

# Synchronization Attacks Against 802.11

Gunjan Khanna, Ammar Masood and Cristina Nita-Rotaru  
Purdue University

**Abstract**—The 802.11 standard specifies mechanisms for channel access as well as a power saving mode that require synchronization between a point coordinator (PC) and the stations. The synchronization is achieved using beacon packets sent periodically by the PC. In this paper we identify new synchronization attacks against 802.11 that exploit the beacon mechanism. We show through simulations that the attack can create significant damage to a large number of nodes inspite of being a low rate attack. In addition, we discuss several mitigation techniques.

## I. INTRODUCTION

The 802.11 [1] standard specifies a family of protocols developed by the IEEE for wireless LAN technology. The most well-know is 802.11b [2] that provides 11 Mbps transmission in the 2.4 GHz band and allows wireless functionality comparable to Ethernet. 802.11 specifies station services such as data delivery, authentication, privacy, and distribution services which enable a node to roam between several access points.

The standard specifies two mechanisms for channel access: the Distributed Coordination Function (DCF), which is mandatory and the Point Coordination Function (PCF) which is optional and used only in the infrastructure mode. PCF defines the access point (AP) to act as a point coordinator (PC). The PC periodically sends a poll message to the nodes to find out if they have data to transmit. In addition, a Power Saving Mode (PSM) is employed by the nodes to save power while they are waiting for the channel to become available for transmissions. A node can communicate to the AP its sleep schedule and the AP can buffer packets until the node wakes up.

Several vulnerabilities have been identified for 802.11b. These include attacks against confidentiality and integrity [3], authentication and de-authentication attacks [4], and selfish behavior from nodes using unfairly the channel [4], [5]. In this paper we identify new synchronization attacks that affect the PCF and PSM mechanisms. Below we describe the attack, provide simulation results that demonstrate the feasibility of the attack and discuss several mitigation techniques.

## II. SYNCHRONIZATION ATTACKS AGAINST 802.11

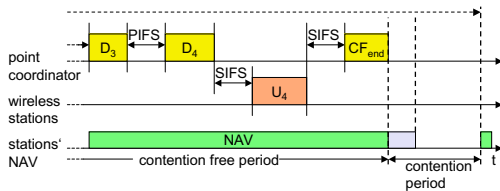


Fig. 1. PCF operation

Both PCF and PSM require synchronization amongst the PC and the stations (STA). In-order to achieve this synchronization

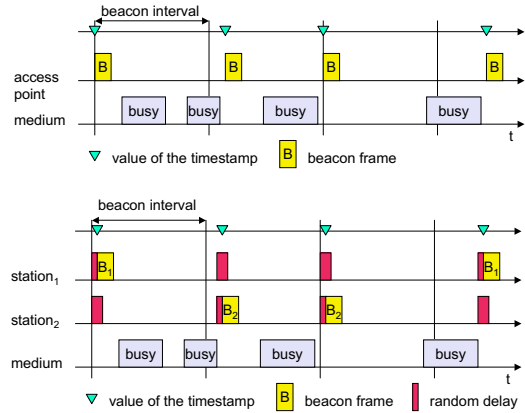


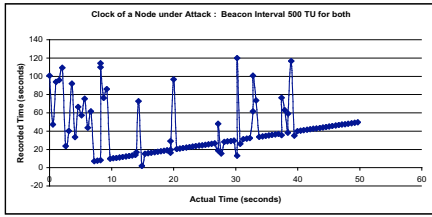
Fig. 3. Synchronization using beacon: ad hoc mode

the PC transmits a beacon packet at periodic intervals. The beacon packets are broadcasted in clear containing a timestamp representing the current local time at the PC. The nodes listening to the beacon adjust their local clocks according to the timestamp in the beacon packet. Typically, the base station broadcasts a beacon frame periodically (10 to 100 times per second). In the PCF mode the initial beacon sent out by the PC denotes the start of the polling period or contention free period. As shown in Figure 1 the beacon indicates the length of the contention free period (CFP). All the nodes back-off according to this value and wait for the polling packet for transmitting data.

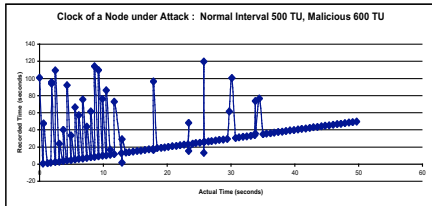
In addition, the beacon contains the next time when a beacon will be transmitted, i.e start of the next CFP period. In case the channel is busy during that time, the beacon is transmitted when the channel becomes free and the timestamp is adjusted accordingly (see Figure 2).

