

A Statistical Approach to detect NAV Attack at MAC layer

K.Sugantha
ksugantha@yahoo.com
Anna University

S.Shanmugavel
ssvel@annauniv.edu
Anna University

Abstract

This paper proposes and investigates a statistical approach to detect the NAV attack in MAC layer. We present simulation and analytical results showing that the NAV attack can under perform the standard 802.11 MAC protocol. Further no approach has been explicitly specified to detect this attack. This approach is a simpler method to detect NAV attack using Glomosim simulator. In this work we investigate the vulnerabilities and detect the NAV attack.

1.Introduction

The IEEE 802.11 standard [1] for WLANs is one of the few highlights of communication technologies in recent years. Two types of MAC access protocols, Distributed Coordination Function (DCF) and Point Coordination Function (PCF) are defined in 802.11.DCF is the basic access mechanism [12] of 802.11 while the latter aims at supporting real-time traffic. The state protocols are modeled [8] using systems of communicating machines.

The rest of the paper is organized as follows. Section 2 reviews the 802.11 standard. Section 3 describes the related work. Section 4 describes the NAV attack. Section 5 presents the simulation and detection of NAV attack. Section 6 concludes the paper.

2.IEEE 802.11 standard

DCF [12] is a fundamental MAC layer operation in 802.11 WLAN.DCF is based on Carrier Sense Multiple Access [10] with Collision Avoidance (CSMA/CA) mechanism. To resolve collisions of packets simultaneously transmitted by different stations, a binary slotted exponential backoff algorithm [9] is employed in DCF.

2.1. State Diagram for DCF:

Figure1 gives the state diagram [8] of DCF. The DCF operation starts when a frame is ready to be sent. The machine starts in state 0. When a frame is received, the state goes to 5.The machine performs the SIFS wait in state 5.Once this timer expires, the machine transmits the ACK frame and gets to state 0. When a machine has a DATA frame to send, it gets to state 1. If there is no backoff or if the medium is free, the machine gets to state 2. If the medium were busy any time the machine reaches state 1. If the medium is free for DIFS duration, the machine reaches state 3. Once in state 3, it performs the additional backoff wait if Backoff is true. The backoff timer is reduced for the time the medium was free. If the medium becomes busy, the backoff timer is frozen, and the machine gets back to state 1 during Backoff. When the backoff timer eventually expires, the machine gets to state 4. In state 4,a timeout or an ACK is sent accordingly. The number of retransmissions is limited. Once this limit is exceeded, the data frame is discarded, and the machine returns to state 0. The reception of an ACK for a frame being currently re-transmitted due to a timeout causes the system to declare the frame to be a success, and the machine returns to state 0. The reception of a corrupt frame retransmits the frame for proper reception. The states are specified as follows:0-Entry for transmission; 1-Ready to transmit state; 2 -DIFS wait; 3-Backoff; 4 -Transmission state; 5-ACK state.

2.2.Virtual Carrier Sense Mechanism

Figure 2 shows the use of RTS and CTS [10] with the NAV value set [2].After waiting for DIFS the sender issues a RTS packet.The RTS packet contains the duration of the whole data transmission.This duration specifies the time interval necessary to transmit the whole data frame and the acknowledgement related to it. Every node receiving this RTS now has to set its NAV in accordance with

the duration field. The NAV specifies the earliest point at which the station can try to access the medium again. If the receiver receives the RTS, it replies with a CTS packet after waiting SIFS time. This CTS packet contains the duration field again and all stations receiving this packet from the receiver of the intended data transmission have to adjust their NAV. Now all the nodes within the receiving distance are informed that they have to wait more time before accessing the medium. Basically this mechanism reserves the medium for one sender exclusively and hence the name, virtual reservation scheme. The RTS and CTS packet contains the field as specified in figures 3a and 3b respectively.

3.Related Work

Recent approaches are more towards the study of the MAC layer misbehavior in adhoc networks. In [4] the virtual carrier sense attack is studied by sending variety of packet streams with a range of large duration values. In this paper [4] a limit accepted by nodes is placed on the duration field. Any packet containing a larger duration value is simply truncated to the maximum value allowable. Strict adherence to the required use of the NAV feature indicates two different limits: a low cap and a high cap. The low

