Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 22, 2015

D. He
Huawei

January 18, 2015

Security Bootstrapping of IEEE 802.15.4 based Internet of Things
draft-he-iot-security-bootstrapping-00

Abstract

Network level security bootstrapping and joining device level security bootstrapping mechanisms are described in this document. They are proposed for security bootstrapping of the Internet of Things networks, which implement IETF protocols (e.g. 6LoWPAN, 6lo, RPL, AODV, DSR) over IEEE 802.15.4. The network level security bootstrapping is useful at the very beginning of a newly deployed IoT network. It automatically and hierarchically adds all the devices to security domain and helps establish security communication. The joining device level security bootstrapping provides comprehensive mechanism for different IoT devices joining an existing IoT network.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 22, 2015.

Copyright Notice

Table of Contents

1. Introduction

An IoT network is composed of various numbers of connected things with communication ability and different functionalities (sensing unit, control logic). They cooperate together to accomplish specific tasks required by users. Things in an IoT network might be supplied by different vendors, and are normally resource-constrained devices that with limited power supply, communication capability, CPU performance and memory volume.

[IEEE802.15.4]is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs). It is widely used in wireless sensor networks nowadays, 6LoWPAN WG (concluded) developed RFC 4944[RFC4944] to describe how to transmit IPv6 packets over 802.15.4, and support mesh routing in LR-WPANs. 6lo WG defines generic IPv6 packet header compression method [RFC7400] for LR-WPANs. 6tisch tries to build adaptation protocol for 802.15.4e protocol. Roll develops routing protocol RPL[RFC6550] for IPv6 based low power and lossy networks. IEEE 802.15.4 is foreseen as the most used lower layer protocol for low rate IoT networks with resource constrained devices.

Creating security domains from previously unassociated IoT devices is a key operation in the IoT network and in the lifecycle of a thing. Because IEEE 802.15.4 maximum payload size is 128 Bytes, a standard security bootstrapping protocol should be light-weight with low complexity. The protocol must allow for commissioning of devices from different manufacturers and facilitate transitions of control amongst devices during the device's and system's lifecycle.

Traditional security bootstrapping approaches include device authentication and key generation/distribution, which tend to impose configuration burdens upon users. For example, users need to follow a series of instruction steps for WPA2-PSK (WiFi Protected Access 2, Pre-shared key) configuration, even though the pre-shared key mode is the simplest option for using WPA. Establishing security among IoT devices becomes more complicated since they don't always provide user interface to input necessary security information. Furthermore, the scale of the IoT network can be large, human intervention in large scale security bootstrapping is expensive and low efficient.

[I-D.pritikin-anima-bootstrapping-keyinfra] proposes a zero-touch bootstrapping key infrastructure to allow joining device securely and automatically bootstraps itself based on 802.1AR certificate. It can't be directly used in 802.15.4 devices due to the high security complexity and heavy communication overhead. Its architecture is not built by considering different possible 802.15.4 network topologies and the underlying routing protocols developed by IETF.

[I-D.struik-6tisch-security-considerations]defines high level requirements and proposes two types of security mechanisms: single-stage and two-stage. Even though the two types of security AA mechanisms offer flexible solutions. The underlying security architecture can neither be used directly by 802.15.4 IoT networks. IEEE 802.15.4 also defines two-step mechanism for nodes joining network with layer 2 authentication. Without considering use of IPv6 infrastructure, the solution is not comprehensive.

Another key challenge for security bootstrapping of a device the above mentioned mechanisms is that they are not feasible to commission a device when the adjacent devices have not been commissioned yet. As a result, this document describes and standardizes two types of automatic bootstrapping methods for 802.15.4 based IoT networks: network level security bootstrapping and joining device level security bootstrapping.

2. new section

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

This specification requires readers to be familiar with all the terms and concepts that are discussed in "Neighbor Discovery for IP version 6 (IPv6)" [RFC4861], "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919].This specification makes extensive use of the same terminology defined in [RFC4944].

3. IEEE 802.15.4 based IoT topologies

A general architectural overview of the IEEE 802.15.4 based IoT is provided in Figure 1. All the devices communicate to backbone server through 6LBR. FFDs communicate with each other directly or indirectly via hopping or 6LBR. RFDs directly connect to FFDs, and the number of RFDs that attach to a FFD may vary.

