ONDAS NETWORKS

IEEE 802.16t Direct Peer-to-Peer (DPP) Authentication

March 7th, 2025

Ondas Networks Inc. | 920 Stewart Drive, Sunnyvale, CA 94085 | (888) 350-9994 | **ondas.com**

Introduction

Trust, integrity, and reliability are essential in Railroads communication systems. The 802.16t Direct Point-to-Point (DPP) standard delivers these essential qualities, offering a robust and standards-based authentication solution for narrow-channel wireless environments. IEEE802.16t DPP authentication framework, leverages proven cryptographic methods. It supports both online and offline modes, adapting to diverse network infrastructures. This document, describes the core principles, operational mechanisms, and key advantages of the 802.16t DPP authentication process, highlighting its ability to maintain wireless security in critical applications through adherence to established security standards.

Challenges in Wireless Authentication

The proliferation of low-bandwidth IoT devices across critical infrastructure sectors like government, oil and gas, transportation, and utilities presents unique security challenges. These environments demand robust authentication mechanisms that can operate efficiently within constrained resources while maintaining uncompromising security. Key challenges include:

- **Resource Constraints:** IoT devices often have limited processing power, memory, and battery life. Traditional authentication protocols can be computationally intensive, leading to performance bottlenecks and accelerated battery drain.
- **Harsh Environments:** Many deployments occur in remote or challenging environments where network connectivity is intermittent or unreliable. This necessitates authentication solutions that can operate effectively in offline or degraded network conditions.
- **High-Value Assets:** The data and control systems within these sectors often manage high-value assets and critical infrastructure. Unauthorized access or data manipulation can have severe consequences, requiring stringent security measures.
- **Scalability and Management:** Deployments can involve a large number of devices distributed across vast geographical areas. Efficient key management and certificate distribution are essential for maintaining security at scale.
- **Long Lifecycles:** Many critical infrastructure devices have long operational lifecycles, requiring authentication solutions that can remain secure against evolving threats over extended periods.

- **Narrow Bandwidth Limitations:** Many of these devices rely on very narrow bandwidth connections. This limitation forces the authentication process to be as efficient as possible.

The 802.16t DPP standard is designed to address these challenges, providing a secure authentication framework tailored for the unique requirements of low-bandwidth IoT deployments in critical infrastructure.

Authentication Framework Overview

The 802.16t DPP authentication framework is specifically engineered for secure communication in narrow-channel wireless environments, particularly for low-bandwidth IoT devices in critical infrastructure. Operating after the initial device pairing, it establishes a secure link through robust authentication, supporting both online and offline modes to accommodate diverse deployment scenarios.

Online Authentication: When a reliable backbone network is available, 802.16t DPP facilitates mutual authentication via an external Certificate Authority (CA). This centralized approach ensures rigorous validation through a trusted entity, enhancing security in environments with consistent network connectivity.

Offline Authentication: In scenarios where a backbone network is absent or unreliable, 802.16t DPP enables direct device-to-device authentication. This mode relies on pre-distributed certificates or shared cryptographic materials, ensuring secure verification even in disconnected environments.

DTLS 1.3 for Robust Security: At the core of the 802.16t DPP authentication framework is Datagram Transport Layer Security (DTLS) 1.3, an adaptation of TLS optimized for unreliable networks. DTLS 1.3 adheres to FIPS 180-4 requirements, incorporating secure cryptographic hash functions, digital signatures, and message authentication mechanisms for comprehensive cryptographic integrity. Its optimized handshake process reduces latency and enhances key derivation efficiency, making it ideal for the resource-constrained nature of 802.16t DPP.

DTLS 1.3 offers flexibility through support for multiple cryptographic algorithms, including AES-GCM, ChaCha20-Poly1305, HMAC-SHA256, and elliptic curve digital signature algorithms (ECDSA and EdDSA). This allows for tailoring security measures to specific system requirements while ensuring compliance with industry standards.