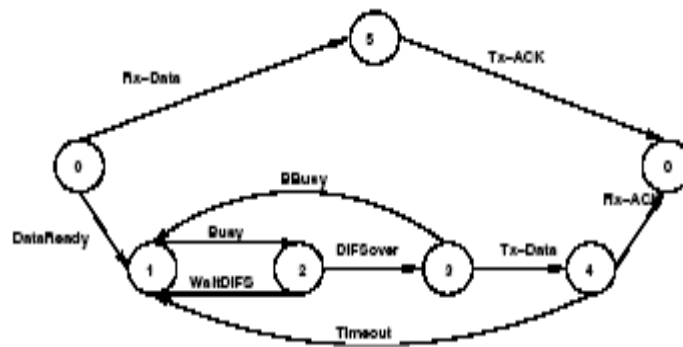


Figure 1. State Diagram for DCF

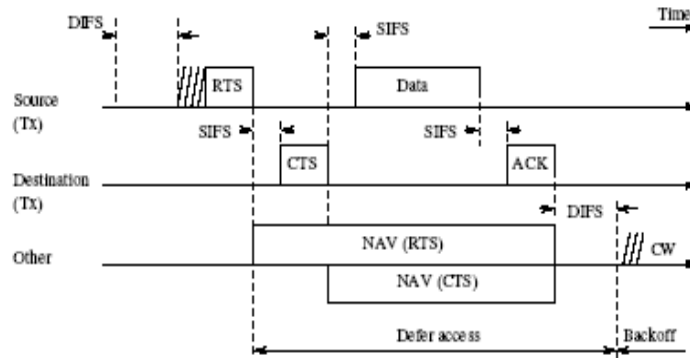


Figure 2. DCF operation using RTS/CTS mechanism

Frame control	Duration	Receiver Address	CRC
---------------	----------	------------------	-----

(a) RTS frame format

Frame control	Duration	Receiver Address	Transmitter Address	CRC
---------------	----------	------------------	---------------------	-----

(b) CTS frame format
Figure 3. Frame format

cap has a value equal to the amount of time required to send an ACK frame, plus media access backoffs for that frame. The low cap is usable when the only packet that can follow the observed packet is an ACK or CTS. This includes RTS and all management (association, etc) frames. The high cap, on the other hand, is used when it is valid for a data packet to follow the observed frame. The limit in this case needs to include the time required to send the largest data frame, plus the media access backoffs for that frame. The high cap must be used in two places: when observing an ACK (because the ACK may be part of a MAC level fragmented packet) and when observing CTS.

The paper [6] explains the concept of packet modification and issues arising due to DCMAC. This [6] explains well the packet timing, which will be useful for the correction mechanism of the NAV attack.

Another approach given by Dazhi chen [7] which states that the misbehaving nodes can arbitrarily set the value of RTS and CTS frames thus falsely blocking the neighboring nodes and that the misbehavior can be detected by looking at the RTS and CTS frame duration. But the misbehaving nodes may falsely advertise the frame duration thus making the detection impossible.

In this paper we have suggested an alternate statistical approach to detect such misbehaviour. This paper involves the study of change in the mean and standard deviation for the normal packet transfer and during attack condition. Such study is useful in the detection of NAV attacks in MAC layer.

4. NAV Attack

A major challenge in the MAC layer is the greedy behavior [3] of a station to gain bandwidth at the expense of other stations. There are two kinds of vulnerabilities namely identity vulnerability and MAC vulnerability. Identity vulnerability arises because of the implicit trust placed on the source address. This poses two attacks namely Deauthentication and Disassociation attack and Power saving mode attack.

MAC vulnerabilities [11] arise because of the collision avoidance mechanism of the 802.11 MAC layer. This causes two kinds of attacks: Time window attack and NAV attack (Virtual carrier sense attack).

4.1 Time window attack

802.11 MAC defines time windows to prioritize access to the channel. Short interframe space (SIFS) is used for existing frame exchange and Distributed

interframe space (DIFS) for new frame exchange with $SIFS < DIFS$. Every station has to wait at least SIFS before transmitting. Therefore, the attacker can completely monopolize the channel by sending a signal before the end of every SIFS interval. However, there is a problem with the attack. Since SIFS is 28 μs (802.11b), the attacker will have to send a signal approx. 37,000 times per second.

