6TSCH
Internet-Draft
Intended status: Informational
Expires: January 11, 2014

S. Chasko
L+G
S. Das
ACS
R. Marin-Lopez
University of Murcia
Y. Ohba, Ed.
Toshiba
P. Thubert
cisco
A. Yegin
Samsung
July 10, 2013

Security Framework and Key Management Protocol Requirements for 6TSCH draft-ohba-6tsch-security-01

Abstract

Since 6TSCH forms layer 3 meshes over IPv6, use of key management protocols defined at layer 3 or above matches the target architecture so they can apply for the process by a new device of joining the mesh to extend it. This document details that particular operation within the whole 6TSCH architecture.

Table of Contents

1. Introduction

The emergence of radio technology enabled a large variety of new types of devices to be interconnected, at a very low marginal cost compared to wire, at any range from Near Field to interplanetary distances, and in circumstances where wiring could be less than practical, for instance rotating devices.

At the same time, a new breed of Time Sensitive Networks is being developed to enable traffic that is highly sensitive to jitter and quite sensitive to latency. Such traffic is not limited to voice and video, but also includes command and control operations such as found in industrial automation or in-vehicular sensors and actuators.

6TSCH aims at providing an open standard with new capabilities, both in terms of scalability (number of IPv6 devices in a single subnet) and in terms of guarantees (delivery and timeliness). Both the ISA100.11a and Wireless HART protocols are gaining acceptance in the automation industry and demonstrate that a level of determinism can be achieved on a wireless medium with adequate guarantees for low speed control loops, used in mission critical Process Control applications. For industrial applications, security is not an option and a power efficient authentication mechanism is strictly required.

For other usages such as rust control, intrusion detection or seismic activity monitoring, the capability to correlate inputs from multiple sources can be critical, and the value of the network directly augments with the number of connected devices. In order to scale to appropriate levels, the need for spatial reuse of the spectrum often implies routing capabilities over short range radios. Proprietary variations demonstrate that RPL can scale to multiple thousands of devices, but at the same time expose a new challenge for security that must enable deployments of any scale with security requirements that may vary widely. If the cost of the security in terms of network operations and system resources depends on that degree of security, then 6TSCH should enable different profiles that can match different requirements and capabilities.

Since 6TSCH forms layer 3 meshes over IPv6, key management protocols defined at layer 3 or above can apply for the process by a new device of joining the mesh to extend it. This document details that particular operation within the whole 6TSCH architecture.

ZigBee IP [ZigBeeIP] ("ZigBee" is a registered trademark of the ZigBee Alliance) is a standard for IPv6-based wireless mesh networks using PANA for network access authentication and secure distribution of a link-layer group key called Network Key to authenticated mesh nodes formed over unslotted CSMA-CA MAC of 802.15.4. Each mesh node in the same ZigBee IP network derives the same link-layer key from the Network Key to protect IEEE 802.15.4 MAC frames exchanged between adjacent mesh nodes. While sharing the same link-layer key among all mesh nodes can make the required key state maintained by each mesh node compact, a compromise of a mesh node can lead to link-layer key leakage in the entire ZigBee IP network. Also, the cost of updating the link-layer key can be high as the key needs to be updated at all mesh nodes whenever the 4-octet frame counter at any single node wraps or the key is considered to be compromised or weak.

In the case of TSCH MAC which uses 5-octet global frame counter referred to as Absolute Slot Number (ASN), the frame counter is not likely to wrap in the expected lifetime of the device, but key update for a common link-layer key is still issue if the key needs to be changed for other reasons.

This document introduces a more secure and scalable key management framework for 6TSCH networks and identifies requirements for key management protocols to be used in the framework.

2. Acronyms

In addition to the acronyms defined in [I-D.palattella-6tsch-terminology], the following acronyms are used in this document.