Encryption and Message Authentication: The 802.16t DPP standard supports robust encryption, including AES-256, to ensure confidentiality in sensitive communications. However, recognizing the resource constraints inherent in many low-bandwidth IoT deployments, the framework also allows for configurations that prioritize message authentication (HMAC). To further enhance message integrity, the framework supports

configurable HMAC lengths up to 256 bytes, allowing for adjustments based on the desired security level. In situations where processing power or bandwidth is limited, relying heavily on HMAC provides essential data integrity and authentication with minimal overhead. This flexibility enables optimal security configurations based on the specific needs of each application, balancing strong encryption with efficient resource utilization. The 802.16t DPP authentication framework utilizes DTLS 1.3 to ensure compliance with FIPS 180-4 and other security standards through the use of approved cryptographic algorithms. This framework provides:

- **Secure Key Exchange:** Utilizes robust cryptographic methods, including the Ephemeral Diffie-Hellman (EDH) cipher suite, for secure session initiation.
- **X.509 Certificate-Based Authentication:** Verifies device identities using a trusted certification process and ensures secure key exchanges through cryptographic validation.
- **Resilience to Packet Loss:** Ensures reliable authentication in lossy wireless environments.

Authentication Message Exchange

The authentication process consists of the following steps:

1. **Pairing Phase.** Devices perform an initial pairing, exchanging identification parameters.
2. **DTLS Handshake Process.** The initiating device sends a **Client Hello** message containing:
    - Supported cipher suites
    - Session parameters
    - Random values for key derivation
    - The responding device replies with a **Server Hello**, providing its certificate and supported security parameters.
3. **Mutual Authentication**
    - Devices exchange **Certificate Verify** messages to confirm their authenticity.
    - A **Finished** message is sent by both parties to finalize session establishment.
4. **Secure Communication.** After successful authentication, DTLS ensures integrity protection for all subsequent data transmissions and offers encryption

as an optional feature, allowing customers to prioritize message authentication (HMAC) for performance optimization.

Security Measures

To enhance authentication security, the system incorporates:

- **Optional Encryption:** Encryption is available as a configurable option but is not mandated, allowing flexibility based on customer requirements.
- **Certificate Expiration Handling:** Ensuring certificates are properly validated and revoked as needed, without mandatory session expiry enforcement.
- **Message Integrity:** Ensuring data integrity through cryptographic hashing and HMAC verification, including a 64-byte HMAC message authentication requirement during the handshake.

Conclusion

The 802.16t DPP authentication framework offers a compelling solution for securing low-bandwidth IoT deployments in critical infrastructure sectors. By combining robust, standards-based cryptographic techniques with the flexibility to adapt to diverse operational environments, 802.16t DPP ensures secure and reliable communication even in resource-constrained and challenging conditions. Its support for both online and offline authentication, coupled with efficient DTLS 1.3 implementation, enables organizations to confidently deploy and manage secure wireless networks across a range of critical applications.

The 802.16t DPP standard empowers industries such as government, oil and gas, transportation, and utilities to protect their high-value assets and critical infrastructure from evolving cyber threats. Its ability to balance strong security with efficient resource utilization makes it an ideal choice for securing the rapidly expanding landscape of low-bandwidth IoT devices.

NGHE Communication Overview

1. Communication between a radio in the locomotive referred to as “Head of Train” or HOT and a radio mounted at the end of the last car of the train and is referred to as “End of Train” or EOT, is used for safety purposes. A major function of HOT

to EOT communication is the delivery of a train stoppage command from HOT to EOT.

