IPv6 over Low Power WPAN Security Analysis
draft-daniel-6lowpan-security-analysis-02.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 20, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).
Abstract

This document discusses possible threats and security options for IPv6-over-IEEE802.15.4 networks. It is an informational document to raise awareness of security issues in IPv6 lowPan networks.

Table of Contents

1. Introduction .................................................. 3
2. Requirements .................................................. 4
3. Terminology .................................................. 5
4. Overview ...................................................... 6
5. Security Threats ............................................... 8
6. Assumptions ................................................... 10
7. 6lowpan security analysis .................................... 11
   7.1. IEEE 802.15.4 Security analysis ......................... 11
   7.2. IP Security analysis .................................... 12
8. Key Management in 6lowpan .................................. 14
   8.1. Existing Key management methods ......................... 14
   8.2. Issues with Key management in 6lowpan .................. 15
9. Security consideration in bootstrapping a 6lowpan node .... 16
10. Possible scenarios using different levels of security ....... 17
11. Security Considerations ..................................... 18
12. IANA Considerations ......................................... 19
13. Acknowledgements ............................................ 20
14. No I-D References ........................................... 21
15. References .................................................. 22
   15.1. Normative References .................................. 22
   15.2. Informative References ................................ 22
Authors’ Addresses .............................................. 23
1. Introduction

The principal object of the 6lowpan working group is to design IPv6 transmission over IEEE 802.15.4 [ieee802.15.4] networks.

IEEE 802.15.4 [ieee802.15.4] is designed to support variety of applications in personal area networks; many of applications are security sensitive.

Specifically, some of the IEEE 802.15.4 optional features actually reduce security and implementation would be limited for their extensions. The applications range from defense systems to building monitoring, fire-safety, patient monitoring etc. If the network is not secured, an intruder can inject incorrect messages to trigger false situations. Thus link-layer security is quite necessary in IEEE802.15.4 networks.

IEEE 802.15.4 is working on improving the link-layer security specification. However, this document will focus on discussing different security threats from the 6lowpan perspective and discuss different options of applying existing security methods to overcome those threats. The goal is to provide a trust model using both link-layer and IP layer security packages, if possible.

Designing a new security protocol for 6lowpan network is out of scope of this document. However, it may state desired security requirements which can be fed to the appropriate IETF security working group in order to suggest appropriate security protocols.
2. Requirements

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

This document uses terminology specific to IPv6 and DHCPv6 as defined in "Terminology" section of the DHCPv6 specification [RFC3315].
4. Overview

As described in \[RFC4919\], unlike regular IP network 6lowpan has some special characteristics such as small packet size, low bandwidth of IEEE 802.15.4 standard \[ieee802.15.4\], low power, low cost, large number of devices, etc. The security aspect, however, seems a bit tradeoff in the 6lowpan since security is always a costly function. This is particularly true to low rate WPAN. Obviously, adding security makes the issue even more challenging. For instance, when putting IPv6 on top of 6lowpan, it seems one could use IP security and turn off the security of WPAN since the security architecture defined by IEEE 802.15.4. But on the other hand, IP security is relatively mature for services at IP or other upper layers.

It is naturally questionable whether the 6lowpan devices can support IP Security (IPSec) as it is. This document explains some of difficulties of adopting IPSec in the following sections. However, Layer 2 security must be used for Layer-2 level operations such as MAC sublayer association, beaconing, orphaning, etc.

Security Considerations paper[802.15.4-ACM] outlines that IEEE802.15.4 link-layer provides access control, message integrity, message confidentiality and replay-protection services. Yet the document is not clear about key management methods, state of ACL table in the event of power loss and support of group keying. Network shared common key may be an answer for link-layer security in this case, but that is vulnerable with replay attacks and with stolen devices. However, in most common cases, network shared keying may be the simple answer to the security at the link-layer for the power-deprived, reduced function-devices, as it is easily configurable among hundreds of devices.

IPSec is mandatory to run IPv6, but considering power constraints and limited processing capability of the IEEE802.15.4 capable devices IPSec may be compute intensive; IKE messaging will not work well in low power networks as we want to reduce signaling in this network. Thus 6lowpan may need to define its own keying methods that require minimum overhead in packet-size and of course a number of signaling messages. IP-layer security will provide authentication and confidentiality between end-nodes and across multiple lowpan-links. This document later discusses applicability of IP-layer security in the case of 6lowpan network usage and applications. IP-layer security may be useful only when two nodes want to send/receive all messages securely. However, in most cases, the security may be requested at the application layer as needed, while other messages can flow in the network without security overhead.

