Computer Networks 86 (2015) 40–56

Contents lists available at ScienceDirect

Computer Networks

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

A novel cheater and jammer detection scheme for IEEE 802.11-based wireless LANs

Eduard Garcia-Villegas*, Muhammad Shahwaiz Afaqui, Elena Lopez-Aguilera

Wireless Networks Group (WNG)—Telematics Department, Universitat Politecnica de Catalunya (UPC)—i2CAT Foundation, 08860 Castelldefels, Barcelona, Spain

ARTICLE INFO

Article history:
Received 11 July 2014
Revised 27 December 2014
Accepted 2 May 2015
Available online 18 May 2015

Keywords:
IEEE 802.11
WLAN
Jamming
Cheater
Security

ABSTRACT

The proliferation of IEEE 802.11 networks has made them an easy and attractive target for malicious devices/adversaries which intend to misuse the available network. In this paper, we introduce a novel malicious entity detection method for IEEE 802.11 networks. We propose a new metric, the Beacon Access Time (BAT), which is employed in the detection process and inherits its characteristics from the fact that beacon frames are always given preference in IEEE 802.11 networks. An analytical model to define the aforementioned metric is presented and evaluated with experiments and simulations. Furthermore, we evaluate the adversary detection capabilities of our scheme by means of simulations and experiments over a real testbed. The simulation and experimental results indicate consistency and both are found to follow the trends indicated in the analytical model. Measurement results indicate that our scheme is able to correctly detect a malicious entity at a distance of, at least, 120 m. Analytical, simulation and experimental results signify the validity of our scheme and highlight the fact that our scheme is both efficient and successful in detecting an adversary (either a jammer or a cheating device). As a proof of concept, we developed an application that when deployed at the IEEE 802.11 Access Point, is able to effectively detect an adversary.

1. Introduction

Wireless Local Area Networks (WLANs) occupy different sections of the 2.4 and 5 GHz Industrial, Scientific and Medical (ISM) radio bands. ISM bands can be used freely at low transmission power without license, making them a very attractive alternative for building domestic wireless communications systems. This is both one of the keys for the success of Wi-Fi based WLANs, and the source of many interference issues affecting the operation of a WLAN. In recent years, growth in IEEE 802.11 WLAN technology has drastically increased due to its ease of deployment, convenience and cost efficiency. The IEEE 802.11 protocols were designed with the assumption that all the nodes that want to communicate, would follow specific predefined rule of engagement to transmit and receive data. These were not designed to withstand adversaries attacks intended to interrupt the transmission. The success of IEEE 802.11 has attracted more and more users to employ these networks, while increasing the potentials for attackers to operate.

With time, the wireless attacks on IEEE 802.11 have become more sophisticated and are evolving to counter every new development made in these networks. The most prominent of these attacks are layer-1 attacks which are seldom considered a threat because they are typically generated from non-Wi-Fi devices sharing the same ISM bands such as micro wave ovens, cordless phones, etc. These non-Wi-Fi devices, when located within a WLAN's coverage area, unintentionally radiate unwanted energy that can affect the whole

* Corresponding author. Tel.: +34 93 413 71 20; fax: +34 93 413 70 07.
E-mail address: eduardg@entel.upc.edu, eduardg@mat.upc.edu (E. Garcia-Villegas).

http://dx.doi.org/10.1016/j.comnet.2015.05.003
1389-1286/

network. Furthermore, most of the people are not familiar with the interference abilities of such devices and the people who are familiar do not have the control over their placement.

These attacks are further aggravated when done purposefully. An attacker/adversary with the intent to disrupt the network can use low-priced and readily accessible RF jammers. Such attacks can appear to be simple in nature but can have devastating consequences for corporate companies since those security breaches can break down the core communication line within a company (e.g. critical voice over Wi-Fi communication lines which require continuous Wi-Fi connection and email services) that can result in reduced productivity. The ease to attack IEEE 802.11 networks is indicated by Fragkiadakis et al. [1] where the authors demonstrate the use of off-the shelf hardware that can be used to severely disrupt the network.

In [2], Xu et al. define an adversary as a *jammer to be an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications*. For the sake of simplicity and keeping in mind the adverse effects caused by non-Wi-Fi devices, we consider them also to be acting as jammers.

