Computer Communications 55 (2015) 102–111

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Demodulation-free protocol identification in heterogeneous wireless networks ☆

Aijing Li [a], Chao Dong [a], Shaojie Tang [b], Fan Wu [c], Chang Tian [a,*], Bingyang Tao [c], Hai Wang [a]

[a] College of Communications Engineering, PLA University of Science and Technology, China
[b] Department of Information Systems, University of Texas at Dallas, TX, USA
[c] Department of Computer Science and Engineering, Shanghai Jiao Tong University, China

ARTICLE INFO

Article history:
Received 3 July 2014
Received in revised form 20 August 2014
Accepted 24 August 2014
Available online 1 September 2014

Keywords:
Protocol identification
Without demodulation
Heterogenous networks
USRP

ABSTRACT

Nowadays various wireless network protocols play respective roles to fulfill different demands. To better adapt to this heterogeneity and coexistence situation, it is critical for nodes to identify the available networks with high accuracy and low cost. Unlike traditional demodulation-based identification method, which is expensive and complexing, in this paper, we propose a novel conception called demodulation-free protocol identification. This method only employs the features of physical layer samples. We first extract features that can be used to identify different protocols. Specifically, a sparse sequence based Precision-Stable Folding Algorithm (PSFA) is proposed to detect periodicity feature, which is common in wireless network protocols. Then we construct a prototype with USRP to identify three commonly used protocols in the 2.4 GHz ISM band. Experiment results show that under low or moderate channel utilization, the accuracy is above 90%. We also show that the computational complexity is polynomial.

1. Introduction

The coexistence of heterogeneous networks has become a prominent trend, since various wireless network protocols play respective roles to fulfill different demands. In addition, most of the channels in these networks are overlapping with each other [1]. Take the city shown in Fig. 1 as an example. Wireless Sensor Networks (WSNs) are deployed in hospitals, forests, and roads for data collecting, e.g. CO_2, temperature, pollution, etc., while WiFi hotspots are deployed to provide Internet access in restaurants and campus. In addition, Wireless Personal Area Networks (WPANs) are used for short-distance communications, like smart home networks. In this context, to enhance coexistence and heterogeneity, it is essential for nodes to have a preliminary view of the wireless networks in current region. Therefore, *accurate and low-cost protocol identification* is playing an important role for quick media access and interoperability.

Traditional protocol identification schemes are demodulation-based. By demodulation and decoding received packets [2–5], the used protocols can be recognized. This requires nodes to implement all possible network protocol waveforms. The cost is high since physical layer (PHY) and most media access control (MAC) functions are implemented in hardware or firmware. Though Software Defined Radio (SDR) [6] can implement all possible waveforms in software and reduce the cost, nodes still need to load and try each waveform one by one [7]. Besides, packet decoding is not always feasible in practical circumstances, especially under war conditions. Various information technologies (e.g., information encryption) and electromagnetic interference (EMI) will be employed in future high-tech wars. In this situation, the SNR of received signals may drop to a level which cannot satisfy the demodulation requirement.

For above reasons, we are motivated to seek a less expensive protocol identification method, which can use PHY signals only and be demodulation-free. As we know, the current networks are based on a layered architecture, which results in the information scarcity of upper layer protocols when working with only PHY signals. Fortunately, protocol level behavior can be reflected to PHY signals, which leaves us a chance to infer upper-layer protocols through RF analysis. Its advantages are as follows:

- It can reduce the implementation cost. As only PHY signal features are used to recognize different protocols, there is no need to try each demodulation scheme, or implement the whole protocol stack of each potential protocol. This can greatly reduce the implementation complexity and financial cost.

☆ A preliminary version of this paper appeared in IEEE WCNC 2012, April 1–4, Paris, France.

* Corresponding author. Address: Box 110, 2 Biaoying, Yudao Street, Nanjing 210007, China.

E-mail address: tianchang126@126.com (C. Tian).

http://dx.doi.org/10.1016/j.comcom.2014.08.014
0140-3664/© 2014 Elsevier B.V. All rights reserved.

