6TiSCH
Internet-Draft
Intended status: Informational
Expires: April 30, 2015

R. Struik
Struik Security Consultancy
Y. Ohba
Toshiba
S. Das
ACS

October 27, 2014

6TiSCH Security Architectural Elements, Desired Protocol Properties, and Framework
draft-struik-6tisch-security-architecture-elements-01

Abstract

This document describes 6TiSCH security architectural elements with high level requirements and the security framework that are relevant for the design of the 6TiSCH security solution.

Table of Contents

1. Security Architecture Elements 2
1.1. Device Types and Roles 2
1.2. Device Enrollment Phases 3
1.3. Desired Protocol Properties 3
2. Security Framework 4
2.1. Single-Stage Authentication Framework 4
2.2. Two-Stage Authentication Framework 5
3. Security Considerations 6
4. IANA Considerations 7
5. Acknowledgments 7
6. Normative References 7
Authors' Addresses 7

1. Security Architecture Elements

1.1. Device Types and Roles

There are two types of devices (or nodes) that are involved in the 6TiSCH security architecture: end devices that intend to join the LLN (commonly known as joining nodes) and network devices that help the joining node to be authenticated and authorized by the network. From a security operations perspective, each device has a distinct role in the network. An end device has normally a client role, while the network device can be a proxy or assume a server role. A proxy is an intermediate node that helps the end device to establish a communication with the server. An end device may move in and out of networks (that may be alien to it) and may have little network management functionality on board. However, it usually does have the right credential required for initializing the network joining process. A proxy is an intermediary node that that may be more tied into a relatively stable infrastructure and may have more support for network management functionality and generally has reliable access to back-end systems of the network. A server provides stable, highly available infrastructure and network management support and is capable of authenticating and authorizing a joining node.

It is important to note that a network node may assume multiple roles at the same time and that a particular role may be assumed by multiple network nodes. Furthermoe, the roles of a network node may change over time and can be dynamic in nature along a node or a network's lifecycle.

1.2. Device Enrollment Phases

Device Authentication: The joining node and network node authenticate each other and establish a shared key, so as to ensure on-going authenticated communications. This may involve a server as a third party.

Authorization: The network node decides on whether/how to authorize a joining node (if denied, this may result in loss of bandwidth). Authorization decisions may involve other nodes in the network.

Configuration/Parameterization: The network node distributes configuration information to the joined node, such as scheduling information, IP address assignment information, and network policies. This may originate from other network devices, for which it acts as proxy. This step may also include distribution of information from the joining node to the network node and, more generally, synchronization of information between these entities.

1.3. Desired Protocol Properties

Security-Related:

1. Parties executing a security protocol should be explicitly aware of its security properties;

2. Compromise of keys or devices should have limited effect on security of other devices or services;

3. Attacks should not have a serious impact beyond the time interval/space during/in which these take place;

4. Security protocols should minimize the impact of network outages, denial of service attacks.

Communication Flows:

1. Security protocols should allow to be run locally, without third party involvement, wherever possibl;

2. The number of message exchanges for a joining device should be reduced;

3. Message exchanges should be structured so as to allow parallel execution of protocol steps, wherever possible.

Computational Cost:

1. Security protocols should not impose an undue computational burden, especially on joining devices (An exception here may arise, when recovering from an event seriously impacting availability of the network.)

Device Capabilities:

1. Dependency on an accurate time-keeping mechanism should be reduced;

2. Computational/time latency trade-offs should be tweaked to benefit those of joining node, wherever possible;

3. Dependency on "homogeneous trust models" should be reduced, without jeopardizing the security properties;

4. Dependency on on-board trusted platforms and trusted I/O interfaces should be reduced.

2. Security Framework

2.1. Single-Stage Authentication Framework

In the single-stage authentication and authorization framework, depicted in Figure 1, it is assumed that devices have access to certificates and that entities have access to the root CA certificate of their communicating parties (initial set-up requirement). Under these assumptions, the authentication step of the device enrollment process does not require online involvement of a third party. Authentication is performed between the joining node and the proxy using their certificates. Upon successful authentication, link-layer keys are established between the client and the proxy. The proxy will deny bandwidth if authorization is not successful. After successful authentication and authorization, configuration information is exchanged.

