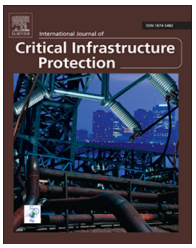
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Wireless infrastructure protection using low-cost radio frequency fingerprinting receivers

Benjamin W. Ramsey[a,*], *Tyler D. Stubbs*[a], *Barry E. Mullins*[a], *Michael A. Temple*[a], *Mark A. Buckner*[b]

[a]*Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, OH 45433, USA*

[b]*Radio Frequency Communications and Intelligent Systems Group, Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA*

ARTICLE INFO

Article history:
Received 19 March 2014
Accepted 30 November 2014
Available online 11 December 2014

Keywords:
Radio frequency fingerprinting
Physical layer security
WPAN
Spoofing
ZigBee Networks

ABSTRACT

Low-data-rate wireless networks incorporated in critical infrastructure applications can be protected through 128-bit encryption keys and address-based access control lists. However, these bit-level credentials are vulnerable to interception, extraction and spoofing using software tools available free of charge on the Internet. Recent research has demonstrated that wireless physical layer device fingerprinting can be used to defend against replay and spoofing attacks. However, radio frequency (RF) fingerprinting typically uses expensive signal collection systems; this is because fingerprinting wireless devices with low-cost receivers has been reported to have inconsistent accuracy. This paper demonstrates a robust radio frequency fingerprinting process that is consistently accurate with both high-end and low-cost receivers. Indeed, the results demonstrate that low-cost software-defined radios can be used to perform accurate radio frequency fingerprinting and to identify spoofing attacks in critical IEEE 802.15.4-based infrastructure networks such as ZigBee.

Published by Elsevier B.V.

1. Introduction

Low-cost, low-data-rate wireless connectivity is pervasive in critical infrastructure applications. IEEE 802.15.4-based wireless personal area networks (WPANs) operate in one-quarter of the surveyed wireless industrial control systems [1], communicate with tens of millions of smart meters [7] and are trusted components in numerous civilian and military healthcare facilities [12,21]. Security in such systems is often an afterthought, exposing critical WPANs to malicious attacks. A recent analysis of WPANs in ten U.S. cities revealed that healthcare and utility control networks operate with faulty security or none at all [17]. The threats to the critical infrastructure and other WPAN applications [15,20] are ever increasing as open source attack tools such as KillerBee [24] and Api-do [9] become more sophisticated.

WPAN security is challenging due to the cost, power and computational constraints levied on IEEE 802.15.4-based hardware. Secure, albeit computationally-intensive, intrusion detection algorithms have been developed for high-power networks, but they are impractical for WPAN applications. While network-layer encryption is a viable option for critical networks, attackers can readily extract keys from inexpensive WPAN hardware when tamper resistance is not a design priority [2,8].

A promising solution for securing WPANs without placing additional burden on end devices is radio frequency (RF) fingerprinting. In such a system, an "air monitor" passively observes WPAN packets and identifies message spoofing (e.g.,

*Corresponding author.
E-mail address: benjamin.ramsey@afit.edu (B.W. Ramsey).

http://dx.doi.org/10.1016/j.ijcip.2014.11.002
1874-5482/Published by Elsevier B.V.

packet replay attacks) through device-unique radio frequency fingerprints. Wireless device classification accuracy exceeding 99% has been demonstrated using high-end signal collection receivers (with per unit cost exceeding USD 50,000) that include a 4 Gsps oscilloscope [3], 8 Gsps oscilloscope [4], 50 Gsps oscilloscope [16], a 95 Gsps Agilent E3238S signal intercept system [5,19], and an Agilent PSA E4448A spectrum analyzer combined with a 4Gsps oscilloscope [22]. The high cost of these signal receivers prohibits their use in practical radio frequency fingerprinting systems. Thus, techniques developed using high-end receivers must be successfully transitioned to low-cost (less than USD 2000) hardware such as universal software radio peripheral (USRP) receivers. Transient-based fingerprinting requires at least 4 Gsps [3,4], which is not possible with USRP receivers that have a 25 Msps limit. However, spectral fingerprinting using wireless preambles has recently been demonstrated with USRP receivers [22,23]. Initial results suggest lower device differentiation accuracy and higher receiver-specific variability with USRP receivers than with high-end receivers.

