Efficacy of Physical Layer Preamble Manipulation for IEEE 802.11a/ac

Benjamin Ramsey, Jonathan Fuller and Christopher Badenhop

Wireless physical layer manipulation is a recently discovered technique for selective packet obfuscation. This process exploits the unique and proprietary nature of transceiver designs rather than manufacturing imperfections. To date, preamble manipulation has only successfully been demonstrated on low data rate transceivers operating in the 2.4 GHz band. This Letter investigates the effectiveness of preamble manipulation on common 5 GHz IEEE 802.11a and IEEE 802.11ac wireless transceivers for the first time. Herein it is demonstrated that the preamble short training sequence length can be manipulated to discern among the six transceiver designs under test with greater than 99% accuracy using fewer than 20 packets.

Introduction: Wireless connectivity is a key enabler in mobile communication systems. The IEEE 802.11ac high data rate standard enables wireless data rates comparable to gigabit Ethernet, while maintaining backward co-existence with IEEE 802.11a. Further refinements to IEEE 802.11ac systems are an active area of research [1][2]. Unfortunately, wireless security continues to pose significant challenges. Open source software tools to conduct MAC address spoofing, deauthentication attacks, and encryption key cracking have become ubiquitous [3]; these developments have spurred novel research into leveraging the physical layer to improve wireless security in depth.

Device manufacturers produce unique and proprietary transceiver designs; recent work reveals that these transceiver design idiosyncrasies can be reliably exploited [4][5][6][7]. The true hardware class of remote transceivers is determined through the use of physical layer preamble manipulation. Promising results have been demonstrated for 2.4 GHz IEEE 802.11b [4] and IEEE 802.15.4 [5][6][7] transceivers. These novel physical layer techniques exploit design idiosyncrasies present in all like-model devices from the same manufacturer. For example, wireless packets manipulated to have a physical layer preamble shorter than the protocol specification become unreceivable by some hardware designs, while reception by other hardware designs remains unaffected. Applications of this phenomenon are numerous, from obfuscated encryption key distribution [5] and wireless intrusion detection system evasion [6], to device fingerprinting [4][7]. Once implementation differences are discovered and published, they can be immediately leveraged in conjunction with any of the millions of such devices worldwide.

This Letter presents the first investigation of physical layer preamble manipulation on high data rate IEEE 802.11a and IEEE 802.11ac transceivers.

PHY preambles in 802.11a and 802.11ac: The IEEE 802.11ac standard utilizes increased spectral bandwidth and improved modulation schemes to increase its effective data rate beyond the earlier IEEE 802.11a protocol. However, since IEEE 802.11ac must still share the 5 GHz band with legacy devices, benign coexistence is important. The solution utilized is a preamble common to both protocols for clear channel assessment.

Preambles begin with a short training field (STF), immediately followed by a long training field (LTF). Each field is 8 μs long, for a combined STF and LTF duration of 16 μs. Fig.1 presents a representative magnitude plot of the STF and LTF regions as collected by a USRP X310 software-defined radio. The background noise floor appears at the left edge of the plot and the transmission progresses through time from left to right. The STF consists of a BPSK-OFDM training signal repeated ten times (t_1 through t_{10} in Fig. 1). The LTF consists of a 1.6 μs guard interval (GI2), followed by two long BPSK-OFDM training symbols (T1 and T2). The STF facilitates automatic gain control convergence and course frequency acquisition in the receiver. Subsequently, the LTF facilitates channel estimation and fine frequency acquisition.

Exploratory analysis reveals STF manipulation manifests greater utility for transceiver discrimination than the LTF. There are two primary reasons for this. First, the LTF is bounded by the preceding STF and successive packet data, fixing its length at 8 μs. Secondly, the LTF has only three components to be manipulated (G12, T1, T2) compared to ten in the STF. Therefore, this Letter focuses on STF length manipulation.