The jammer spreads energy over the targeted spectrum, where it becomes difficult to extract the desired signal from interfering signals. Furthermore, due to Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) based channel access, the Wi-Fi networks become an easy target by these adversaries, where a jammer can even utilize low power to disrupt the network. IEEE 802.11 standard [3] provides different operating modes: Distributed Coordination Function (DCF), Point Coordination Function (PCF), Hybrid Coordination Function (HCF) with HCF Distributed (EDCA) and Controlled Channel Access (HCCA). The DCF is the mode currently employed in most deployments and uses CSMA/CA contention-based MAC algorithm. In this case, before initiating a transmission, a station senses the channel to determine whether it is busy during a period of time called the Distributed Inter-frame Space (DIFS). If the medium is sensed busy, the transmission is delayed until the channel is idle again, and a slotted binary exponential backoff interval is chosen in the range [0, CW-1], where CW is the contention window. The value of CW is set to its minimum value, CW_{min}, in the first transmission attempt and increases in integer powers of 2 at each retransmission, up to a pre-determined value CW_{max}. For each data frame successfully received, the receiver transmits an ACK frame after a Short Inter-frame Space (SIFS) period. The protocol described above is called the basic or two-way handshake mechanism. In addition, the specification also contains a four-way frame exchange protocol known as the RTS/CTS (Request to Send/Clear to Send) mechanism.

Due to CSMA/CA characteristics, this contention-based MAC mechanism is very sensitive to Denial of Service (DoS) attacks based on jamming techniques. This kind of attacks consists in the transmission of a powerful signal in the frequency band employed by IEEE 802.11 devices. Thus, the medium is always sensed busy during the jammer signal by IEEE 802.11 clients. Obviously, jammer influence will lead to very harmful effects in MAC protocol performance. Jamming attack in IEEE 802.11 can prevent the nodes to perform legitimate MAC operations or can cause the collision of frames that force repeated backoff which can even jam the complete transmission process. The jamming signal interferes and corrupts the desired signal in reception, while causing the co-channel transmitters to reschedule the transmission for longer period of time. Different factors are incorporated in the effectiveness of interference that a jammer creates namely distance between a jammer and a wireless device, transmission power of jammer and the network devices, and the MAC protocol used within the network.

Different attack strategies can be employed by a jammer while trying to interfere with other communicating nodes. In [2], the authors have differentiated jammers based on their attack model. They have defined four types of jammers namely constant jammers, deceptive jammers, random jammers and reactive jammers. According to the authors, a constant jammer continues to transmit radio signal without following any MAC layer protocol, a deceptive jammer continuously transmits regular frames without any gap, thus deceiving other communicating nodes to believe that a legitimate transmission is occurring, a random jammer that transmits for a time and goes to sleep, where both the transmission time and the sleep time can be random, and a reactive jammer that starts transmitting jamming signals as soon as it detects activity on the shared medium and goes to sleep when there is no one transmitting.

An intelligent jammer can also exploit the standard DCF that is used to coordinate nodes for medium access within IEEE 802.11. In [4] Pelechrinis et al. define intelligent jamming models and methods used to jam IEEE 802.11 networks. In [5], the authors investigate the fabricated CTS attack to the MAC scheme of IEEE 802.11 and propose a mechanism to prevent such attack. This attack is based on a jammer acquiring the use of shared channel by transmitting a fabricated CTS signal, which contains large Network Allocation Vector (NAV) to falsely defer transmissions from other users for longer duration.

A jammer can also be a cheating device that misuses the IEEE 802.11 MAC constraints in order to attain bandwidth gains. This device can have the ability to choose Clear Channel Assessment (CCA) threshold, backoff window size and/or inter-frame space. By increasing the CCA threshold, the cheating device can improve its opportunity to transmit and thus can effectively disable channel sensing. It can continue to transmit over the medium, while causing other transmitting stations (STA) to undergo collisions and thus backoff from transmitting. The cheating device can also observe collision but the backoff period is kept shorter (is not frozen because carrier sensing is already disabled). The authors in [6] extensively explain how a selfish station with higher CCA can experience bandwidth gains. Similar bandwidth advantages can also be achieved by utilizing a smaller contention window, which helps the cheating node to backoff for smaller periods than average, when collisions occur. The cheating device can also maneuver to cheat the IEEE 802.11 MAC constraint by reducing its DIFS. By reducing the DIFS, the cheating station can gain quick access to the medium, thus depriving other stations from their fair share.

Therefore, finding solutions to eliminate jamming is very important in IEEE 802.11 networks. This solution can only be found by first enabling the network to detect the