

IPv6 over Low Power WPAN (6lowpan)
Internet-Draft
Intended status: Informational
Expires: September 16, 2011

S. Park
Samsung Electronics
K. Kim
Ajou University
W. Haddad (Ed.)
S. Chakrabarti
Ericsson
J. Laganier
Juniper
March 15, 2011

IPv6 over Low Power WPAN Security Analysis
draft-daniel-6lowpan-security-analysis-05

Abstract

This document discusses possible threats and security options for IPv6-over-IEEE802.15.4 networks. Its goal is to raise awareness about security issues in IPv6 lowPan networks.

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 September 16, 2011.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Requirements	4
3.	Terminology	5
4.	Overview	6
5.	Security Challenges	9
6.	Security Requirements	10
7.	Security Threats	11
8.	Assumptions	14
9.	6Lowpan Security Analysis	15
9.1.	IEEE 802.15.4 Security analysis	15
9.2.	IP Security analysis	16
10.	Key Management in 6Lowpan	17
10.1.	Existing Key Management Methods	17
10.2.	Issues With Key Management in 6Lowpan	18
11.	Security Consideration in Bootstrapping a 6lowpan Node	19
12.	Possible Scenarios Using Different Levels of Security	20
13.	Security Considerations	21
14.	IANA Considerations	22
15.	Acknowledgements	23
16.	No I-D References	24
17.	References	25
17.1.	Normative References	25
17.2.	Informative References	25
	Authors' Addresses	26

1. Introduction

IEEE 802.15.4 [[ieee802.15.4](#)] specification defines Physical and MAC layers targeted for the Low Rate Wireless Personal Area Networks (LR-WPAN) using short distance applications with low power and low cost communication networks, particularly for the short range applications such as Wireless Sensors Network (WSN). In an IEEE 802.15.4 compliant WPAN, a central controller device, i.e., the PAN coordinator, builds a WPAN with other devices within a small physical space known as the personal operating system. IEEE 802.15.4 is designed to support a variety of applications in personal area networks; many of these applications are security sensitive. The principal goal of the 6lowpan working group is to design IPv6 transmission over IEEE 802.15.4.

In fact, 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.

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

Designing a new security protocol for 6lowpan network is out of scope of this document. However, the document states desired security requirements, which can be fed into the appropriate IETF security working group in order to design 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 the "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, large number of devices, etc. 6lowpan devices are generally assumed to be resource-limited with respect to computation power, storage, memory and especially battery life. One common feature, which is worthy to remember is the disproportionately high cost of transmitting information as compared to performing local computation. For example, a Berkeley mote spends approximately 800 instructions as it does in sending a single bit [[Madden](#)]. It thus become a main design criteria for 6lowpan to reduce the number of bits forwarded by intermediate nodes, in order to extend the entire network's lifetime as recharging may not be practical in some deployment scenarios.

IEEE 802.15.4 nodes can operate in either secure mode or non-secure mode. Two security modes are defined in the specification in order to achieve different security objectives:

- Access Control List (ACL) mode which provides limited security services and requires each device to maintain its own ACL. This mode allows receiving frames only from nodes that are present in the device's ACL, i.e., considered as trusted nodes. Frames from non-registered devices are filtered. However, cryptographic protection is not provided in this mode.
- Secure mode provides all the security services according to the defined security suite. It provides confidentiality of the frame along with the message integrity, access control, and sequential freshness.

However, the specification is not clear about key management methods, state of ACL table in the event of power loss and support of group keying in which case, network shared common key may be an answer for the link layer security but is vulnerable to replay attacks launched from stolen devices. Yet, in most common cases, network shared keying can be the simple answer to the link layer security as it is easily configurable among large number of devices.

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 may seem possible to use IP security protocol [[RFC4301](#)] and turn off the security mechanism defined by IEEE 802.15.4. But on the other hand, IPsec is relatively mature for services at IP or upper layers. Furthermore, due to their inherent properties and/or

constraints mentioned earlier, 6lowpan poses unique challenges to which, traditional security techniques cannot be applied directly. For example, public key cryptography primitives are typically avoided (as being too expensive) as are relatively heavyweight conventional encryption methods.

Consequently, it becomes questionable whether the 6lowpan devices can support IPsec as it is. This document explains in the following

sections some of the difficulties resulting from adopting IPsec. However, Layer 2 security must be used for all associated operations such as MAC sub-layer association, beaconing, orphaning, etc.