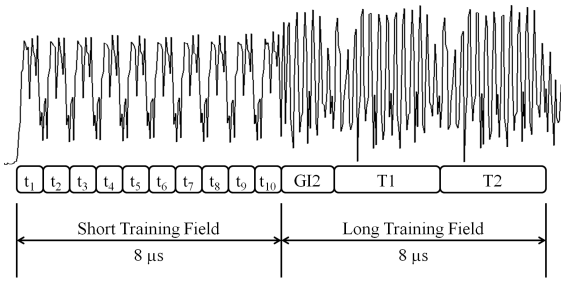

Fig. 1 *Magnitude plot of the first 16 μs of a standard IEEE 802.11a physical layer preamble as received by the USRP X310*

Experiment methodology: This experiment is designed to address the question of how preamble manipulations affect wireless packet reception by IEEE 802.11a and IEEE 802.11ac transceivers. This question is addressed by transmitting wireless packets with specific manipulations made to their preambles to six different transceiver types and observing the percentage of reception for each manipulation on each transceiver. Table 1 lists the six transceiver designs under test and their corresponding Device IDs (used for the remainder of this Letter). All six designs support IEEE 802.11a, while Dev1, Dev2, and Dev3 also support IEEE 802.11ac.

Multiple channels are available for IEEE 802.11a and IEEE 802.11ac transmissions in the 5 GHz band. IEEE 802.11a transmitters always use 20 MHz wide channels, while IEEE 802.11ac can use 40, 80, or (optional) 160 MHz wide channels. For this experiment the center frequency for IEEE 802.11a tests is 5785 MHz and the center frequency for the separate IEEE 802.11ac tests is 5795 MHz. Experiments involving IEEE 802.11ac are conducted using a 40 MHz configuration to make a clear distinction from IEEE 802.11a, while also being accessible to the CBX-40 daughterboard in the USRP X310 software-defined radio.

Experiment system configuration: The logical topology of the experiment setup is illustrated in Fig. 2. The Access Point is a Linksys WRT 1900AC, the laptop is a DELL Precision M4500, and the Desktop PC is a Dell Precision T7500 with 24 GB of RAM. The USRP X310 is controlled via GNU Radio on the Desktop PC, connected by a 10GBase SFP+ cable. A RAM drive is configured on the Desktop PC such that in phase and quadrature (I/Q) data streams from the Desktop PC to the USRP X310 without being read from a hard disk drive. Wireless packets with manipulated PHY preambles are transmitted from the USRP X310 to the transceivers under test, connected one at a time to the Laptop. The transceivers under test are wirelessly associated to the Access Point using the appropriate center frequency and spectral bandwidth during each test.

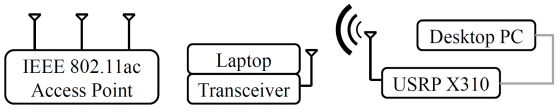

Fig. 2 *Logical topology of the experiment equipment*

Data collection procedure: Each of the six transceiver designs in Table 1 are investigated individually. Once the transceiver under test is associated to the Access Point, 300 ICMP echo requests with standard (non-manipulated) PHY preambles are transmitted from the USRP X310 to the transceiver at a rate of one per second. Percentage of packet reception is monitored using Wireshark on the Laptop. Once 100% packet reception is confirmed for standard packets, the preamble manipulation experiment begins. The 100% packet reception baseline is subsequently reconfirmed between each test to ensure that extraneous wireless interference is not a confounding influence.

For each of the preamble manipulations investigated, 300 ICMP echo requests with the given PHY manipulation are transmitted to the transceiver under test and the percentage of packet reception is monitored using Wireshark. The STF is shortened or lengthened by up to five symbols from the standard length of 10 ($length \in \{5, 6, ..., 15\}$) while the LTF remains standard. All tests are conducted at both high and low received signal strength conditions to investigate the consistency of the results across the operational range of the transceivers. The physical

Table 1: Six transceiver designs under test and device ID nomikers

Device ID	Adapter Type	Transceiver
Dev1	Linksys AE6000	MT7610U
Dev2	ASUS USB-AC53	BCM43526
Dev3	TP-LINK T4U	RTL8812AU
Dev4	Intel PRO 3945ABG	W62534RDE
Dev5	Cisco AIR-CB21AG-A-K9	AR5212
Dev6	Linksys WPC600N	BCM4328

distances between the laptop and USRP transmitter in Fig. 2 are 1 m (-28 dBm) and 38 m (-78 dBm), respectively. Even with a standard PHY, packet reception falls below 100% at distances beyond 38 m, causing intermittent network connectivity loss. Therefore, a maximum distance of 38 m is chosen for the experiment.