KMP: Key Management Protocol

PANA: Protocol for carrying Authentication for Network Access

SA: Security Association

MAC: Media Access Control

3. Security Framework

This section describes a security framework consisting of four phases as shown in Figure 1. The architecture is applicable to not only 6TSCH networks but also non-time synchronized mesh networks. Each node in a mesh network runs through the following phases:

- Phase-0 (Implanting Phase): In this phase, a node installs credentials used for subsequent phases in a physically secure and managed location before the node is placed to where it is expected to operate. Details on Phase-0 is outside the scope of this document.

- Phase-1 (Bootstrapping Phase): In this phase, a node (re)installs credentials used for subsequent phases from an authentication server after it is placed to where it is expected to operate. The credentials installed during Phase-1 include Phase-2 credentials and Phase-3 credentials, and may also include long-term Phase-1 credentials if the initial Phase-1 credentials are intended for one-time use such as a temporary PIN. An authentication and key establishment protocol called a Phase-1 KMP is conducted between the node and the authentication server using Phase-1 credentials. The Phase-1 credentials have longer lifetime than Phase-2 and Phase-3 credentials so that Phase-2 and Phase-3 credentials can be

renewed using the Phase-1 credentials. Both symmetric and asymmetric key credentials can be used as Phase-1 credentials. In Phase-1 KMP, the Phase-2 and Phase-3 credentials are distributed from the authentication server to the node. When the authentication server is multiple hops away from the node, mutual authentication between the node and the authentication server is conducted via a neighboring node acting as an authentication relay. There may be no link-layer security available between the node and its neighboring node in this phase. An authentication server is typically (but is not necessarily) co-located with the coordinator of the mesh network. Phase-1 is optional if Phase-2 credentials are installed during Phase-0 and do not need to be updated.

- Phase-2 (Link Establishment Phase): In this phase, the node performs mutual authentication with its neighboring node using the Phase-2 credentials to establish SAs between adjacent nodes for protecting 802.15.4 MAC frames. The authentication and key establishment protocol used in this phase is referred as a Phase-2 KMP or a link establishment KMP. For highly scalable mesh networks consisting of thousands of mesh nodes, certificates are used as the Phase-2 credentials. The SA of a link between node i and node j maintains link-layer keys, i.e., 128-bit keys used in AES-CCM* mode, a variant of the Counter with Cipher Block Chaining - Message Authentication Code (CBC-MAC) Mode, for encryption, authentication or authenticated encryption of 802.15.4 frames. K_i denotes a link-layer key for protecting broadcast MAC frames originated at node i. K_ij denotes a link-layer key for protecting unicast MAC frames originated at node i and destined for node j. There are several variations of forming link-layer keys.

  1. K_ij=K_i for all j, K_i!=K_j for all i, j (i!=j)

  2. K_ij=K_ji, K_i!=K_j for all i,j (i!=j)

  3. K_ij!=K_ji, K_i!=K_j for all i,j (i!=j)

  In model 1, unicast and broadcast keys for protecting MAC frames originated at a given node are the same. In models 2 and 3, unicast and broadcast keys originated at a given node are distinct. The difference between models 2 and 3 is that unicast keys are bi-directional in model 2 while they are uni-directional in model 3. One model may be chosen among three depending on the required security level and the number of keys maintained by each node.

- Phase-3 (Operational Phase): In this phase, the node is able to run various higher-layer protocols over IP over an established secure link. Additional authentication and key establishment may take place for the higher-layer protocols using Phase-3 credentials. A node in Phase-3 is able to process Phase-1 and Phase-2 KMPs. Example use cases are:

  * A Phase-3 node can initiate a Phase-1 KMP to update its Phase-2 or Phase-3 credentials.

  * A Phase-3 node can forward Phase-1 KMP messages originated from or destined for a Phase-1 node that is joining the mesh network through the Phase-3 node.

  * A Phase-3 node can initiate a Phase 2 KMP to establish a new link with a newly discovered neighbor node.