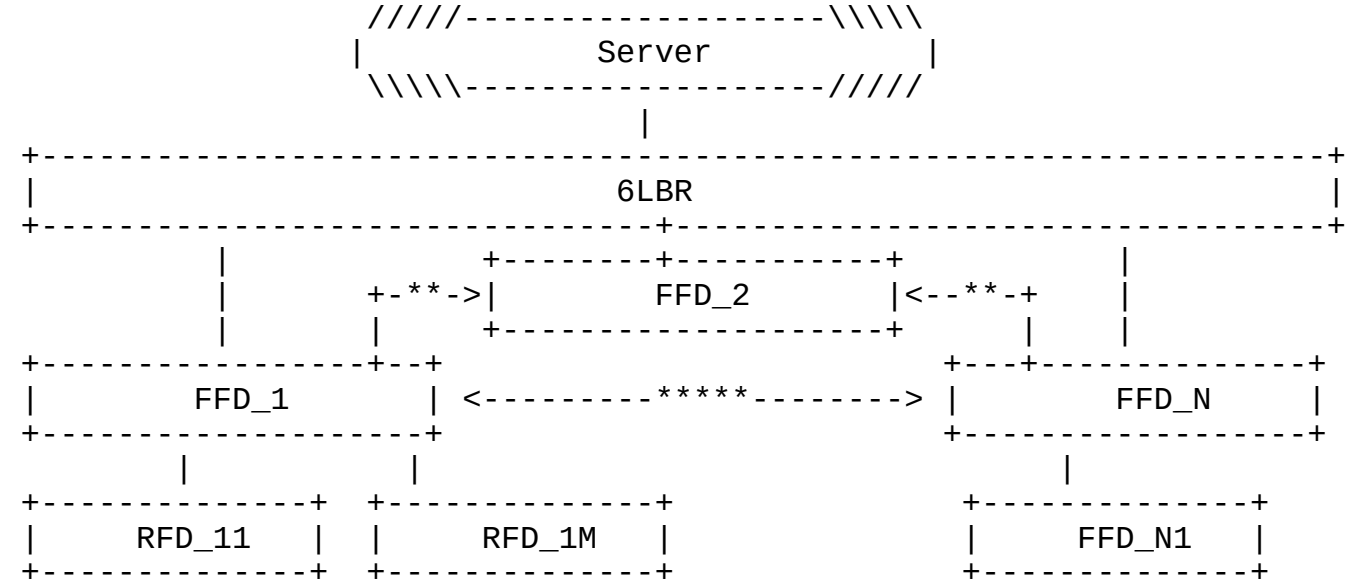

Figure 1

4. Network level security bootstrapping

At the very beginning of the networking once nodes are deployed, network level security bootstrapping assist automatically creates security domain and hierarchically adds devices to network. The mechanism is realized by three phases:

Phase 1: Security bootstrapping for the first hop FFDs via 6LBR

Phase 2: Security bootstrapping for further FFDs via configured FFDs

Phase 3: Security bootstrapping for RFDs via configured FFDs

4.1. Security bootstrapping for the first hop FFDs via 6LBR

When devices are power-on, 6LBR broadcasts beacon frames to neighboring nodes. The FFDs that receive the beacon frames are the first-hop FFDs. As shown in Figure 2, upon receiving the beacon frame, a first-hop FFD associates with 6LBR at link layer according to IEEE 802.15.4. The FFD then presents credential to 6LBR, which are forwarded to trust center to be validated. EAP can be used to realize the authentication procedure. If the validation is successful, the IP address and network key are generated and delivered to the FFD. Further configurations such as cluster head selection, routing protocol, etc., can be realized afterwards. Otherwise if the validation fails, the 6LBR refuses adding the FFD to its domain.