While IPsec is mandatory with IPv6, considering the power constraints and limited processing capabilities of IEEE802.15.4 capable devices, IPsec is computationally expensive; Internet key exchange (IKEv2) messaging described in [\[RFC5996\]](#) will not work well in 6lowpans as we want to minimize the amount of signaling in these networks. Thus, 6lowpan may need to define its own keying management method(s) that requires minimum overhead in packet-size and in number of signaling messages exchange. IPsec will provide authentication and confidentiality between end-nodes and across multiple lowpan-links, and may be useful only when two nodes want to apply security to all exchanged messages. 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.

Attacks against 6lowpans can be classified into external attacks and internal ones. In an external attack, the attacker is not an authorized entity of the 6lowpan. External attacks can be further divided into two categories: passive and active. Passive attacks involve mainly eavesdropping on network's radio frequency range in an attempt to discover sensitive information. Among active attacks against 6lowpans, denial-of service (DoS) attack at the physical layer can produce devastating consequences. To this end, the attacker can broadcast a powerful signal within the WPAN zone, i.e., jamming, and paralyzes part(s) or even the entire network.

An attacker may also disable a 6lowpan node (e.g., by smashing it!) or capture one, extracts the key(s) and uses it for eavesdropping purposes and/or to directly intervene at some point in time, by injecting false but valid data in order to disturb the overall system, e.g., trigger an undesired chain of events. Consequently, a challenging issue facing 6lowpans is to provide resiliency against node capture attack.

Data collection and dissemination being their ultimate goals, 6lowpans also highlights privacy concerns. In fact, as devices are in general, getting smaller (i.e., easier to conceal) and cheaper

(i.e., easier to obtain), an obvious risk is that 6lowpan technology

might be used for privacy violation purposes, e.g., employers might spy on their employees, neighbors might spy on each other.

Possible threats in 6lowpan include intrusion, sink-hole and replay attacks. As in traditional networks, routing mechanisms in 6lowpan present another window from which, an attacker might disrupt and significantly degrade the 6lowpan overall performance. Attacks against unsecure routing aim mainly to contaminate WPAN networks with false routing information resulting in routing inconsistencies. A malicious node can also 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 laptop. It can also easily drain 6lowpan devices batteries by sending broadcast messages, redirecting routes etc.

A possible solution to address security issues in the 6lowpan networks might consist of implementing application level security, e.g., SSL, on top of link layer security. In such case, link layer security protects from intrusion and the application level security protects from another user peeking at the data and against impersonation.

5. Security Challenges

We summarize the security challenges in 6lowpan networks as it follows (for more information about this section and the following ones, please check the references):

- Minimizing resource consumption and maximizing security performance.
- 6lowpan deployment enables link attacks ranging from passive eavesdropping to active interfering.
- In-network processing involves intermediate nodes in end-to-end information transfer.
- 6lowpan communication characteristics render traditional wired based security schemes unsuitable.

6. Security Requirements

Security requirements for 6lowpan can be listed as it follows:

- Data Confidentiality: make information inaccessible to unauthorized users. For example, a 6lowpan node should not leak some of its collected data to neighboring networks.
- Data Authentication: since an adversary can easily inject messages, the receiver needs to ensure that data are originated from a trusted sources.
- Data Integrity: ensures that the received data is not altered in transit by an adversary.
- Data freshness: this could mean data freshness as well as key freshness. Informally, data freshness implies that each data is recent, and it ensures that no adversary replayed old messages.
- Availability: ensures the survivability of network services to (only) authorized parties when needed, despite a DoS attack(s).
- Robustness: ensures operation continuity despite abnormalities, such as attacks, failed nodes, etc.
- Resiliency: is the network ability to provide and maintain an acceptable level of security in case some nodes are compromised.
- Resistance: is the network ability to prevent the adversary from gaining full control of the network by node replication attack in case some nodes are compromised.
- Energy efficiency: a security scheme must be energy efficient so as to maximize network lifetime.
- Assurance: is the ability to disseminate different information at different assurance levels.

7. 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. The suggested threat model assumes that the attacker is fully capable at all times except during the deployment phase.

6lowpan is highly susceptible to physical attacks. i.e., threats due to physical node destruction relocation and masking. By physical attacks, one or multiple 6lowpan nodes can be knocked out permanently, so the losses are irreversible. Physical attack can extract cryptographic secrets from the associated circuitry, modify programming in the nodes, and may allow the malicious node to take control over them. These compromises can result into code modification inside the node and to change the mission-oriented role 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 can be launched by tampering and jamming electromagnetic (EM) signals by swarming the limited resources of 6lowpan devices with the high resource devices very easily.