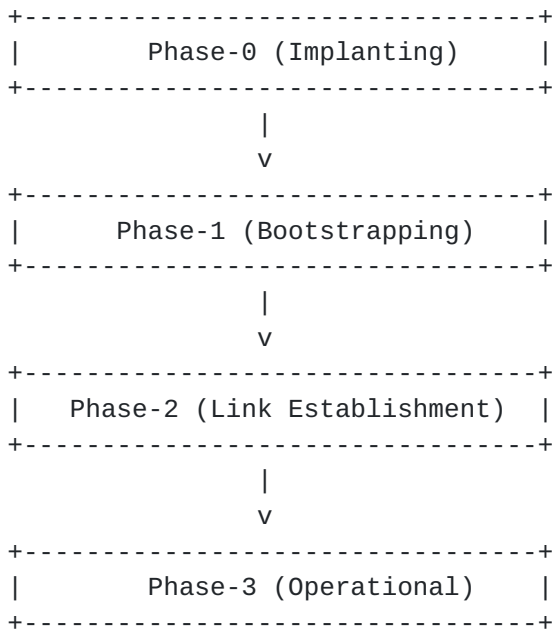

Figure 1: 4-Phase Key Management Model

```
            N)s - Node N is running Phase-1 KMP as a server
            N)c - Node N is running Phase-1 KMP as a client
            N)r - Node N is running Phase-1 KMP as a relay
            N)) - Node N is running Phase-2 KMP
            .  .. ...
            N, N,  N  - Node N is in Phase-1, -2 and -3, respectively

     .          .          ..         ...        ...         ...
     A          A)s        A))         A)s        A           A
               / \        / \        / \        / \         / \
   .   .     .   .      ..  ..    ... ...    ... ...     ... ...
   B   C     B)c C)c    B)) C))    B)r C      B)) C))     B   C
                                  / \ /      / \ /       / \ /
  .   .     .   .      .   .      .   .      ..  ..     ... ...
  D   E     D   E      D   E      D)c E)c    D)) E))     D   E

     (0)  ->   (1)   ->   (2)   ->   (3)  ->   (4)   ->   (5)
```

(0) Initially all nodes are in Phase-1. (1) Nodes B and C run Phase-1 KMP with Node A (i.e., the authentication server) to obtain Phase-2 and Phase-3 credentials. (2) Nodes B and C run Phase-2 KMP with Node A. (3) Nodes D and E run Phase-1 KMP using Node B as an authentication relay. (Alternatively, Node E may use Node C as an authentication relay.) (4) Node D runs Phase-2 KMP with Node B. Node E runs Phase-2 KMP with Nodes B and C. (5) All nodes are operational.

Figure 2: Example Sequence

Since we already identified PANA as the Phase-1 KMP due to its authentication relay and secure credential distribution capabilities, and Phase-3 KMP requirements would depend on application protocols, we focus on Phase-2 KMP requirements in the next section.

4. KMP requirements

4.1. Phase-1 KMP requirements

Requirements on Phase-1 KMP are listed below.

R1-1: Phase-1 KMP MUST support mutual authentication.

R1-2: Phase-1 KMP MUST support stateless authentication relay operation.

R1-3:s Phase-1 KMP MUST support secure credential distribution.

4.2. Phase-2 KMP requirements

Requirements on Phase-2 KMP are listed below.

R2-1: Phase-2 KMP Nodes MUST mutually authenticate each other before establishing a link and forming a mesh network. No authentication server is involved in the Phase-2 authentication.

R2-2: Phase-2 KMP authentication credentials MAY be pre-provisioned or MAY be obtained via Phase-1 KMP.

R2-3: Phase-2 KMP authentication credentials MUST have a lifetime.

R2-4: Phase-2 KMP MUST support certificates for scalable operation.

R2-5: Phase-2 KMP message exchanges MUST be integrity and replay protected after successful authentication.

R2-6: Phase-2 KMP MUST have the capability to establish security association and unicast session keys after successful authentication to protect unicast MAC frames between nodes.

R2-7: Phase-2 KMP MUST have the capability to establish security association and broadcast session keys after successful authentication to protect broadcast MAC frames between nodes.

R2-8: Phase-2 KMP MUST support confidentiality to distribute the broadcast session keys securely.