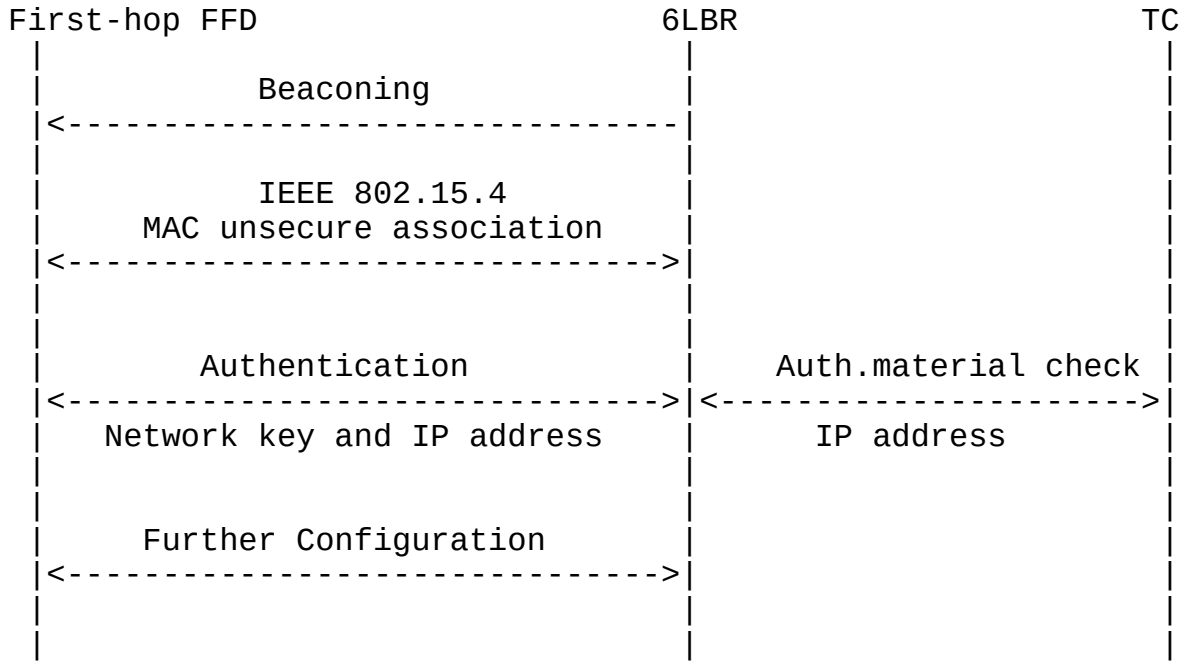

Figure 2

4.2. Security bootstrapping for further FFDs via configured FFDs

The configured FFDs broadcast beacon frames to neighboring nodes. The unconfigured FFD that receives the beacon frame associates with the configured FFD at link layer. A FFD may receive multiple beacon frames from more than one configured FFDs, it can select the first one to associate or the one with strongest received power strength. The selection policy is out of the scope of the current document. The unconfigured FFD then presents credential to the associated configured FFD, which are forwarded to 6LBR and TC to be validated. If EAP is used, PANA can be used to relay the authentication message from configured FFDs to 6LBR. If the validation is successful, the IP address and network key are generated and delivered to the FFD. Further configurations such as routing protocol can be realized afterwards. Otherwise if the validation fails, the 6LBR refuses adding the FFD to its domain.

