Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: April 11, 2019

Southeast University

October 8, 2018

Authentication by Physical Layer Features
draft-linning-authentication-physical-layer-00

Abstract

This document proposes an authentication method using physical layer features from terminal unit. This document assumes that the reader is familiar with some concepts and details regarding physical layer security.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The classical device authentication method includes MAC address, pre-shared key or digital certificate. However, the MAC address is easy to be imitated, which can hardly ensure the security. The security of the pre-shared key and digital certificate is mainly due to the strength of the digital key and authentication algorithms.

Physical layer feature based device identification provides a physical layer security protection for networks. Utilizing the inherent physical layer feature of terminal unit, it is possible to realize identity authentication via only the received waveform.

It has been demonstrated that physical layer feature owns uniqueness and persistence, which could be used for terminal unit identification. The physical layer feature could be obtained via transient feature extraction, spectrum feature extraction or modulation feature extraction. [Ref_1] After that, gateway could identify the identity of the terminal unit via the received signal waveforms by identification algorithms.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Applicability

This mechanism authenticates the identity of the terminal unit by physical layer features, which is suitable for wireless, wired and optical networks.

When network node transmits message to other network nodes, the binary message is transformed to analogical signal in physical layer. This physical layer signal includes the unique physical layer feature of the transmitter. The receiver utilizes the physical layer features from the transmitter signal.

The steps are listed below:

2.1. Physical layer feature extraction

The physical layer feature extraction methods can be generally summarized into three categories, namely transient-based method, spectrum-based method, and modulation-based method. [Ref_1] The obtained physical layer features are digitalized to a feature vector, which is used for authentication.

2.2. Physical Layer Feature based Authentication

The gateway uses the extracted physical layer features to authenticate the accessing terminal device.

3. Physical Layer Feature Extraction

The physical layer features include transient-based feature, spectrum-based feature, and modulation-based feature.

The transient-based method measures the turn-on/off transient or transmitting signal variations for device identification. These features are extracted by measuring the envelope of the transient signal. Signal processing methods such as principal component analysis (PCA) and discrete Fourier transform (DFT) are employed for further feature process. In addition, statistical methods are also used for transient-based feature extraction. The standard deviation, variance, skewness and kurtosis of the transient amplitude, phase and frequency are extracted for physical layer features. A vector of these features are directly employed for authentication.[Ref_1][Ref_2]

Signal spectrum is another important physical layer feature. The power spectrum density (PSD) is directly extracted from the samples of the receiver signal. In general, the non-linearity behavior of the device transmitter is the main source of the signal spectrum feature. The signal spectrum feature can be quantified by selecting several significant regions at PSD. The in-band outline and out-of-band outline of PSD is another important physical layer feature for authentication. [Ref_1]

Modulation-based methods extract stable features from the received signal, including auto gain control (AGC) responds, amplifier nonlinearity characteristics, sampling frequency offset, carrier frequency offset, differential constellation trace figure (DCTF) and so on. These modulation-based features can be extracted in the baseband by specific methods. [Ref_3]

The extracted physical layer features are grouped into a feature vector. This feature vector is further used for authentication.

4. Physical Layer Feature based Authentication

In physical layer feature based authentication, the gateway has two process, including a training process and decision process. In training process, the system works in a secure connection. The identity of the accessing device is true and known at gateway. The gateway capture the physical layer signal and extract the physical layer feature. The obtained physical layer feature is stored in database for decision process in authentication. In decision process, the system works in an open network. Gateway receives the signal of accessing terminal device. Gateway authenticate the identity of the terminal using the stored features in database.

In terminal identity authentication problem, the gateway is faced with two situations. The first situation is that the identity of the terminal device has been registered before, the terminal device declare its identity in its accessing. In this case, gateway compare the extracted physical layer feature to the feature vector stored in the database. The result of the comparison is a degree of similarity between the accessing terminal device and legitimate device. Gateway confirm the identity of the accessing terminal device when the degree of similarity is higher than a threshold. If the identity of the accessing terminal device is legitimate, gateway opens the connection of the terminal device to the internal network. The second situation is that the identity of the terminal device has not been registered before. In this case, gateway also extracts the physical layer feature of the accessing terminal device. The gateway compare the extracted feature to all of the feature vectors stored in the database. A final result of degree of similarities between the accessing terminal device and stored features is obtained. Gateway confirm the new identity of the accessing terminal device when all of degree of similarities are lower than a threshold. Gateway close the connection of the terminal device to the internal network.