5. 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.watteyne-6tsch-tsch-lln-context]. 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 6TSCH solution MUST provide a mechanism by which mesh nodes can use the available time slots to run Phase-1 and Phase-2 KMPs and provide integrity protection to EB frames.

6. IANA Considerations

There is no IANA action required for this document.

7. Acknowledgments

We would like to thank Thomas Watteyne, Jonathan Simon, Maria Rita Palattella and Rene Struik for their valuable comments.

8. References

8.1. Normative References

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

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

[RFC6345] Duffy, P., Chakrabarti, S., Cragie, R., Ohba, Y., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA) Relay Element", RFC 6345, August 2011.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6786] Yegin, A. and R. Cragie, "Encrypting the Protocol for Carrying Authentication for Network Access (PANA) Attribute-Value Pairs", RFC 6786, November 2012.

[I-D.palattella-6tsch-terminology] Palattella, M., Thubert, P., Watteyne, T., and Q. Wang, "Terminology in IPv6 over Time Slotted Channel Hopping", draft-palattella-6tsch-terminology-00 (work in progress), March 2013.

[I-D.watteyne-6tsch-tsch-lln-context] Watteyne, T., Palattella, M., and L. Grieco, "Using IEEE802.15.4e TSCH in an LLN context: Overview, Problem Statement and Goals", draft-watteyne-6tsch-tsch-lln-context-02 (work in progress), May 2013.

[I-D.moskowitz-hip-rg-dex] Moskowitz, R., "HIP Diet EXchange (DEX)", draft-moskowitz-hip-rg-dex-06 (work in progress), May 2012.

8.2. Informative References

[RFC4137] Vollbrecht, J., Eronen, P., Petroni, N., and Y. Ohba, "State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator", RFC 4137, August 2005.

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

[RFC5705] Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", RFC 5705, March 2010.

[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.

[I-D.keoh-tls-multicast-security] Keoh, S., Kumar, S., and E. Dijk, "DTLS-based Multicast Security for Low-Power and Lossy Networks (LLNs)", draft-keoh-tls-multicast-security-00 (work in progress), October 2012.

[I-D.ietf-hip-rfc5201-bis] Moskowitz, R., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", draft-ietf-hip-rfc5201-bis-12 (work in progress), June 2013.

[I-D.draft-palattella-6tsch-terminology] Palattella, MR., Ed., Thubert, P., Watteyne, T., and Q. Wang, "Terminology in IPv6 over Time Slotted Channel Hopping. draft-palattella-6tsch-terminology-00 (work in progress) ", March 2013.

[I-D.draft-thubert-6tsch-architecture] Thubert, P., Ed., Assimiti, R., and T. Watteyne, "An Architecture for IPv6 over Time Synchronized Channel Hopping. draft-thubert-6tsch-architecture-00 (work in progress) ", March 2013.

8.3. External Informative References

[IEEE802154e] IEEE standard for Information Technology, "IEEE std. 802.15.4e, Part. 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendament 1: MAC sublayer", April 2012.

[IEEE802154]
IEEE standard for Information Technology, "IEEE std. 802.15.4, Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks", June 2011.

[ZigBeeIP]
ZigBee Public Document 15-002r00, "ZigBee IP Specification", 2013.

Appendix A. KMP candidates

A.1. Phase-1 KMP candidates

PANA [RFC5191] is the Phase-1 KMP candidate since it supports mutual authentication, stateless authentication relay function [RFC6345] and encrypted distribution of attributes [RFC6786]. The PANA Authentication Agent (PAA) is located in the coordinator of the mesh network.

A.2. Phase-2 KMP candidates

Once Phase-1 is complete by using PANA, it is assumed that node will have a certified public key (and associated private key). A candidate Phase 2 KMP must use this certified public key to perform an authentication process. As a consequence of a successful authentication some cryptographic material for unicast and multicast link protection between nodes must be generated.