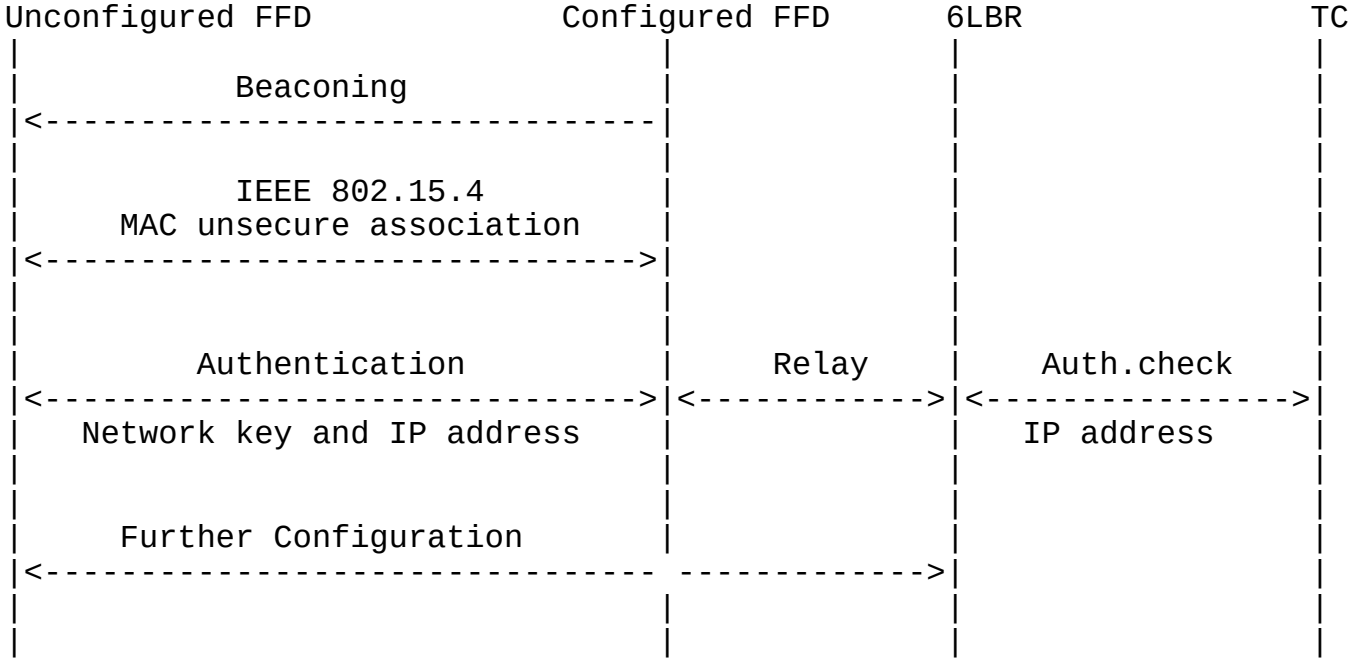

Figure 3

4.3. Security bootstrapping for RFDs via configured FFDs

The configured FFDs broadcast beacon frames to neighboring nodes. The unconfigured RFD that receives the beacon frame associates with the configured FFD at link layer. A RFD may receive multiple beacon frames from more than one configured FFDs. It can select one device to associate, e.g. the first one that replies or the one with strongest received power strength. The unconfigured RFD then

presents credential to the associated configured FFD, which are forwarded to 6LBR and TC to be validated. If the validation is successful, the IP address and network key are generated and delivered to the RFD. Otherwise if the validation fails, the FFD refuses adding the RFD to its domain.

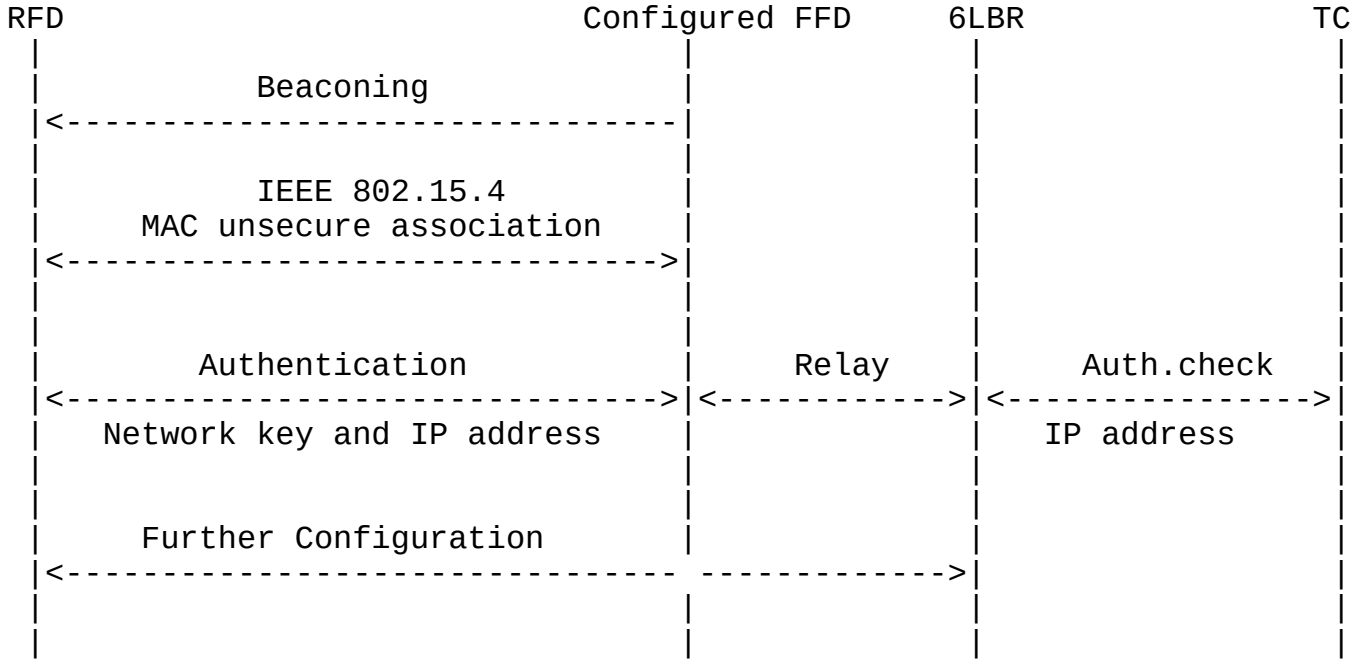

Figure 4

5. Joining Device Security Bootstrapping

New devices may be added to an existing IoT due to various reasons. As a result the security bootstrapping can be devided into the bootstrapping of joining RFD and bootstrapping of joining FFD.

