March 2022

TRUSTED RPL PROTOCOL FOR FIELD AREA NETWORKS

Niranjan M M

TRUSTED RPL PROTOCOL FOR FIELD AREA NETWORKS

AUTHOR:
Niranjan M M

ABSTRACT

Multiple companies have developed Field Area Network (FAN) solution for Industrial IoT (IIoT), which is evolving from smart metering (electricity, gas, water) to smart cities. The wireless mesh FAN deployment consists of many Endpoints and tens of Border Routers. Routing Protocol for Low Power and Lossy Networks (LLN) (RPL) [RFC6550] is used in wireless mesh FAN deployments, it is a flexible and open standard. The RPL is a generic Distance Vector protocol that is well suited for low energy Internet of Things (IoT) networks. But it is vulnerable to several forms of attacks such as Physical and Cyber-attacks (eavesdropping, spoofing, false data injection, replay attacks etc.,). The classical approach to mitigate above attacks is to use cryptographic methods to provide authentication, integrity and confidentiality to the information exchanged during the topology discovery and route setup. However, these cryptographic methods are not sufficient to provide trustworthiness between Endpoint and Border Router in FAN deployment. If any of the Endpoint (EP) or Border Router is compromised, i.e., it is no longer a trusted entity, which could pose any of the above attacks listed and can leads to non-secure path (route) selection. The techniques presented herein define method to RPL protocol used in FAN for providing Proof of Integrity during Topology Discovery (RPL) and Route Setup (DAO/P-DAO) messages exchanged between Endpoint and Border Router. Topology discovery and Route setup messages between Endpoints and Border Routers are extended with extensions that carry Proof of Integrity and intent to validate Proof of Integrity.

DETAILED DESCRIPTION

Multiple companies have developed Field Area Network (FAN) solution for Industrial IoT (IIoT), which is evolving from smart metering (electricity, gas, water) to smart cities. Also, many companies are leading member of the Wi-SUN alliance, which is promoting IPv6-based wireless mesh Field Area Network (FAN) solution for smart utility and smart city applications. FANs rely on a variety of wireless communication technologies, and they are increasingly vulnerable to

physical and cyber-attacks such as eavesdropping, spoofing, false data injection, replay attacks etc., As per research, approx. 60% of respondents report cyber-attacks focusing on both IT and OT infrastructure. The top three areas of security concerns related to FANs are SCADA systems, Distributed Automation and AMI Meters.

The wireless mesh Field Area Network (FAN) deployment consists of many Endpoints and tens of Border Routers. Routing Protocol for Low Power and Lossy Networks (LLN) (RPL) [RFC6550] is used in wireless mesh Field Area Network (FAN) deployments and it is a flexible and open standard. The RPL is a generic Distance Vector protocol that is well suited for low energy Internet of Things (IoT) networks. But it is vulnerable to several forms of attacks such as Physical and Cyber-attacks (eavesdropping, spoofing, false data injection, replay attacks etc.,). The classical approach to mitigate above attacks is to use cryptographic methods to provide authentication, integrity and confidentiality to the information exchanged during the topology discovery and route setup. However, these cryptographic methods are not sufficient to provide trustworthiness between Endpoint (RPL Node) and Border Router (RPL Root) in FAN deployment. If any of the endpoint (EP) or Border Router is compromised, i.e., it is no longer a trusted entity, which could pose any of the above attacks listed and can leads to non-secure path (route) selection. Currently, there are no methods which provides trustworthiness to RPL routing protocol used in wireless mesh FAN deployments.

The main components of control plane of FAN architecture are

1. Topology Discovery: Network topology is built based on the RPL (IETF RFC6550) routing protocol.
2. Route Computation: The Border Router computes the routes.
3. Route Setup: It is based on the DAO/P-DAO protocol.
4. Sibling Selection: It provides topology information to compute routes.

The main components of data plane of FAN architecture are

1. Flow identification: It is based on the P-DAO protocol.
2. Route optimisation: it is based on RAW (Reliable Available Wireless) protocol.

The techniques presented herein define method to RPL protocol used in Field Area Network (FAN) for providing Proof of Integrity during Topology Discovery (RPL) and Route Setup (DAO/P-DAO) messages exchanged between Endpoint and Border Router. Topology discovery and Route setup messages between Endpoints and Border Routers are extended with extensions that carry Proof of Integrity and intent to validate Proof of Integrity.

The techniques presented herein propose method to add attestation information to the RPL and DAO packets as an extension that embeds:

- Hardware fingerprint (derived from SUDI or similar)
- Software - OS, BIOS, Kernel, Version, Application binaries/libraries, KGV - Known Good Values) etc.,
- Platform information - counters, time-ticks, PCR etc.,

Proof of Integrity: TPM functionality is used as root of trust and as Proof of Integrity of Endpoint and Border Router.

