont slot}}] = p_c e^{-\lambda c} \{ p_s + (1 - p_s) (p_{inc} + p_{mnc}) \}. \] (20)

For the non-contention portion of the contention slot, the transmission expressions are

\[
E_{\text{Xmt nc in cont slot}} = t_{nc} P_{tx} + T_{z-rx} P_{z-rx} + T_{r-rx} P_{r-rx} \]

and

\[
\text{Pr}[E_{\text{Xmt nc in cont slot}}] = p_c p_{inc} \times \{ p_s + (1 - p_s) (1 - p_s) \} \] (22)

while the reception expressions are

\[
E_{\text{Rcv nc in cont slot}} = t_{nc} P_{rx} + T_{r-rx} P_{r-rx} \]

and

\[
\text{Pr}[E_{\text{Rcv nc in cont slot}}] = p_c p_{mnc} \times \{ p_s + (1 - p_s) (1 - p_s) \} \] (24)

where \( p_{inc} = 1 - e^{-\lambda c} \) and \( t_{nc} = t_{s} - t_{m} - k t_{m} \).

Finally, we can calculate the energy consumption in the sleep state as

\[
E_{\text{sleep}} = P_s (t_s - T_{\text{Rcv dest bitmap}} - n \{ \text{Pr}[E_{\text{sampling}}] T_{\text{sampling}} + \text{Pr}[E_{\text{Xmt non cont slot}}] T_{\text{Xmt non cont slot}} + \text{Pr}[E_{\text{Rcv non cont slot}}] T_{\text{Rcv non cont slot}} + \text{Pr}[E_{\text{Xmt cont slot}}] T_{\text{Xmt cont slot}} + \text{Pr}[E_{\text{Rcv cont slot}}] T_{\text{Rcv cont slot}} + \text{Pr}[E_{\text{Rcv nc in cont slot}}] T_{\text{Rcv nc in cont slot}} + \text{Pr}[E_{\text{Rcv nc in cont slot}}] T_{\text{Rcv nc in cont slot}} \}) \] (25)

We combine (10) - (25) to arrive at the mean total per node per frame energy consumption as

\[
E_{\text{total}} = E_{\text{sleep}} + E_{\text{Rcv dest bitmap}} + n \{ \text{Pr}[E_{\text{sampling}}] E_{\text{sampling}} + \text{Pr}[E_{\text{Xmt non cont slot}}] E_{\text{Xmt non cont slot}} + \text{Pr}[E_{\text{Rcv non cont slot}}] E_{\text{Rcv non cont slot}} + \text{Pr}[E_{\text{Xmt cont slot}}] E_{\text{Xmt cont slot}} + \text{Pr}[E_{\text{Rcv cont slot}}] E_{\text{Rcv cont slot}} + \text{Pr}[E_{\text{Rcv nc in cont slot}}] E_{\text{Rcv nc in cont slot}} + \text{Pr}[E_{\text{Rcv nc in cont slot}}] E_{\text{Rcv nc in cont slot}} \} \] (26)

We plot these results in Figure 8 and see, as expected, that mean energy consumption increases as the probability of an attack increases.

We can consider solutions to address this contention beacon vulnerability by understanding the
underlying issue. The issue is that legitimate nodes cannot differentiate between the contention beacon of another legitimate node and the contention beacon of an attacking node. This is problematic because contention beacons can and often will be transmitted simultaneously by multiple legitimate nodes. Thus, it is difficult to embed identifying information in these beacons since they often collide at the individual nodes.

As an alternative, a legitimate node can ignore a contention beacon with some probability. This is essentially what occurs when the preamble sampling probability is set to some value less than one [14]. The acknowledgement mechanism in the contention mode will recover from any “missed” transmissions, but there is no similar mechanism in the non-contention mode. Thus, we cannot recover from collisions or missed traffic in the non-contention mode which implies that a slot owner with non-contention traffic to send cannot ignore the contention beacon. To do so would create a non-zero probability of collision during its subsequent non-contention transmission. The introduction of an acknowledgement mechanism in the non-contention mode would further increase the protocol’s immunity to a contention beacon attack at the added overhead of reduced throughput and increased delay in the non-contention mode [17].

4.2. Minislot contention scheme

Given traffic-adaptive CWS-MAC’s Slotted ALOHA contention scheme in an attacker can artificially raise his Slotted ALOHA transmission probability. If set to one, this will cause the attacker to contend for every minislot by transmitting a minislot destination bitmap at the beginning of each minislot. If a legitimate node attempts to contend for the minislot as well by transmitting its own minislot destination bitmap, there will be a collision. This will have the effect of driving the contention mode throughput to zero since no legitimate node will be able to successfully “win” a transmission minislot. While this is a form of denial of service, traffic-adaptive CWS-MAC does have a degree of immunity against this attack. When the contention throughput drops to zero, this will cause the flow-specific queues at the individual nodes to begin to back up. Eventually, these nodes will reach the switching threshold and be shifted into the non-contention mode. At this point, the traffic will be transmitted in the non-contention mode with the accompanying increase in delay. Thus, the ultimate performance effect of this attack is not a reduction in throughput, but an increase in delay because traffic will be transmitted in the non-contention mode vice the contention mode. This attack can be combined with the previous contention beacon attack to further reduce the non-contention throughput, though.