5.1. Bootstrapping of joining RFD via configured FFD

A joining RFD broadcasts beacon frames to neighboring nodes. The configured FFDs that receive the beacon frames, decide whether allowing the RFD associating at link layer. A RFD may receive multiple replies from more than one configured FFDs. It can select one device to associate, e.g. the first one that replies or the one with strongest received power strength. The joining RFD then presents credential to the associated configured FFD, which is forwarded to 6LBR and TC to be validated. If the validation is successful, the IP address and network key are generated and delivered to the RFD. Otherwise if the validation fails, the FFDrefuses adding the RFD to its domain.

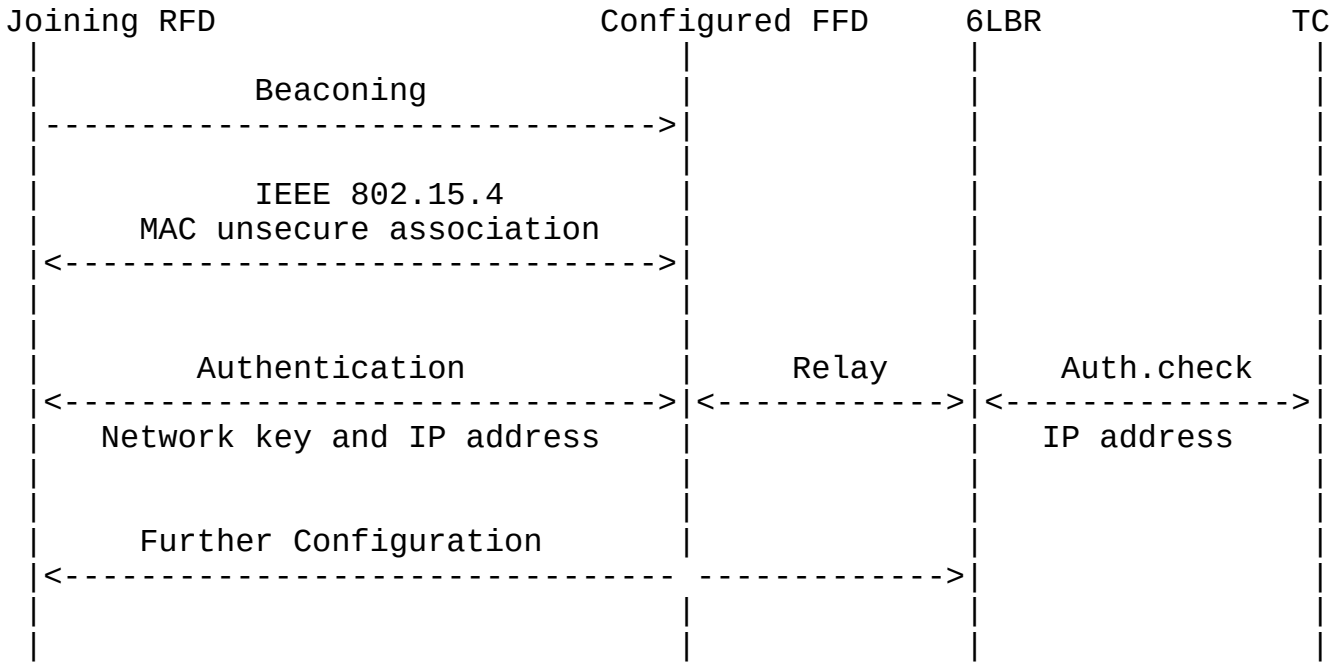

Figure 5

5.2. Bootstrapping of joining FFD via configured FFD/6LBR

A joining FFD broadcasts beacon frames to neighboring nodes. The configured FFDs that receive the beacon frames, decide whether allowing the FFD associating at link layer. A FFD may receive multiple replies from more than one configured FFDs or directly from the 6LBR. It can select one device to associate, e.g. the first one that replies or the one with strongest received power strength. The joining FFD then presents credential to the associated configured FFD/6LBR, which is forwarded to TC to be validated. If the validation is successful, the IP address and network key are generated and delivered to the FFD. Further configurations such as routing protocol can be realized afterwards. Otherwise if the validation fails, the 6LBR refuses adding the FFD to its domain.