Observations of STF manipulation in IEEE 802.11a and IEEE 802.11ac: Table 2 and Table 3 report reception rates for the six transceivers under test while operating in IEEE 802.11a mode. Short STFs are examined in Table 2, long STFs are examined in Table 3, and the baseline standard length STF (l = 10) appears in both. Notably, the observed packet reception rates at -28 dBm and -78 dBm are statistically indistinguishable (99% CI, n = 300) for all scenarios examined. This is strong evidence for transceiver response consistency throughout the operational range of the devices. It is also clear from Table 2 and Table 3 that the reception differences among the six devices are sufficiently distinct as to be useful for message obfuscation and device fingerprinting. For example, only half of the devices (Dev1, Dev4 and Dev5) can receive packets with a longer-than-standard STF of l=14. Results are identical for Dev1, Dev2 and Dev3 operating in IEEE 802.11ac mode.

Transceiver fingerprinting proof of concept: In this scenario, the investigator can be a network auditor or an attacker. The investigator is unaware of the type of the transceiver within a wireless device operating in IEEE 802.11a or IEEE 802.11ac mode. By transmitting acknowledgment requests (e.g., ICMP echo requests) with varying preamble lengths, the pattern of replies and non-replies allows the investigator to accurately identify the unknown or unverified transceiver.

The classification decision tree in Fig. 3 is a proof-of-concept modeled after those in [4], for IEEE 802.11b, and [7], for IEEE 802.15.4. The tree is designed using fewest states (STF length) such that the number of required test packets at each step (n) is minimized. Furthermore, the probability of correctly identifying Dev4 (which requires observing a response during each of three steps) exceeds 99% (P = 99.26%).

The algorithm begins with the successful reception of an acknowledgment reply (standard PHY) from the device under test. Next, up to four test packets are transmitted to the device under test. Once a reply is observed in response to a PHY manipulated test packet, additional test packets at that decision step in the tree are not necessary. If a reply is observed in response to every test packet (following initial contact), the investigator determines the transceiver under test to be of type Dev4 (W62534RDE) using only three packets. Similarly, if all test packets after the initial response test go unanswered, the investigator can posit that the transceiver under test is of type Dev3 (RTL8812AU) with six packets (4 + 1 + 1 tries). This algorithm can be extended and improved as response patterns from additional transceiver designs are revealed. The only modification to Fig. 3 required for high packet loss scenarios is an arbitrarily greater number of tries at each decision step.

Table 2: Packet reception rates (n = 300) versus STF length ($length \in \{5, 6, ..., 10\}$) for the transceivers while operating in IEEE 802.11a mode. The dashes represent zero reception, for visual emphasis

		l = 5	l = 6	l = 7	l = 8	l = 9	l = 10
Dev1	-28 dBm	-	-	-	-	-	100%
	-78 dBm	-	-	-	-	-	100%
Dev2	-28 dBm	100%	100%	100%	100%	100%	100%
	-78 dBm	100%	100%	100%	100%	100%	100%
Dev3	-28 dBm	-	-	-	-	100%	100%
	-78 dBm	-	-	-	-	100%	100%
Dev4	-28 dBm	16%	21%	31%	68%	80%	100%
	-78 dBm	8%	17%	32%	72%	72%	100%
Dev5	-28 dBm	-	-	100%	100%	100%	100%
	-78 dBm	-	-	100%	100%	100%	100%
Dev6	-28 dBm	100%	100%	100%	100%	100%	100%
	-78 dBm	100%	100%	100%	100%	100%	100%

Table 3: Packet reception rates (n = 300) versus STF length ($length \in \{10, 11, ..., 15\}$) for the transceivers while operating in IEEE 802.11a mode. The dashes represent zero reception, for visual emphasis

		l = 10	l = 11	l = 12	l = 13	l = 14	l = 15
Dev1	-28 dBm	100%	100%	100%	100%	100%	100%
	-78 dBm	100%	100%	100%	100%	100%	100%
Dev2	-28 dBm	100%	100%	100%	100%	-	-
	-78 dBm	100%	100%	100%	100%	-	-
Dev3	-28 dBm	100%	100%	-	-	-	-
	-78 dBm	100%	100%	-	-	-	-
Dev4	-28 dBm	100%	100%	100%	100%	88%	70%
	-78 dBm	100%	100%	100%	100%	80%	60%
Dev5	-28 dBm	100%	100%	100%	100%	100%	-
	-78 dBm	100%	100%	100%	100%	100%	-
Dev6	-28 dBm	100%	100%	100%	-	-	-
	-78 dBm	100%	100%	100%	-	-	-