As mentioned in https://tools.ietf.org/html/rfc6550#section-6 (RPL Control Message), RPL provides support for carrying number of options. These options are used as additions to the protocol without breaking backwards compatibility with earlier versions. This method adds attestation information as another option to be carried in Topology Discovery (RPL) packets to provide Proof of Integrity.

Similarly as mentioned for DAO (https://tools.ietf.org/html/rfc6550#section-6.4) and DAO-ACK (https://tools.ietf.org/html/rfc6550#section-6.5) provides support for carrying number of options. This method adds attestation information as another option to be carried in DAO and DAO-ACK packets to provide Proof of Integrity.

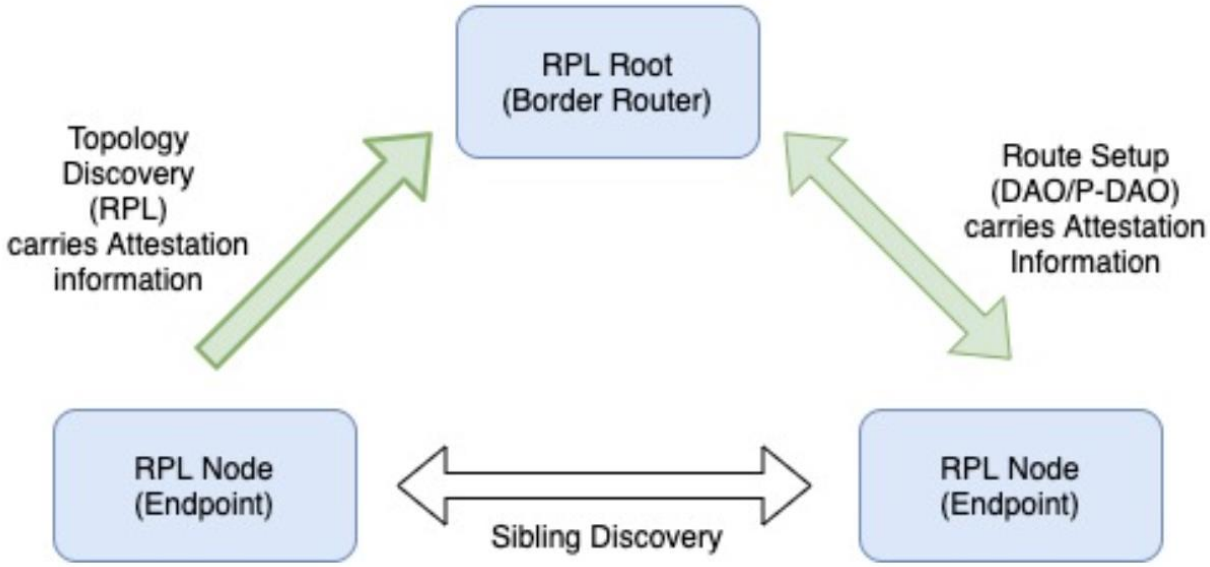

Figure-1

Freshness of the Proof of Integrity:

Proof of Integrity can also be accompanied with a signature to prove freshness of the Proof of Integrity i.e., by adding a signature over random nonce (aka entropy) presented by the peer in the DAO and DAO-ACK packets. This would help in detecting the replay of old evidence via a "nonce". A "nonce" is a random number provided by the entity making the request. This nonce is passed into the TPM. Results coming out of the TPM include a signature based on the "nonce". This result is the output from the TPM which could not have been generated before that "nonce" was provided.