4.2 NAV attack

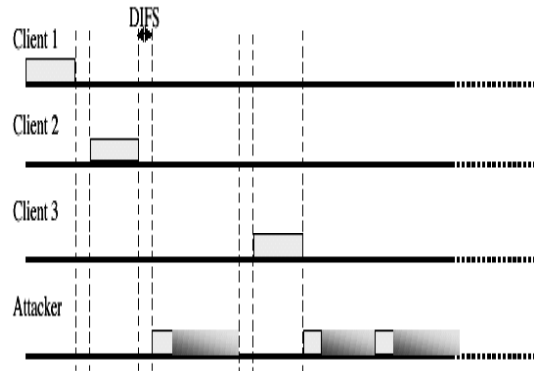


Figure 4. NAV attack

A more serious vulnerability arises from the virtual carrier-sense mechanism used to mitigate collisions from hidden terminals. An attacker may exploit this feature by asserting a larger duration field, thereby preventing well behaved clients from gaining access to the channel (as shown in Figure 4). This type of attack is called NAV attack. While it is possible to use almost any frame type to control the NAV, including an ACK, using the RTS has some advantages. The misbehaving nodes set the value of the duration of the RTS and/or CTS packets to reserve the channel for an additional time. Since a well-behaved node will always respond to RTS with a CTS, an attacker may co-opt legitimate nodes to propagate the attack further than it could on its own. Moreover, this approach allows an attacker to transmit with extremely low power or using directional antennae, thereby reducing the probability of being located. The maximum time that the channel can be reserved for in a single frame is limited by the size of the duration field, a maximum of 32767 microseconds [1]. Assuming that the attacker sets maximum value, he has to transmit only 30 times per second, and therefore, easy for the attacker.

5. Simulation

The NAV attack can be easily determined by a statistical method of detection. Generally each

node follows a distribution while packets are transmitted. When the normal process is violated the nodes show a variation in this distribution. Our method basically uses this approach to detect an attacker for NAV attack. In our simulation all nodes follow uniform distribution. For each node, when the packets are received, the mean and standard deviation is calculated and a threshold level is set. However under attack the mean and standard deviation varies largely. If the values fall below the threshold level then it is an abnormal behavior. Thus the deviation from the normal value asserts the abnormal behavior.

In this section we evaluate the attacks at the MAC layer. We have used GLOMOSIM [5] for our simulations. The assumption in this simulation is that no packets are dropped due to retransmission. The simulation is for 80 seconds. The simulation contains 10 nodes, with all nodes sending CBR traffic of 512 bytes of 1000 packets to node 3. Node 3 is the receiver. Node 3 receives the packets, every .0625s, from each node. The throughput of the each node is recorded and given below in figure 5.

Under NAV attack, node 1 tries to gain more throughput by transmitting more number of packets. This is more significant when large packets are transmitted. In figure 5 node 1 gains more throughput compared to other nodes under NAV attack and some packets are dropped in other nodes. The end-to-end delay for both the cases are shown in figure 6.

Table 1 below shows the number of packets received within the time interval [0,4], [4,15], [15,26],[26,37],[37,48],[48,59],[59,70],[70,81] ie.for node0,112 packets are received for the interval[4,15] and so on. Fig 7a and 7b shows the uniform distribution of packets received for node 0 and node 4 respectively.

The receiver calculates the mean and standard deviation for each node based on the packets received. The receiver is a trust-worthy node, which collects all the information and sets the mean value and standard deviation for all the nodes. Table 2 shows the number of packets received under attack. For example, for node0 the number of packets received for the interval [4,15] is 112 and for [70,80] it is 8 and for others it is 160. But under attack it is clear that there is a variation in the packets received and is not the same for any interval. Under attack, the nodes fail to follow the normal distribution. This is shown in figure 8a and 8b, which shows that for the same nodes 0 and 4, the distribution changes. Now under attack the receiver calculates mean and standard deviation of each node by the packets it has received.

The receiver now compares the values with the normal behavior. Under attack condition, the mean and standard deviation falls below the threshold thus confirming the misbehavior. This is shown in figure 9 where the mean and standard deviation values falls below the threshold level. The threshold for mean and standard deviation for each node is 142.8571 and 52.45. Any node below these values confirms the NAV attack. Nodes 2,5,8 all have their mean value below the threshold. Also the standard deviation for node 5 falls below the set standard deviation threshold.