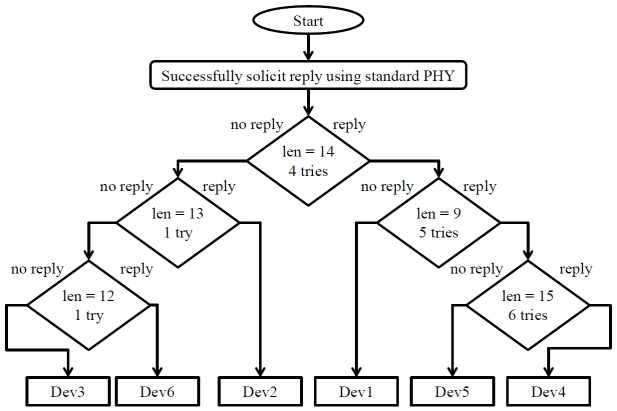

Fig. 3 *Example classification decision tree for IEEE 802.11a/ac transceivers*

Conclusion: The burgeoning research field of physical layer protocol manipulation leverages discoveries made about transceiver design idiosyncrasies. This Letter presents the first investigation of PHY manipulation on high data rate IEEE 802.11a and IEEE 802.11ac transceiver designs commonly found worldwide. It is discovered that the preamble STF length can be manipulated to discern among the six transceiver designs under test with greater than 99% accuracy. Design idiosyncrasies of real-world hardware cannot be determined through mathematical modeling or network simulation. Therefore, experiments must be conducted with as many transceiver and protocol designs as possible. Future work will explore additional technologies, from Z-Wave and Bluetooth low energy, to satellite communication protocols.

Acknowledgment: This work has been supported by Department of Homeland Security ICS-CERT Proposal 2016-008R.

B. Ramsey, J. Fuller and C. Badenhop (*Air Force Institute of Technology, WPAFB, USA.*)

E-mail: benjamin.ramsey@afit.edu

References

1 Valls, V., Leith, D.: 'Proportional fair MU-MIMO in 802.11 WLANs,' *IEEE Wireless Commun. Lett.*, 2014, **3**, (2), pp. 221–224
2 Aajami, M., Suk, J.: 'Optimal TXOP sharing in IEEE 802.11ac,' *IEEE Commun. Lett.*, 2015, **19**, (7), pp. 1141–1144
3 Milliken, J., Selis, V., Yap, K., *et al.*: 'Impact of metric selection on wireless deauthentication DoS attack performance,' *IEEE Wireless Commun. Lett.*, 2013, **2**, (5), pp. 571–574
4 Kulesza, N., Ramsey, B., Mullins, B.: 'Wireless intrusion detection through preamble manipulation'. Proc. Int. Conf. Cyber Warfare and Security, West Lafayette, USA, March 2014, pp. 132–139
5 Ramsey, B., Mullins, B.: 'Defensive rekeying strategies for physical-layer-monitored low-rate wireless personal area networks', in Butts, J. and Shenoi, S. (Eds.): 'Critical Infrastructure Protection VII' (Springer, Berlin, 2013, 1st edn.), pp. 63–79
6 Jenkins, I., Shapiro, R., Bratus, S., *et al.*: 'Speaking the local dialect: exploiting differences between IEEE 802.15.4 receivers with commodity radios for fingerprinting, targeted attacks, and WIDS evasion'. Proc. ACM Conf. Security and Privacy in Wireless and Mobile Networks, Oxford, UK, July 2014, pp. 63–68.
7 Ramsey, B., Mullins, B., Temple, M., *et al.*: 'Wireless intrusion detection and device fingerprinting through preamble manipulation,' *IEEE Trans. Dep. Secure Comput.*, 2015, **12**, (5), pp. 585–596