The possible threats in this type of network are intrusion, sink-hole...
and replay attacks. A third party entity can inject bad routes in the network, act as a default router attracting all the packets to itself, or it can snoop packets and then launch replay attacks on the 6lowpan nodes. These attacks can cause harm especially when the attacker is a high-power device, such as a laptop. It can easily drain batteries of the 6lowpan devices by sending broadcast messages, redirecting routes etc.

A possible solution to security issues in the 6lowpan network might be application level security (for example, SSL) on top of link-layer security. Link-layer security protects from intrusion in the link and the application-level security protects from another user peeking at the data and impersonation.
5. Security Threats

Most of the attacks and threats against user and data security in 6lowpan are plausible and may be very destructible in effect, because of its wireless radio access and connectivity to the Internet. The security analysis of 6lowpan starts with the appreciation of various threats posed at respective ISO OSI layers. In this section, we classify and discuss the threats in layer-wise order.

6lowpan is highly susceptible to physical attacks, i.e., threats due to physical node destruction relocation and masking. By the Physical attacks, 6lowpan nodes can be condemned permanently, so the losses are irreversible. Physical attack can extract cryptographic secrets from the associated circuitry, modify programming in the sensors, and the malicious node can take control over them. These compromises can result into code modification inside the sensor node to change the mission-oriented roles of full fledged networks, let alone sensors.

In 6lowpan environment, several types of DoS attacks can be triggered in different layers. At the Physical Layer, the DoS attacks could be tempering and jamming electromagnetic (EM) signals. It can be executed by swarming the limited resources of 6lowpan devices by the high resource devices very easily. At the Link Layer, it could be collision and contention of deliberate stray frames. At the Network Layer, it could be the an outburst of packets in the name of network traffic during homing. At the Transport Layer, attacks could be performed by half open and half close TCP segments. Because of its internet connectivity, 6lowpan is highly vulnerable as those kinds of attacks can exacerbate.

Since some 6lowpan nodes might need to work together to execute a complete task, there is a burgeoning need to distribute subtasks and ensure redundancy of information. Sybil Attacks may also be triggered in such 6lowpan environments. In such a kind of attack, a node can pretend to be more than one node, using the identities of other sensors. Sybil attacks may be performed against the distributed storage, routing mechanism, data aggregation, voting, fair resource-allocation and misbehavior detection, etc. It is not very easy to be aware of a Sybil attack in progress, but measuring the usage of radio resources, the Sybil attacks may be detected, though with very little probability.

In the Black Hole attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. In this attack, the attacker listens to requests for routes then replies to the requesting nodes that it contains the high quality or shortest path to the base station. Once the malicious device is able to insert itself between the communication nodes, it is able to do anything...
with the packets passing through it. In fact, this attack can affect even the nodes those are spatially farther from the malicious node.

In the Wormhole attack, the attacker records the packets (or bits) at one location in the network and tunnels those to another location. Such attacks can be fatal to the working for the 6lowpan, since, this sort of attack does not require compromising a sensor in the network; rather it could be performed even at the initial phase when the sensors start to discover the neighboring information.
6. Assumptions

The [RFC4919] describes two security concerns as follows;

In Section 4.6 Security: Although IEEE 802.15.4 provides AES link layer security, a complete end-to-end security is needed.

In Section 5 Goals: Security threats at different layers must be clearly understood and documented. Bootstrapping of devices into a secure network could also be considered given the location, limited display, high density and ad hoc deployment of devices.

This document will meet the above considerations.

In addition, existing IP security technologies will be simplified to be implemented on the 6lowpan small devices. 6lowpan security architecture will shed off lots of fat from IP security technologies whenever available.

IEEE 802.15.4 AES (Advanced Encryption Standard) will be used for 6lowpan security architecture in conjunction with IP security whenever available.
7. 6lowpan security analysis

In this section, both IEEE 802.15.4 MAC security and IP security are tackled to search for a new 6lowpan trust models and available solution spaces if feasible. The principal object of these analysis is to improve 6lowpan security level as we use IP layer security mechanism as possible regardless of 802.15.4 vulnerable MAC security. 802.15.4 MAC enhancement and amendment are not scope of this document but IEEE 802 standard stuff.

7.1. IEEE 802.15.4 Security analysis

The MAC of IEEE 802.15.4 provides security services that are controlled by the MAC PIB (PAN Information Base). For security purpose, the MAC sublayer maintains an access control list (ACL) in its MAC PIB. By specifying a security suite in the ACL for a communication peer, a device can indicate what level security should be used (i.e., none, access control, data encryption, frame integrity, etc.) for communications with that peer. In addition, MAC sublayer offers a secured mode and an unsecured mode.