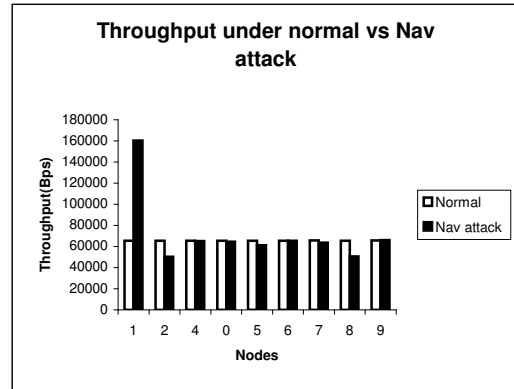


Figure 5. Throughput of nodes

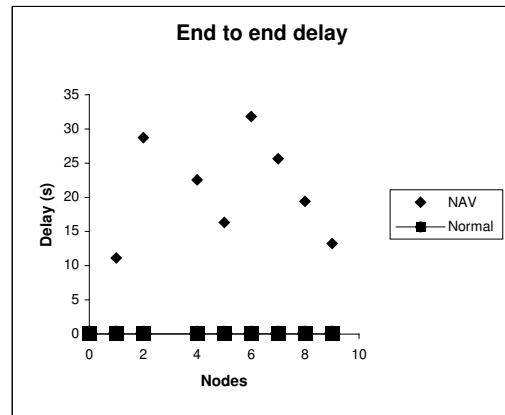


Figure 6. End to end delay of nodes

The deviation from the normal behavior detects the NAV attack. Also from the figure 6, node 1 has very less end-to-end delay compared to other nodes and a large throughput compared to other nodes thus being detected as the misbehaving node.

Table 1. Number of packets received by node3 (receiver) for each node under normal condition

Duration in seconds	No. of packets received from Node 0	No. of packets received from Node 1	No. of packets received from Node 2	No. of packets received from Node 4	No. of packets received from Node 5	No. of packets received from Node 6	No. of packets received from Node 7	No. of packets received from Node 8	No. of packets received from Node 9
0-4	0	0	0	0	0	0	0	0	0
4-15	112	160	144	128	96	64	48	32	16
15-26	176	176	176	176	176	176	176	176	176
26-37	176	176	320	176	176	176	176	176	176
37-48	176	176	176	176	176	176	176	176	176
48-59	176	176	176	176	176	176	176	176	176
59-70	176	136	152	168	176	176	176	176	176
70-80	8	0	0	0	24	56	72	88	104

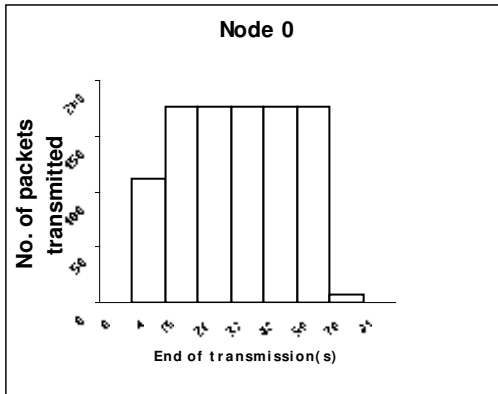


Figure 7(a)

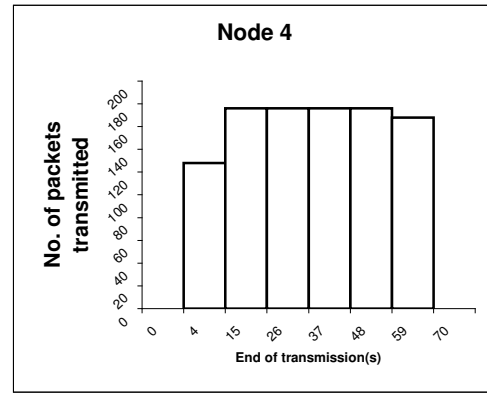


Figure 7(b)

Table 2. Number of packets received by node3 (receiver) for each node under NAV attack

Duration in seconds	No. of packets received from Node 0	No. of packets received from Node 1	No. of packets received from Node 2	No. of packets received from Node 4	No. of packets received from Node 5	No. of packets received from Node 6	No. of packets received from Node 7	No. of packets received from Node 8	No. of packets received from Node 9
0-4	0	0	0	0	0	0	0	0	0
4-15	97	160	137	128	87	58	24	20	13
15-26	154	176	180	164	150	159	74	137	172
26-37	192	176	152	135	163	154	248	103	131
37-48	168	176	188	193	184	201	141	20	178
48-59	121	176	129	181	107	169	196	147	220
59-70	247	136	126	199	126	201	204	230	174
70-80	21	0	0	0	115	58	75	75	112

6. Conclusion and Future Work:

Handling Mac layer misbehavior is an important requirement in ensuring a reasonable throughput share for well-behaved nodes in the presence of misbehaving nodes. The above

simulation results have indicated that our scheme provides fairly accurate diagnosis of the NAV attack. Once the NAV attack is detected, the correction method can be used as suggested in [4]. We have proposed this statistical method to detect the misbehavior due to NAV attack.

We have proposed the scheme for a constant Bit Rate traffic. We plan to extend the proposed scheme for other traffic classes and make the detection method adoptable for any type of traffic. We also plan to develop these detection methods to HTTP, Telnet, and FTP traffic classes. We also plan to propose a correction method for such type of classes.