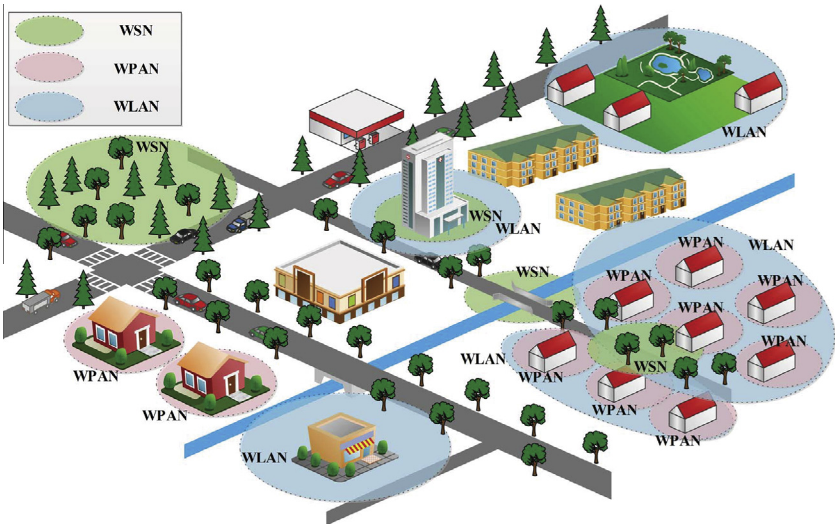

Fig. 1. Heterogeneous wireless networks in a city.

- It can reduce the computational cost. Compared with traditional identification approaches, some signal processing modules are not necessary, such as frequency offset compensation, phase offset compensation, and timing recovery. This reduces the computational complexity.
- It can be used in situations where reliable decoding is not feasible. For example, when scanning with omnidirectional antenna, the received SNR may be low for demodulation. We can first detect the existence of signals without demodulation. Then with beamforming and the direction of arrival estimation, received SNR can be strengthened and interested signals may be able to be demodulated.

Despite of the advantages, it may be more challengeable to consider raw PHY layer samples. Due to the layered architecture of networks, different layers work independently. Thus characterizing different signals and classifying them with these features can be difficult with original PHY layer samples.

Following the above idea, we propose a new conception called *demodulation-free protocol identification*, which only relies on PHY information. The key contributions of this paper can be summarized as follows:

- We propose the conception of demodulation-free protocol identification. It only employs features of PHY samples. This approach can be embedded into intelligent devices for network identification before media access, and provide interoperability across heterogeneous platforms.
- We investigate and extract the features of PHY signals that can be used to identify different wireless protocols. We analyze different signal features in both time domain and frequency domain. Specifically, a sparse sequence based Precision-Stable Folding Algorithm (PSFA) is proposed to detect the periodicity feature, which is common in wireless protocols [3,4].
- Taking three commonly used wireless protocols as an example, we construct a system design with USRP [8] to validate the feasibility and performance of the proposed conception. Experiments show that under low or moderate channel utilization ratio, the detection accuracy is above 90% for both single and multiple APs. We also show that the computational complexity is polynomial.

The remainder of this paper is organized as follows. Section 2 presents a review of related works. In Section 3, we investigate the features of different signals in both time domain and frequency domain. Section 4 describes the design and implementation of the identification system. The experimental results are shown in Section 5. Finally, Section 6 concludes the paper and presents future work.

2. Related works

Most of the protocol identification schemes are demodulation-based. By decoding and extracting information carried in the headers, we can obtain the necessary knowledge of the protocols used in each layer of the protocol stack. Protocol identification can be achieved either in an active or in a passive way. We introduce the two methods in the rest of this section.

2.1. Active protocol identification

Some of the existing systems solve the protocol identification problem by broadcasting active probing, for example, the beacon messages in most wireless protocols [3,4]. Kanuparthy et al. [9] investigate a user-level probing approach to detect and diagnose 802.11 pathologies. By introducing a probing server and probing client, detection and diagnosis can be done without any information from 802.11 devices and other link layer monitors. But this work is limited to only WiFi networks. Konark [10] is a service discovery and delivery protocol in Ad Hoc networks. Each device acts as a server and a client simultaneously. Clients use a discovery process known as active pull mechanism. Servers use an advertisement process to periodically announce their registered services. Then service can be discovered and delivered by pulling and advertising. Without a doubt, the broadcasting messages may introduce extra overhead to the network, which implies fewer transmitting opportunities for data packets and performance deterioration. Therefore, for the sake of performance, passive detection is preferable.

2.2. Passive protocol identification

The concept of Cognitive Gateway (CG) was proposed to promote interoperability across heterogeneous communication systems [11]. CGs can successfully classify four different types of wireless signals and provide corresponding communication services. The core design of CG is a Universal Classification Synchronization