If the attacking node marks all nodes as receivers in his transmitted minislot destination bitmap, this will cause all nodes to remain awake during the subsequent minislot to wait for the expected contention traffic. An energy exhaustion attack, this will increase the per node energy consumption by artificially raising the probability that a node will be awake to receive contention traffic in (20). It should be noted though, that a collision in a minislot (the result of a legitimate node also trying to transmit a minislot destination bitmap), will cause the bitmaps to be corrupted and will allow the remaining nodes to enter the sleep state since they will not receive a legible minislot destination bitmap for that minislot. While this seems to provide some degree of immunity to this type of energy exhaustion attack, it is of limited impact because eventually all of the legitimate flows will be transitioned out of the contention mode and, hence, the probability of a collision will eventually go to zero.

4.3. Frame destination bitmap

In the non-contention mode, an attacker can generate a “broadcast” frame destination bitmap for its non-contention transmission slot in which it designates all nodes as receivers of its upcoming non-contention transmission. An energy exhaustion attack, this will cause all nodes to wake up for the duration of the attacking node’s non-contention slot and, thus, increase per node energy consumption by artificially increasing the value of $p_{\text{mc}}$ in (12), (16), (20) and (24).

Traffic-adaptive CWS-MAC does have a certain degree of immunity to this attack because a node can only wake other nodes up by designating them as receivers in its own transmission slot. Thus, for
example, if a node is only assigned a single non-contention slot per frame then he will only be able to wakes the other nodes up for the duration of this single slot. In addition, an attacking node would need to have been assigned a transmission slot in the non-contention mode setup phase to be able to conduct this type of attack. A hostile node that has not been assigned a transmission slot in the slot assignment process cannot mount this attack. In discussing this latter inherent immunity to an “outsider,” we make the implicit assumption that the slot assignment is “attack free.” This implies, to a certain degree, that the slot assignment process is centralized and is preceded by some type of authentication process [12].

4.4. Traffic-adaptive switching mechanism

An attacker can artificially (or unfairly) raise the value of its queue-based switching thresholds. These thresholds are illustrated in Figure 9 where $\theta_1$ and $\theta_2$ define the points at which a given flow will transition into and out of, respectively, the non-contention mode. This will cause the attacker’s traffic to remain in the contention mode (with the associated improved delay performance) for a disproportionate amount of time. In addition, this will also cause the legitimate traffic flows to transition to the non-contention mode (with its associated increase in delay performance) earlier than anticipated. If the attacker sets its threshold to infinity, then its traffic will never transition out of the non-contention mode. This is a form a “greedy” attack in which the attacking node does not seek to reduce the performance of the network as a whole, but does seek to unfairly improve its own performance at the expense of other legitimate nodes.

For the case of two flows, the relationship between the switching mechanism and the probability that a flow will be in a given state is given from the results of [13]. The probability that a flow is in the non-contention state depends on the utilization in both the contention and non-contention states as well as the choice of the switching thresholds.

4.5. Jamming

We close this section with a discussion of jamming. While, as noted earlier, “brute force” jamming can be viewed as an attack at the physical layer vice the data link layer [11], we can nevertheless evaluate its effect on traffic-adaptive CWS-MAC. Jamming will fundamentally result in an increase in collisions. In the contention-mode, this will be evaluated as a rise in contention levels that will eventually drive all of the flows into the non-contention mode. While in the contention mode, though, collision recovery is achieved through the use of the acknowledgement mechanism. This can be seen as providing some degree of immunity against this denial of service attack, but eventually all flows will transition to the non-contention mode in which no collision recovery mechanism is provided so it is of limited impact.

In contrast to the brute force approach, intelligent jamming seeks to exploit specific vulnerabilities within the protocol to minimize the energy required to conduct the attack [11]. Targets of intelligent jamming in the IEEE 802.11 networks include Clear-to-Send packets, acknowledgement packets and data packets. Similarly, traffic-adaptive CWS-MAC is susceptible to targeted jamming of its control and data transmissions including the acknowledgement packets in the contention-mode and the destination bitmaps. In all cases, this type of attack will result in a decrease in throughput and an increase in delay with an accompanying rise in energy consumption as packets are retransmitted.

Potential physical layer solutions to the jamming problem include forward error correction, directional antennas, and [15],[11]. Higher layer approaches include varying protocol parameters to reduce the effectiveness of targeted jamming [18] and putting nodes to sleep during the duration of the jamming [15]. The latter requires the ability to detect the presence of the jamming. At the data link layer, this could be achieved using traffic-adaptive CWS-MAC by adding an acknowledgement mechanism in the non-contention mode [17]. This modification would come at the expense of reduced throughput in this mode.

5. Conclusions

In this paper, we identified and analyzed the security vulnerabilities found in traffic-adaptive CWS-MAC, a flow-specific medium access scheme. Critical vulnerabilities were found that expose the protocol to denial of service, energy exhaustion and “greedy” attacks. The effect of attacks exploiting these vulnerabilities include decreased throughput and increased delay in both the contention and non-contention modes as well as increased per node energy consumption. Solutions were suggested that can mitigate to some degree the effect of these attacks including the introduction of a contention beacon sampling approach that necessitates the use of a non-contention error control mechanism.
6. References