When a device rejoins the network in the same authorization domain, the authorization step could be omitted if the server distributes the authorization state for the device to the proxys when the device initially joined the network. However, this generally still requires the exchange of updated configuration information, e.g., related to time schedules and bandwidth allocation.

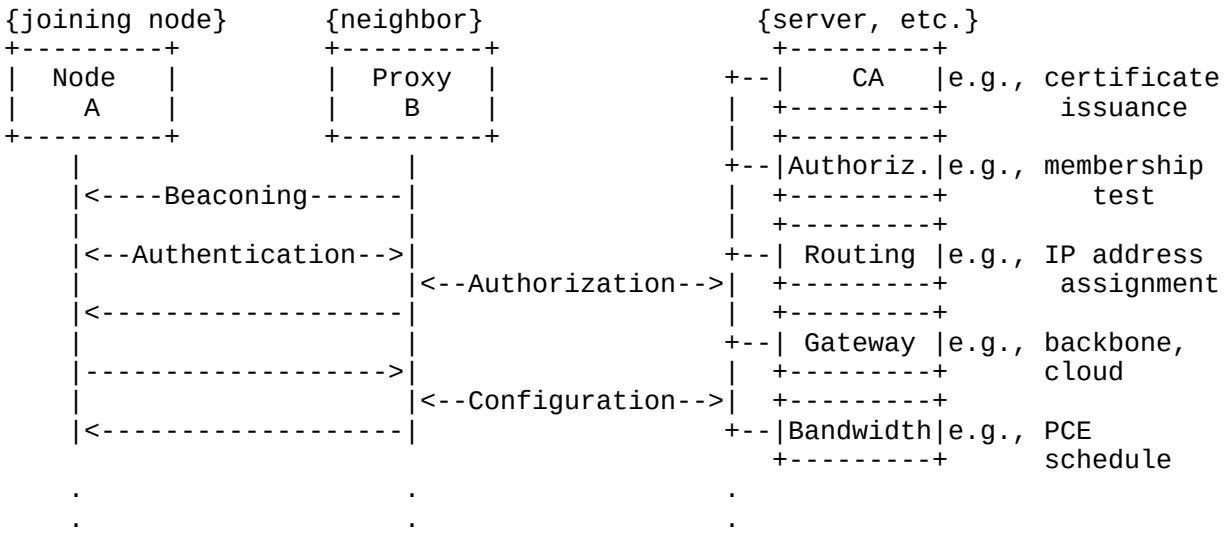

Figure 1: Single-stage authentication/authorization

2.2. Two-Stage Authentication Framework

In the two-stage authentication and authorization framework, depicted in Figure 2, a joining node performs two authentication and authorization steps. The first step, called Phase-1 authentication, is performed between the joining node and the server via a proxy. Phase-1 authentication and authorization uses deployment-specific enrollment credentials and results in issuance of a certificate by the CA to the joining node. Here, the node's certificate and root CA certificates of its communicating parties are distributed from the server to the client.

The second step, called Phase-2 authentication, follows the successful completion of Phase-1 authentication and authorization. Phase-2 authentication is performed between the joining node and the proxy using their certificates. Upon successful authentication, link-layer keys are established between the joining node and the proxy. The proxy will deny bandwidth if Phase-2 authorization is not successful. After successful authentication and authorization, configuration information is exchanged.

Once a joining node obtains a certificate for Phase-2 authentication, no additional Phase-1 authentication and authorization is needed, i.e., only Phase-2 authentication and the configuration are required for rejoining the network via a proxy under the same authorization

domain. This reduces to the single-stage authentication framework discussed in the previous section.