Attacks on MAC layer involves collision, exhaustion and unfairness. Being always power hungry, 6lowpan devices try to sleep as often as possible in order to conserve it. Such constraints open the door for an attacker to let the device execute a large number of tasks in order to deplete its battery. This is called "sleep deprivation

torture" [[Stajano](#)]. To achieve such goal, an attacker can for example, target different destination devices with unnecessary packets, possibly in other WPANs, regardless of whether the destination WPAN and/or device actually exist or not. Such attack can also lead to depleting the PAN coordinator battery power, i.e., since the downlink packets have to be explicitly requested from the PAN coordinator, this will keep it busy (as well as an eventual destination).

An attack against network availability can consist of flooding the network by simply transmitting a large number of large(st) packets size. In such case, the attacker may degrade the network performance and drastically reduce the throughput.

In WPAN specification, the replayed message is prevented by the replay protection mechanism, i.e., sequential freshness. In a

replay-protection attack, the malicious node sends many frames containing large counters to a particular receiver, which in turn raises the replay counter up. Then, when a normal device sends a frame with a lower frame counter, it will be rejected by the receiver and thus, leading to DoS attack.

As the ACK frame integrity is not protected, it also opens the door for a malicious node to prevent a legitimate device from receiving a particular frame. This is possible by forging an ACK using the un-encrypted sequence number from the data frame and sending it to the source while creating enough interference, in order to prevent the legitimate receiver from receiving the frame. In such scenario, the source device is led to believe that the frame has been received.

A corrupted device can also attack the key distribution process since the WPAN coordinator announces the IDs of devices who are about to change the link key in plain-text in the beacon frame. Therefore, the attacker can send request packet with the ID of the legitimate node. The goal from such request is to push the coordinator to trigger a key exchange process while the legitimate recipient may not be ready.

Attacks against network layer fall into one of the following categories:

- Spoofed, altered, or replayed routing information: in this attack, the malicious node uses spoofing, altering and/or replaying to target routing information exchanged between nodes in an attempt to create routing loops, attract/repel network traffic, extend/shorten source routes, generate false error messages, etc.

- Selective forwarding: in this attack, the malicious device may refuse to forward certain messages (e.g., by dropping them). In this case, neighboring devices may conclude that the malicious device has failed and thus, try to seek another route. A more subtle form of this attack is when the malicious device selectively forward packets in which case, neighboring nodes won't be able to reach the conclusion that another route is needed which in turn, would encourage them to re-send the data packets.

- Sinkhole attack: in a sinkhole attack, the malicious device tries to get all traffic from one particular area which can potentially result in a DoS attack. In order to launch a sinkhole attack (aka blackhole attack), the attacker can listen 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 communicating nodes, he/she is able to do anything with the packets passing through it. In

fact, this attack can affect even the nodes that are spatially located farther from the malicious node.

- Sybil attack: in a Sybil attack, a single node presents multiple identities to other nodes in the WPAN. Sybil attacks pose a significant threat to geographic routing protocols and MAY be performed against the distributed storage, routing mechanism, data aggregation, voting, fair resource-allocation and misbehavior detection, etc. Note that it is not easy to detect a Sybil attack in progress (measuring the usage of radio resources MAY lead to detect it, though with very little probability).

- Wormhole attack: in a Wormhole attack, the attacker records packets (or bits) at one location in the network and tunnels them to another one. Such attacks can be devastating to the working of the 6lowpan since it does not require compromising a node in the WPAN; instead, it could be performed at the initial phase when 6lowpan nodes start to discover the neighboring information. Wormhole attacks can target

for example, routing function or application.

- Neighbor Discovery attacks: a modified version of the IPv6 Neighbor Discovery protocol (described in [[RFC4861](#)]) has been specifically designed for WPAN. However, the modified version (described in [[I-D.ietf-6lowpan-nd](#)]) inherits threats which applies in the WPAN deployment. This includes unsecured router advertisement, neighbor discovery DoS attacks. Threats against neighbor discovery protocol are described in [[RFC3756](#)].

At the transport layer, attacks could be performed by half open and half closed TCP segments. A malicious device can repeatedly forge messages carrying sequence numbers or control flags which will ultimately cause the endpoints to request retransmission of missed frames.

[8.](#) Assumptions

[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.

Park, et al.	Expires September 16, 2011	[Page 14]
--------------	----------------------------	-----------

Internet-Draft	6LoWPAN Security Analysis	March 2011
----------------	---------------------------	------------

[9.](#) 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 this 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.

[9.1.](#) IEEE 802.15.4 Security analysis

As mentioned earlier, IEEE 802.15.4 MAC layer 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 security level should be used (i.e., none, access control, data encryption, frame integrity, etc.) for communications with that peer.

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. IEEE 802.15.4 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 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.