Inexpensive analog components in low-end receivers introduce noise and variability during signal reception and confound the radio frequency fingerprinting process. While some distortion is unavoidable, the underlying hypothesis in this paper is that the variability in collection center frequency and environmental noise can be mitigated through post-collection signal processing. This paper demonstrates signal processing techniques that mitigate the radio frequency fingerprinting limitations of low-cost receivers. A key experiment described in this paper employed two radio frequency receivers (a high-end National Instruments (NI) PXIe-1085 system and a low-cost NI USRP-2921 system) under identical signal collection conditions to simultaneously collect device emissions. The results demonstrate accurate device spoofing identification in scenarios involving real-world attack hardware and smart meters.

2. Radio frequency fingerprinting

The earliest radio frequency fingerprinting systems were developed by militaries to differentiate between friendly and hostile radar transmissions [11]. The costs associated with radio frequency fingerprinting have declined over the last past decades to such a degree that commercial cell phone companies often use radio frequency fingerprinting to detect device cloning [13]. In order to be commercially viable, the radio frequency fingerprinting of low-cost WPANs in critical infrastructure applications must be practical and must leverage inexpensive, small-form-factor receiver technologies.

Ur Rehman et al. [22,23] were among the first to attempt robust radio frequency fingerprinting using low-cost USRP receivers. Their fingerprints consist solely of power spectral density (PSD) features of IEEE 802.11a (5 GHz WiFi) preambles. IEEE 802.15.4 based WPANs (e.g., ZigBee) also feature a preamble at the start of every burst transmission that is amenable to radio frequency fingerprinting. However, recent work with high-end receivers [19] reports that radio frequency fingerprints based solely on power spectral density features underperform those based on time-domain features. The fundamental hypothesis is this paper is that radio frequency fingerprinting performance using USRP receivers can match the performance of high-end receivers with proper feature selection and robust processing.

Instead of using power spectral density features, a series of instantaneous time-domain features is used to enhance the relative fingerprinting accuracy of USRP receivers. The robust radio frequency fingerprinting methodology is presented in Section 4.

3. WPAN threat scenarios

The open source zbassocflood tool included with KillerBee [24] enables attackers to generate fake network address requests from numerous spoofed WPAN source MAC (medium access control) addresses. These requests consume the finite pool of network addresses of higher-layer WPAN protocols such as ZigBee, causing denial-of-service attacks against legitimate devices that request access.

The standard bit-level defense against such attacks is to distribute MAC address filtering throughout a network. Access lists require time-consuming administrator management and increased memory usage on already-limited WPAN hardware. In any case, these measures are ineffective if the spoofed MAC addresses are the same as those belonging to authorized devices. A list of valid in-use MAC addresses on a network is readily found by recording nearby traffic using the zbdump tool in KillerBee or by evesdropping with a Microchip ZENA wireless adapter. Route poisoning, fake leave requests and other disruptive packets can be made to appear from valid source MAC addresses. Fortunately, the radio frequency fingerprints of attacker transmissions do not closely match those of legitimate devices. Thus, they would be identified as being fake by air monitors – routers would then reject the traffic based on air monitor feedback and warnings would be sent to system administrators that an attack is underway.

Replay attacks can also be used to disrupt WPANs. The zbreplay tool in KillerBee makes it relatively easy to conduct replay attacks. For example, an attacker could observe a WPAN-based security or control system for activity that could be replicated later (e.g., to unlock a door or open a utility valve). In such an attack, WPAN traffic that initiates the action of interest is recorded and replayed at will. The ZigBee WPAN specification does not mandate sequence number checks [19] to prevent these attacks. Even if the 8-bit ZigBee sequence field is verified by the targeted network, successful replay attacks are possible after every 255 valid frames. As with the spoofing attacks described above, the radio frequency fingerprint of the message replays would reveal that they originated from an unauthorized device. The replayed messages would be rejected and warnings would be sent to system administrators.

WPAN device localization for network auditing and cyber situational awareness are active areas of research. Inexpensive open source tools [14,18] may be used by system administrators to track down attacker hardware.

4. Radio frequency fingerprinting methodology

Since the USRP sampling rate is insufficient for transient-based radio frequency fingerprinting [3,4] and recent research