5. Example

An application example is introduced as follows:

The authentication by physical layer feature system includes four elements: terminal unit, physical layer feature extraction unit, internal network unit and accessing control unit. The terminal unit is connected to the physical layer feature extraction unit and accessing control unit. The physical layer feature extraction unit is connected to the accessing control unit. The internal network unit is connected to the accessing control unit. The signal is transmitted from terminal unit to physical layer feature extraction unit. The signal is also transmitted from physical layer feature extraction unit to accessing control unit. The terminal unit and accessing control unit have mutual signal exchange. The internal network unit and accessing control unit also have mutual signal exchange.

The physical layer feature extraction unit includes three components: front-end signal capture device and processor. The processor extracts the physical layer feature using the capture signal from front-end signal capture device. The accessing control unit includes two components: storage and processor. The processor authenticates the accessing terminal device using the physical layer feature. The authentication rule and identity information are stored in the database of storage. The extracted physical layer feature is also stored in the database of storage.

In training process, physical layer feature extraction unit initially obtains physical layer feature and transmits the physical layer feature to accessing control unit. Accessing control unit binds the physical layer feature to the identity of terminal device. The physical layer feature of the trained device is stored in database at accessing control unit.

In decision process, physical layer feature extraction unit captures the signal of accessing terminal device. Physical layer feature extraction unit further extracts the physical layer feature from the captured signal. Physical layer feature extraction unit transfers the physical layer feature to accessing control unit. In decision process, the authentication has two situations. In the first situation, the identity of the terminal device has been registered before in the database. The terminal device declares his identify when it accesses the network. The accessing control unit compares the extracted physical layer feature to the stored physical layer feature in the database with the declared index. This comparison gets a result of degree of similarity. If this degree of similarity is higher than a threshold, accessing control unit confirms the identity of the device and opens the connection of terminal unit to the internal network unit. If this degree of similarity is lower than a threshold, accessing control unit rejects the access of the device and closes the connection of terminal unit to the internal network unit. In the second situation, the identity of the terminal device has not been registered before in the database. The terminal device does not declare his identify when it accesses the network. The accessing control unit compares the extracted physical layer feature to all of the stored physical layer feature in the database. This comparison gets a result of highest value of degree of similarity. If the highest value of degree of similarity is lower than a threshold, the accessing control unit confirms the new identity of the accessing terminal device and closes the connection of terminal unit to the internal network unit. If the highest value of degree of similarity is higher than a threshold, the accessing control unit requires other authentication method to confirm the identity of the terminal device.

6. IANA Considerations

This document includes no request to IANA.

7. Security Considerations

This section will address only security considerations associated with the use of physical layer features for authentications. The similarity of physical layer features between different devices is relied on the consistency of physical devices, measurement accuracy of the gateway. If the gateway cannot distinguish the physical layer features between different devices, authentication methods in higher layer is required.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

8.2. Informative References

[Ref_1] Danev, Boris., "https://dl.acm.org/citation.cfm?id=2379782", 2012.

[Ref_2] J.Carbino , Timothy., "https://ieeexplore.ieee.org/document/7069371/", 2015.

[Ref_3] Peng, Linning., "https://ieeexplore.ieee.org/document/7752534/", 2016.

Authors’ Addresses

Linning Peng
Southeast University
No.2 SiPaiLou
NanJing, JiangSu 210096
China

Phone: +86 25 52091692
Email: pengln@seu.edu.cn

Aiqun Hu
Southeast University
No.2 SiPaiLou
NanJing, JiangSu 210096
China

Phone: +86 25 52091692
Email: aqhu@seu.edu.cn