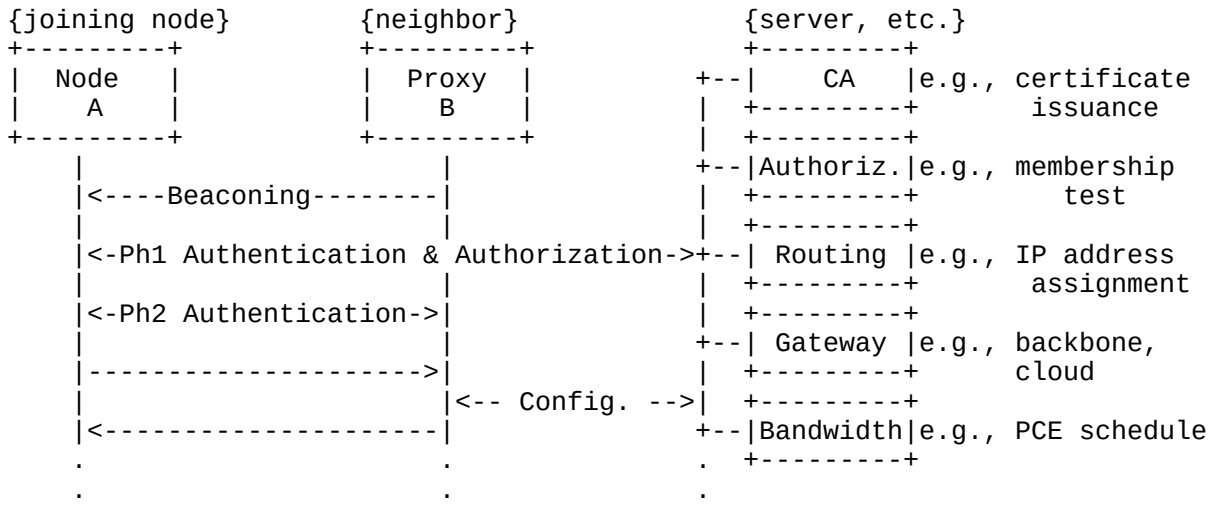

Figure 2: Two-stage authentication/authorization

3. Security Considerations

In this section, security issues that can potentially impact the operation of IEEE 802.15.4e TSCH MAC are described.

In TSCH MAC, time synchronization and channel hopping information are advertised in Enhanced Beacon (EB) frames [I-D.ietf-6tisch-terminology]. The advertised information is used by mesh nodes to determine the timeslots available for transmission and reception of MAC frames. A rogue node can inject forged EB frames and can cause replay and DoS attacks to TSCH MAC operation. To mitigate such attacks, all EB frames MUST be integrity protected. While it is possible to use a pre-installed static key for protecting EB frames to every node, the static key becomes vulnerable when the associated MAC frame counter continues to be used after the frame counter wraps. Therefore, the 6TiSCH solution MUST provide a mechanism by which mesh nodes can use the available time slots to run authentication protocols and provide integrity protection to EB frames.

For use cases where certificates are used for authentication, pre-provisioning of absolute time to devices from a trustable time source using an out-of-band (OOB) mechanism is a general requirement.

Accuracy of time depends on the OOB mechanism, including use of the time hard-coded into the installed firmware. The less time accuracy is, the more attack opportunities during Phase-1. In addition, use of CRL is another requirement for authentication employing certificates to avoid an attack that can happen by a compromised server or CA certificate.

4. IANA Considerations

There is no IANA action required for this document.

5. Acknowledgments

TBD.

6. Normative References

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

[I-D.ietf-6tisch-terminology] Palattella, M., Thubert, P., Watteyne, T., and Q. Wang, "Terminology in IPv6 over the TSCH mode of IEEE 802.15.4e", draft-ietf-6tisch-terminology-02 (work in progress), July 2014.

Authors' Addresses

Rene Struik
Struik Security Consultancy

Email: rstruik.ext@gmail.com

Yoshihiro Ohba
Toshiba Corporate Research and Development Center
1 Komukai-Toshiba-cho
Saiwai-ku, Kawasaki, Kanagawa 212-8582
Japan

Phone: +81 44 549 2127
Email: yoshihiro.ohba@toshiba.co.jp

Subir Das
Applied Communication Sciences
1 Telcordia Drive
Piscataway, NJ 08854
USA

Email: sdas@appcomsci.com