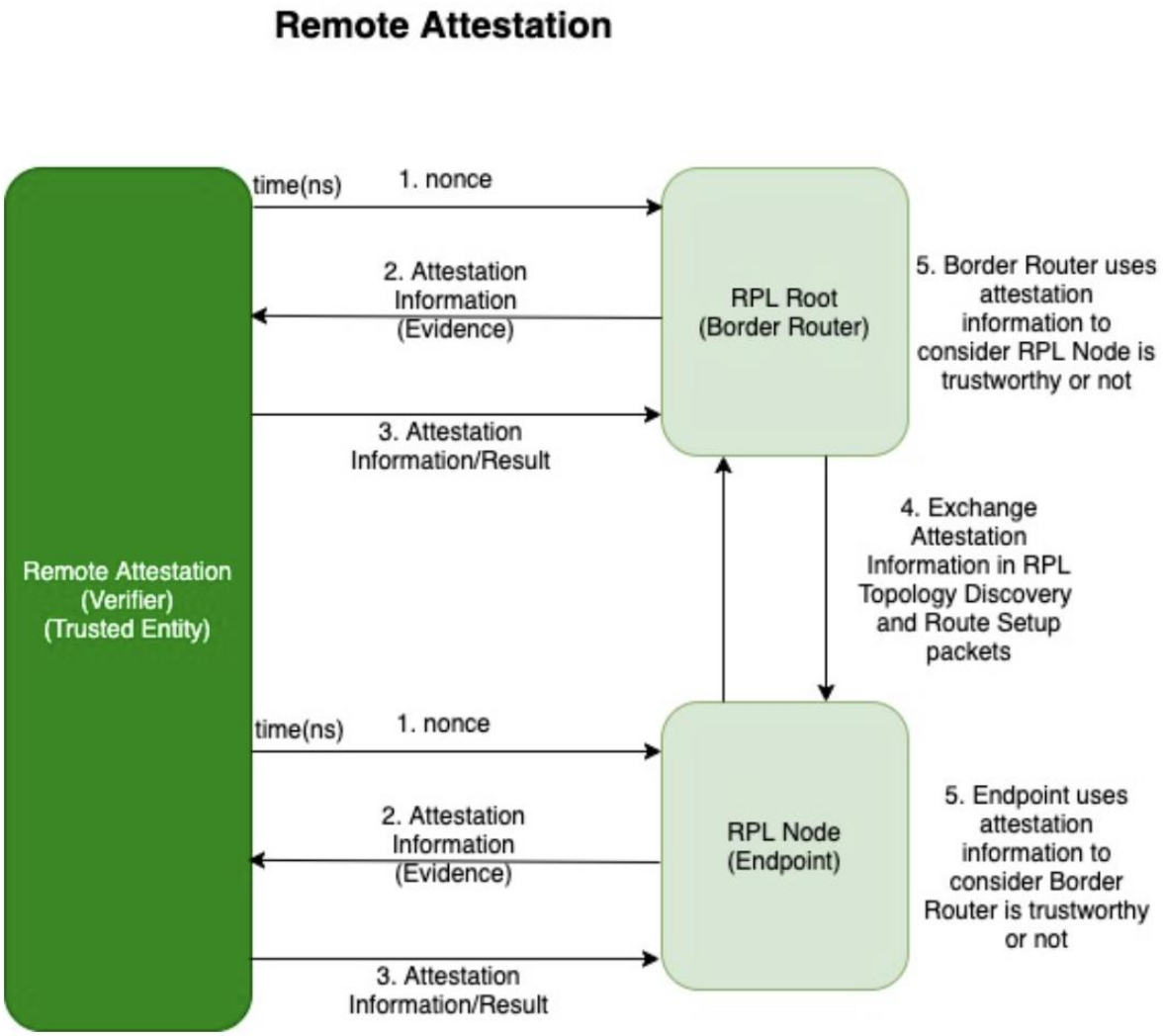

Figure-2

For Example: Destination Advertisement Object (DAO) is the RPL message for route setup to be exchanged between the Endpoint and Border Router. The operation consists of the DAO and DAO-ACK messages. DAO from the Endpoint contains random data/nonce, it is extended to carry intention to validate Proof of Integrity. DAO-ACK from Border Router carries an extension to its Proof of Integrity along with a signature over random data/nonce received in DAO.

Endpoints and Border Routers participating in RPL protocol exchange will use this attestation information to verify whether the peer who send the topology discovery or DAO or DAO-ACK message is trustworthy or not and make decision to accept/reject the respective messages.

Protocol Extension Options of RPL protocol messages would be extending to carry attestation information as defined below

Option Type	TBD (To be allocated by IANA)
Option Length (Variable)	2 to 252 Bytes
Option Value (Attestation Information)	ID (1 Byte): Defines the ID of the following token, it takes value from 0 to 254 (ID=255 is Reserved) Token: 1 to 251 Bytes of binary data Using the first byte of the value of an ID to distinguish different types of Attestation Token

For Example:

Option Type	10 RPL_ATTESTATION_TOKEN (Suggested value - to be assigned by IANA)
Option Length (Variable)	17 Bytes
Option Value (Attestation Information)	0x0A000102030405060708090A0B0C0D0E0F (Here first byte 0A is the Token Type for Hardware Fingerprint, remaining 16 Bytes is the Attestation Information carry Hardware Fingerprint)

Figure-3

The techniques presented herein provides trustworthiness to RPL routing protocol messages (Topology discovery, DAO, DAO-ACK) exchanged between Endpoint and Border Routers. Moreover, trust is required in Field Area Network deployments which is over wireless mesh technology (as with all networks, wireless technology comes with vulnerability to cyber-attacks etc.,). Additionally, this method provides trusted IIoT to meet the requirements of customers with respect to security and trust (as we know IOT devices are prone to several attacks and vulnerabilities).