A list of candidate protocols may provide the requirements defined in Section 4.2 (this is a preliminary list that may be extended in the future):

- HIP DEX [I-D.moskowitz-hip-rg-dex]. The Host Identity Protocol Diet EXchange (HIP DEX) is a lighter version of the HIP Base Exchange (HIP BEX) [I-D.ietf-hip-rfc5201-bis] specifically designed to be used in constrained devices (e.g., sensor networks). In particular, HIP DEX may be used to authenticate two IEEE 802.15.4 nodes and provide key material for a MAC layer security protocol as supported in IEEE 802.15.4. However, by just using the value of the public key and the private key is not enough to carry out the authentication between nodes. In particular, a node A and node B should not be able to successfully finish HIP DEX execution if they both have not been authenticated in Phase-1. Thus, HIP DEX will require the inclusion of the certificate of each node to achieve full mutual authentication. The information in the certificate must ensure that the node was authenticated in Phase-1. In consequence, HIP DEX must include a

CERT parameter for carrying this certificate. Once the HIP DEX protocol has successfully finished a Pair-Wise Key SA is derived. This SA is used to secure and authenticate user data, thus it can be used to provide the required keys for protecting IEEE 802.15.4 unicast MAC frames. The same message is used to refresh the Pair-Wise Key SA. So far HIP DEX only specifies how this key material is used for protecting data traffic with ESP. To distribute multicast keys HIP DEX may also use UPDATE message. For less resource-constrained devices, HIP-BEX (Basic Exchange) is more suitable than HIP-DEX since HIP-BEX has better security properties (such as use of ephemeral Diffie-Hellman) than HIP-DEX at the cost of increased complexity.

- PANA [RFC5191] and some certificate-based EAP method. Another candidate is to use PANA between node A and node B. In this case, one of the nodes (e.g. node A) acts as PaC while the other (e.g. node B) is acting as PAA. Moreover the PAA will operate in standalone mode [RFC4137]. That is, the EAP server is placed on the PAA and not in a backend authentication server. Finally, the selected EAP method must work with public key/private key cryptography. Once the PAA authentication is complete, the PaC and PAA can derive cryptographic material (for instance, from the MSK) which can be used to protect unicast MAC frames. Furthermore, by using the extension defined in [RFC6345] is possible to distribute a multicast key encrypted with the PANA SA. It is worth noting that, though this candidate solution leverages the PaC implementation from Phase-1, each node needs to deploy a PAA implementation, an EAP server and a specific EAP method, which may be different from the one used for Phase-1.

- DTLS [RFC6347]. Datagram Transport Layer Security (DTLS) is being considered in constrained devices for protecting application data traffic (e.g. CoAP). It is not only being considered for unicast application data traffic but also for multicast data traffic [I-D.keoh-tls-multicast-security]. In particular, a multicast key is distributed over an unicast DTLS channel established between two nodes (node A and node B). This multicast key is used to protect multicast traffic by using TLS records. The Phase2-KMP should be able to export this key material to the IEEE 802.15.4 MAC layer so that the protection is carried out at link layer. In [RFC5705], a mechanism for exporting key material after a TLS/DTLS execution is defined. Nevertheless, the exported key material is intended to be used in unicast communications for upper layers or protocols at upper layers. However, a mechanism for exporting multicast key is not specified. In principle, this exported key material may be used for protecting unicast IEEE 802.15.4 MAC frames. However, this usage and multicast key management using DTLS for multicast IEEE 802.15.4 protection need further investigation.

Authors' Addresses

Stephen Chasko
Landis+Gyr
3000 Mill Creek Ave.
Alpharetta, GA 30022
USA

Email: Stephen.Chasko@landisgyr.com

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

Email: sdas@appcomsci.com

Rafa Marin-Lopez
University of Murcia
Campus de Espinardo S/N, Faculty of Computer Science
Murcia 30100
Spain

Phone: +34 868 88 85 01
Email: rafa@um.es

Yoshihiro Ohba (editor)
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

Pascal Thubert
Cisco Systems, Inc
Village d'Entreprises Green Side
400, Avenue de Roumanille
Batiment T3
Biot - Sophia Antipolis 06410
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@yegin.org