In case of an ad-hoc mode where no PC is available, synchronization using beacons is carried in a distributed fashion (Figure 3). At the start of a beacon interval each node chooses a random back-off timer and listens to the channel. In case a beacon is heard before one's timer expires then that node ends its timer and does not send a beacon until the next beacon interval. All nodes which hear the beacon adjust their local clocks according to the timestamp in the beacon. If no beacon is heard and the timer expires then the node sends a beacon containing timestamp .

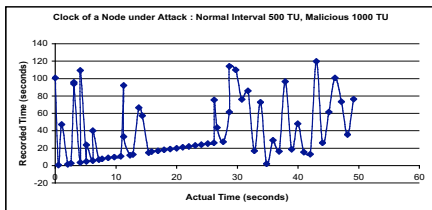
The Power Saving Mode (PSM) is employed by the nodes to save power while they are waiting for the channel to become available for transmission. A STA can go to power saving mode i.e. sleep at a particular time which is supported by AP. During the period of sleep the AP buffers the packets and hands them over to the STA when it wakes up. If a malicious



(a) Beacon interval length set at 500ms for normal and malicious PC



(b) Beacon interval length set to 600ms for malicious node



(c) Beacon interval length set to 1000ms

Fig. 4. Beacon Attacks: Synchronization Attacks

node can make the STA to wake up at different time this could lead to a reduced throughput because of loss of packets.

One way to attack both PCF and PSM is to de-synchronize the clocks of correct STA. The clock of a correct STA can be deviated by sending a single beacon with a malicious time value. This clock error will exist until a correct beacon is received by that node. The de-synchronization inherently de-stabilizes any protocol services which depend on synchronization.

### III. SIMULATION RESULTS

We use the NS-2 network simulator [6] version for simulating the attack scenarios. We modify the original 802.11 MAC protocol available in NS-2 to introduce the behavior of malicious STA. We simulate the synchronization attack using a network topology consisting of a set of 6 nodes, where one of them runs a malicious MAC implementation: it sends beacon packets with incorrect timestamps only during the CFP period.

In Figure 4 we plot the clock of normal nodes versus the global clock, while under attack. As seen in Figures 4 (a) and (c) the larger the CFP period of a malicious node, the larger the fluctuations in the clock of the normal node.

As another beacon is received by a normal node(STA), it can change the clock assuming the beacon time value is different from its clock value. In case of normal operation, the clock of the node must match the global clock and hence the plot must be a straight line with 45 degree slope. In Figure 4 (c) the malicious node has a double CFP period compared to the

normal point coordinator causing the malicious node to send a significant more beacons. Thus it leads to more fluctuations in the clock. We can see from the results that a malicious node sends a single beacon packet during each beacon interval making it a low rate attack which can cause significant de-synchronization in the network.

### IV. ATTACK MITIGATION TECHNIQUES

One way to prevent the attack is to authenticate every beacon and to require a STA to accept only authenticated beacons. This way only an authenticated point coordinator or the AP would be able to send beacons which can be used for time synchronization. Authentication can remove the attack vulnerability in the case of a centralized scenario where only one node has the responsibility of sending the beacon. We note that authentication will not be enough if the PC was compromised and is under the control of an adversary.

In case of ad-hoc networks where the time synchronization is performed in a distributed fashion, it is more difficult to provide authentication for all the nodes when nodes are dynamically joining and leaving. One possible solution that can protect against the attack to some extent is to have each node maintaining a *guard time*. A node can only change its clock if the time stamp in the beacon and its clock difference is within the guard time. This can prevent drastic changes in the clock of the nodes. However, if nodes join in later and clocks are not synchronized then this method can cause lack of synchronization between the new node and the existing network in case the clocks differ more than the guard time. The guard time can decrease the effectiveness of the attack but an attacker can still try to introduce drift by repeated sending well crafted time stamps which will be within the guard time but incorrect values. A more effective solution will be to use state information to detect incorrect behavior of neighbor nodes, and then ignore beacons coming from malicious nodes.

### V. CONCLUSIONS

In this paper we identify new synchronization attacks against the 802.11 MAC protocol that exploits the beacon mechanism. We show through simulations that the attack is a low rate attack that can create significant damage to a large number of nodes. We are currently performing a more detailed analysis of the impact of the attack and of the proposed defense mechanisms.

### REFERENCES

- [1] *IEEE Std 802.11, 1999 Edition*. 1999. <http://standards.ieee.org/catalog/olis/lanman.html>.
- [2] *IEEE Std 802.11b-1999*. <http://standards.ieee.org/>.
- [3] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *In 7<sup>th</sup> Annual International Conference on Mobile Computing and Networking*, July 2001.
- [4] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *In USENIX 2003*, 2003.
- [5] P. Kyasanur and N. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks," in *International Conference on Dependable Systems and Networks (DSN'03)*, June 2003.
- [6] "The network simulator - ns2." <http://www.isi.edu/nsnam/ns/>.