A critical function of IEEE 802.15.4 MAC is frame security. Frame security is actually a set of optional services that may be provided by the MAC to the upper layers (applications). The standard strikes a balance between the need for these services in many applications, and the desire to minimize the burden of their implementation on those applications that do not need them. As described in [802.15.4-ACM], if an application does not set any security parameters, then security is not enabled by default. The [ieee802.15.4] defines four packet types: beacon packets, data packets, acknowledgements packets and control packets for the media access control layer. It does not support security for acknowledgement packets. But on the other hand, other packet types can optionally support integrity protection and confidentiality protection for the packet’s data field.

Due to the variety of applications targeted by IEEE 802.15.4, the processes of authentication and key exchange are not defined in the standard. Devices without the key cannot decrypt the encrypted messages.

In addition, unsecured mode is suitable for some applications in which implementation cost is important, and security is either not required or obtained in other ways. An example of this is that all 6lowpan devices are assigned a default key by the administrator they can exchange data encrypted with that key. This may work in some situations, but this solution is not quite scalable. In this case, 802.15.4 node is very vulnerable.
The security service enables the MAC to select the devices with which it is willing to communicate. The device may decide to communicate with some devices, and not others. To minimize complexity, the access control service is performed on an individual device basis, rather than on groups or collections of devices.

Unlike file transfer or voice communication applications common with other protocols, IEEE 802.15.4 applications often transmit messages that do not convey secret information.

7.2. IP Security analysis

IPsec (IP security protocol) can guarantee integrity and optionally confidentiality of IP (v4 or v6) packets exchanged between two peers.

Basically, IPsec works well on non-low-power devices which are not subject to severe constraints on host software size, processing and transmission capacities. IPsec supports AH for authenticating the IP header and ESP for authenticating and encrypting the payload. The main issues of using IPsec are two-fold: (1) processing power and (2) key management. Since these tiny 6lowpan devices do not process huge number of data or communicate with many different nodes, it is not well understood if complete implementation of SADB, policy-database and dynamic key-management protocol are appropriate for these small battery-powered devices.

Given constraints existing in 6lowpan environments, IPsec might not be suitable as is to use in such environments. Especially, 6lowpan node may not be able to operate all IPsec algorithms on its own capability either FFD or RFD.

Bandwidth is a very scarce resource in 6lowpan environments. The fact that IPsec additionally requires another header (AH or ESP) in every packet, thus increasing per-packet header overhead, makes its use problematic in 6lowpan environments.

IPsec requires two communicating peers to share a secret key that is typically established dynamically with the IKE (Internet Key Exchange) protocol. Thus, it has an additional packet overhead incurred by IKE packets exchange.

If NDP (Neighbor Discovery Protocol) is applied to 6lowpan, SeND (Secure Neighbor Discovery) should at least considered to provide security in conjunction with neighbor discovery protocol. So far, CGA (Cryptographically Generated Addresses) [RFC3972] and SeND options [RFC3971] are newly designed by IETF and it works well over existing IP networks. However, RSA based CGA and SeND options could requires larger packet-size and processing time than ECC based keying.
algorithm. Therefore, it could be reasonable to use the Secure Neighbor Discovery protocol if it is extended to support ECC for 6lowpan networks application.
8. Key Management in 6lowpan

In order to provide security in 6lowpans, a robust encryption mechanism MUST be in place. Only the non-tamperable keys can provide an encryption infrastructure that is thorough enough to provide a wide range of security services such as but not limited to authentication, authorization, non-repudiation and prevention from replay attacks. In this section, the important issue of key management is discussed.

8.1. Existing Key management methods

The characteristics of sensors, communicating devices and resulting sensor networks, such as limited resources at the node and network level, lack of physical protection, unattended operation, and a close interaction with the physical environment, all make it infeasible to implement some of the most popular key exchange techniques in their literal forms for 6lowpans. In this section, we visit the three widely known schemes such as trusted-server scheme, pre-distribution scheme and public key cryptography schemes in order to reach to a pragmatic key management mechanism for 6lowpans.

The trusted-server scheme relies solely on the server for key agreement between nodes, e.g., Kerberos. If the server is compromised, the trust amongst sensor nodes is severed. Such a scheme is not suitable for sensor networks because there is usually no guarantee of communicating seamlessly with a trusted server at all the times in sensor networks.