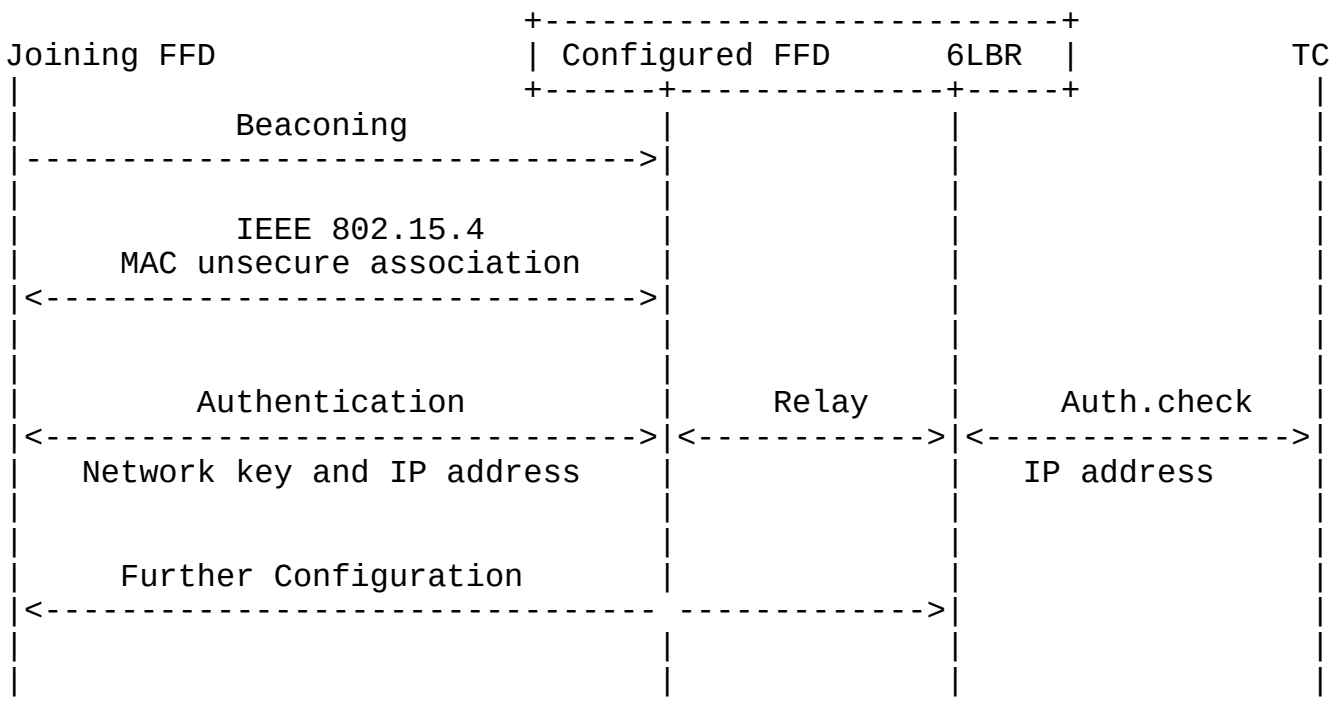

Figure 6

6. Security Considerations

TBD

7. Acknowledgement

TBD

8. References

8.1. Normative References

[IEEE802.15.4]
IEEE Standard, , "IEEE Std. 802.15.4-2011", October 2011, <http://standards.ieee.org/findstds/standard/802.15.4-2011.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, August 2007.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, November 2014.

8.2. Informative References

[I-D.pritikin-anima-bootstrapping-keyinfra]
Pritikin, M., Behringer , M., and S. Bjarnason , "Bootstrapping Key Infrastructures", November 2014.

[I-D.struik-6tisch-security-considerations]
Struik , R., "6TiSCH Security Architectural Considerations", January 2015.

Author’s Address

Danping He
Huawei

Email: ana.hedanping@huawei.com