2. The HOT antenna is mounted on the locomotive roof with good line of sight to the surrounding area. The EOT antenna is obstructed by the rear wall of the last car and quite often has no line of sight to the surrounding area.
3. Many trains may be in range of each other. This is for example the case in a railroad yard. When multiple trains are in range, HOT to EOT communication employing the same communication channels, may interfere with each other. For example, 2 x 12.5 kHz channels are used today in the US to serve all EOT to HOT communication. One of these channels is used for HOT to EOT communication and the other is used for EOT to HOT communication. In the future, both 12.5 kHz channels may be used for two-way communication. The arrangement in which one channel is used for HOT to EOT communication and another channel is used for EOT to HOT communication is referred to as "Duplex". The arrangement in which the same channel is used for two-way communication is referred to as "Simplex".
4. Interference between EOT-HOT communication of multiple trains can be minimized by employing CSMA/CA channel access, i.e., EOT and HOT radios on all trains, are only transmitting when the channel is idle. For CSMA/CA to be effective, each HOT and EOT radios need to have good connectivity to all other EOT and HOT radios so that they can detect if any other radio is transmitting. The scenario in which this condition is not met is referred to as the "hidden node problem", i.e., one or more of the radios are unable to detect transmission by one or more of the other radios. Given the EOT poor connectivity to its surrounding area, the EOT is highly likely to be hidden from some of the other radios.
5. This document describes a solution to the hidden EOT problem. The solution relies on the characteristics of NGHE message communication as follows:
    a. Most of the EOT messages are transmitted by the EOT in response to a command received from HOT.
    b. There are multiple types of message transactions between HOT and EOT. The type of transaction can be decoded from the command message transmitted by HOT.
    c. The communication parameters of the transaction, e.g., Modulation and Coding Scheme and Repetition factors, can also be decoded from the command message transmitted by the hot.
    d. Leveraging b and c above, the HOT decoding a command message of another HOT, can compute the duration of the entire transaction. Here are two transactions type examples:
        i. Massage transaction without positioning: this is a two-message transaction including a Command message from HOT to EOT and a Status message with no positioning from EOT to HOT.

ii. Message transaction with positioning: this is a three- message transaction including a Command message from HOT to EOT, A Status message with positioning from EOT to HOT and an ACK message from HOT to EOT.

Each of these message transactions along with the parameters of communication can be translated into the duration of the transaction.

Simplex Channel Access

1. Both HOT and EOT perform CSMA/CA. Sensing is performed against the RX frequency (which for Simplex, equals the TX frequency).
2. A deferral mechanism is used to minimize the probability of collisions, especially when the EOT is hidden from some of the other links. This mechanism runs at the HOT in addition to the basic CSMA/CA mechanism that runs in both EOT and HOT:
    a. The HOT monitors NGHE commands of all NGHE links in range. When an NGHE command of another HOT is detected, the HOT suspends its transmission for a period equal to the duration of the entire message transaction.
    b. The HOT may also decode a status message transmitted by a foreign EOT and defer transmission for the remaining duration of the transaction.
    c. The HOT will identify a message as being transmitted by a foreign HOT or EOT by looking at the id of the sender in the message header.
    d. The HOTs will typically have line of sight, i.e., the likelihood of a hidden HOT is small. The EOT acts in response to a HOT command, and as such, a hidden EOT is resolved by its master HOT.

Duplex Channel Access

1. Both HOT and EOT perform CSMA/CA. Sensing in the HOT is done in the HOT to EOT communication channel. It may also be done in the EOT to HOT communication channel but given the deferral mechanism described below; this is not necessary.
2. When the HOT wants to transmit, it tunes its receiver to the HOT to EOT communication channel, performs the sensing and transmits the message if the HOT to EOT channel is idle. The HOT tunes its receiver to the EOT to HOT channel only during the message transaction with the EOT. At any other time, the HOT receiver is tuned to the HOT to EOT channel so that it can detect Command messages transmitted by foreign HOTs. When the EOT wants to transmit, it tunes its receiver to the EOT to HOT communication channel, perform the sensing and transmit the message if the EOT to HOT channel is idle. At any time other than

prior to message transmission, the EOT receiver is tuned to the HOT to EOT communication.