The key agreement scheme is key pre-distribution, where key information is distributed among all sensor nodes prior to deployment. If the network deployers were to know which nodes were more likely to stay in the same neighborhood before deployment, keys MAY be decided a priori. However, because of the randomness of the deployment, knowing the set of neighbors deterministically might not be feasible. Furthermore, the presence of intruder nodes right from the network deployment and initiation time cannot be rejected outright as implausible. Some schemes like network shared keying, pair-wise keying, and group keying, have been defined as variants of key distribution. On-site key management mechanisms, while warranting the same level of security as key pre-distribution schemes have an obvious edge to cope up with network dynamics.

This class of key management scheme depends on asymmetric cryptography, such as public key certificates that are irreversible singularly. This irreversibility comes at a price—often staked by the limited computation and energy resources of sensor nodes. However, these are the hardest cryptanalyze. Some of the most
popular examples include, but are not limited to Diffie-Hellman key agreement, RSA or ECC [RFC2631]. Recent works on ECC implementation for low power devices has proven its feasibility for sensor networks. It provides security with smaller key size that is comparable to security provided by RSA or AES with much higher key size.

Network topologies for 6LowPan (i.e star and mesh) and presence of FFD and RFD makes cluster based dynamic key management schemes the most appropriate. These schemes use Master Keys; Network Keys and Links keys which could be pre installed for first round and can be distributed by key transport mechanism during later rounds. This scheme provides ease in key distribution and key revocation [ZigBee].

8.2. Issues with Key management in 6lowpan

- In a 6lowpan, a malicious node MAY sit amongst other nodes at the deployment phase—a problem of secure key assignment at bootstrap time.

- A node is compromised during the operating time of 6lowpan—A key revocation system MUST be employed.

- In a sleep-mode enabled 6lowpan, keys to sleeping nodes MUST be deprived and reinstated after such nodes resume active state.

- In case the keys are compromised, a mechanism to diagnose security violation MUST be invoked.

- It SHOULD allow and support dynamic addition of a new node.
9. Security consideration in bootstrapping a 6lowpan node

This section should discuss how does a node configures itself securely with a IPv6 router in the network. It involves assignment of IPv6 prefix and the default IPv6 router in the 6lowpan. Further details will be collaborated with 6lowpan commissioning/bootstrapping works in near future according to the 6lowpan working group rechartering.
10. Possible scenarios using different levels of security

This section may suggest example scenarios with example solutions in different cases (IPSec, SSL, other type of Solutions) although this document does not recommend or specify any security solutions. Further details will be collaborated with 6lowpan architecture works in near future according to the 6lowpan working group re-chartering.
11. Security Considerations

This document addresses only security issues around IPv6 over Low Power WPAN.
12. IANA Considerations

There is no IANA considerations.
13. Acknowledgements

Thanks to Myungjong Lee at CUNY, USA, Rabia Iqbal, Mustafa Hasan and Ali Hammad Akbar all at Ajou University for their valuable comments to improve the document. Special thanks to Jung-Hyun Oh for his valuable help on this document.
14. No I-D References

All references shown in this section MUST be added into the Informative References before publishing it officially.


15. References

15.1. Normative References


15.2. Informative References


Authors’ Addresses

Soohong Daniel Park
System Solution Laboratory, Samsung Electronics.

Email: soohong.park@samsung.com

Ki-Hyung Kim
Ajou University

Email: kkim86@ajou.ac.kr

Eunil Seo
Samsung AIT

Email: eunil.seo@samsung.com

Samita Chakrabarti
IP infusion

Email: samitac@ipinfusion.com

Julien Laganier
DoCoMo Euro-Labs

Email: lulien.ietf@laposte.net
Intellectual Property and Copyright Statements

Full Copyright Statement

Copyright (C) The IETF Trust (2008).
This document is subject to the rights, licenses and restrictions
tained in BCP 78, and except as set forth therein, the authors
retain all their rights.

This document and the information contained herein are provided on
an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE
REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE
IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL
WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE
ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS
FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any
Intellectual Property Rights or other rights that might be claimed
to pertain to the implementation or use of the technology described
in this document or the extent to which any license under such
rights might or might not be available; nor does it represent that
it has made any independent effort to identify any such rights.
Information on the procedures with respect to rights in RFC
documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any
assurances of licenses to be made available, or the result of an
attempt made to obtain a general license or permission for the use
of such proprietary rights by implementers or users of this
specification can be obtained from the IETF on-line IPR repository

The IETF invites any interested party to bring to its attention any
copyrights, patents or patent applications, or other proprietary
rights that may cover technology that may be required to implement
this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF
Administrative Support Activity (IASA).