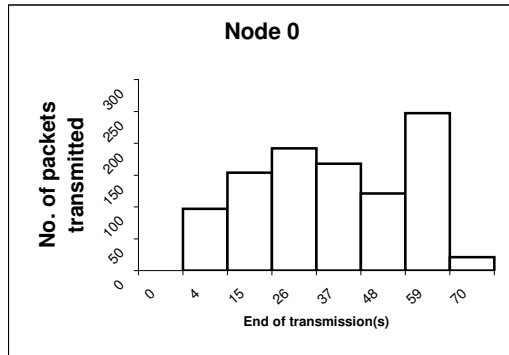


Figure 8(a)

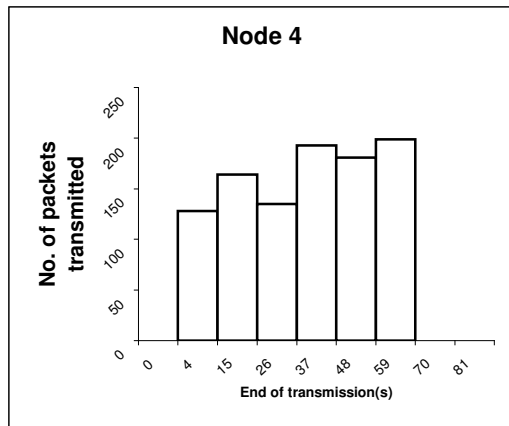


Figure 8(b)

References:

[1] IEEE Standard for wireless LAN – Medium Access Control and Physical layer Specification, P802.11”, 1999.
 [2] IEEE 802.11 tutorial, eecs.berkeley.edu, June 2002.
 [3] Domino: A system to Detect Greedy Behavior in IEEE 802.11 Hotspots, MobiSYS 2004, June 6-9, 2004, Boston, Massachusetts, USA.
 [4] John Bellardo and Stefan Savage -802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, In proceedings of USENIX security symposium, August 2003.
 [5] Glomosim: <http://pcl.cs.ucla.edu/projects/glomsim/>.

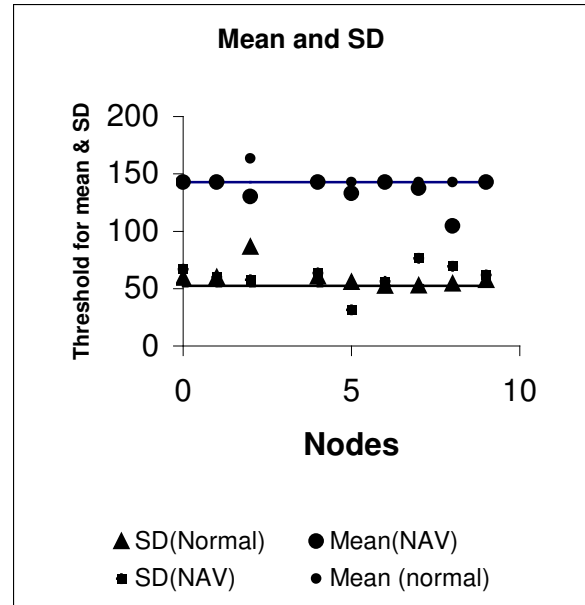


Figure 9

[6] Explicitly pipelining IEEE 802.11 to enhance performance, University of Illinois at Urbana – Champaign 2003.
 [7] Protecting wireless networks against a denial of service attack based on virtual jamming, Dazhichen, JingDeng, PramodVarshney, Mobicom2003.
 [8] Specification and Analysis of the DCF and PCF Protocols in the 802.11 Standard Using Systems of Communicating Machines, Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP’02) 1092-1648, 2002.
 [9] A TCP-like Adaptive contention window scheme for WLAN – Qixiang Pang, Soung Chang Liew, Jack Y.B. Lee, IEEE Communications society, 2004
 [10] Investigation of the IEEE 802.11 Medium Access Control (MAC) Sub layer Functions, IEEE Computer Society, 1997.
 [11] Security in Mobile Ad Hoc Networks: Challenges and Solutions, IEEE wireless communications, Feb 2004.
 [12] A Performance Analysis of the 802.11 Wireless LAN Communications in Information and Systems, Nitin Gupta and P.R. Kumar, Vol. 3, No. 4, pp. 279-304, Communication in Information and Systems, September 2004
 [13] IEEE 802.11 Optimal Performances: RTS/CTS mechanism vs. Basic method, Raffaele Bruno, Marco Conte, Enrico Gregori, 0-7803-7589-0/02, IEEE Computer Society, 2002.