9.2. IP Security analysis

IPsec 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 existing constraints in 6lowpan environments, IPsec may not be suitable to use in such environments, especially that 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 makes its use problematic in 6lowpan environments.

IPsec requires two communicating peers to share a secret key that is typically established dynamically with the Internet Key Exchange (IKEv2) protocol. Thus, it has an additional packet overhead incurred by IKEv2 packets exchange.

As neighbor discovery protocol will be applied to 6lowpan, Secure Neighbor Discovery (SeND) protocol [[RFC3971](#)] should be considered to provide security in conjunction with 6lowpan NDP. SeND works well over existing IP networks. However, the crypto-generated address (CGA) (described in [[RFC3972](#)]) used in SeND is based on RSA based and thus, requires larger packet-size and processing time than in the case where Elliptic Curve Cryptography (ECC) keying algorithm is used. Therefore, it could be reasonable to use the SeND protocol if

it is extended to support ECC for 6lowpan networks application.

[10.](#) 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. Key management issues are discussed in the following section.

[10.1.](#) Existing Key Management Methods

The characteristics of 6lowpan communicating devices and resulting WPANs, 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 three widely known schemes such as trusted-server scheme, pre-distribution scheme and public key cryptography schemes in order to reach 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 nodes is severed. Such scheme is not suitable for 6lowpan networks because there is usually no guarantee of seamless communication with a trusted server at anytime.

The key agreement scheme is key pre-distribution, where key information is distributed among all 6lowpan 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 6lowpan 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. ECC 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 seem 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](#)].

[10.2](#). 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.

[11.](#) Security Consideration in Bootstrapping a 6lowpan Node

This section aims to 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.

[12.](#) 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.

[13.](#) Security Considerations

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

[14.](#) IANA Considerations

There is no IANA considerations.

15. 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.

[16.](#) No I-D References

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

[ieee802.15.4] IEEE Std., 802.15.4-2003, ISBN 0-7381-3677-5, May 2003.

[802.15.4-ACM] Sastry, N. and Wagner, D., Security Considerations for IEEE 802.15.4 Networks, ACM WiSE'04, October 2004.

[Madden] Madden, S. R., Franklin, M. J., Hellerstein, J. M., and Hong, W., "TAG: a Tiny AGgregation service for ad-hoc sensor networks". In Proceedings of the 5th Annual Symposium on Operating Systems Design and Implementation, 2002.

[Stajano] Stajano, F., and Anderson, R., "The Resurrecting Duckling: Security Issues for Ubiquitous Computing". In IEEE Computer Journal, Volume 42, Issue 5, 2002.

[WSN] Shi, E., and Perrig, A., "Designing Secure Sensor Networks", In IEEE Wireless Communications, December 2004.

[MAC802154] Misic V. B., Fung J., and Misic, J., "MAC Layer Security of 802.15.4-Compliant Networks". In MASS 2005 Workshop, IEEE WSN Conference.

[SEC802154] Xiao, Y., Sethi, S., Chen, H. H., and Sun B., "Security Services and Enhancements in the IEEE 802.15.4 Wireless Sensor Networks". In IEEE GlobeCom 2005.

[SECWSN] Chen, X., Makki, K., Yen, K., and Pissinou, N., "Sensor Network Security: A Survey". In IEEE Communications Surveys & Tutorials, Volume 11, No. 2, 2nd Quarter 2009.

[ZigBee] Specification Version 1.0, December 2004.

[17.](#) References

[17.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.

[17.2.](#) Informative References

- [I-D.ietf-6lowpan-nd] Shelby, Z., Chakrabarti, S., and E. Nordmark, "Neighbor Discovery Optimization for Low-power and Lossy Networks", [draft-ietf-6lowpan-nd-15](#) (work in progress), December 2010.
- [RFC2631] Rescorla, E., "Diffie-Hellman Key Agreement Method", [RFC 2631](#), June 1999.
- [RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", [RFC 3756](#), May 2004.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), December 2005.

- [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.
- [RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", [RFC 5996](#), September 2010.

Park, et al. Expires September 16, 2011 [Page 25]

Internet-Draft 6LoWPAN Security Analysis March 2011

Authors' Addresses

Soohong Daniel Park
System Solution Laboratory, Samsung Electronics
416 Maetan-3dong, Yeongtong-gu
Suwon-si, Gyeonggi-do 442-742
KOREA

Phone: +82 31 200 4635
Email: soohong.park@samsung.com

Ki-Hyung Kim
Ajou University
San 5 Wonchun-dong, Yeongtong-gu
Suwon-si, Gyeonggi-do 442-749
KOREA

Phone: +82 31 219 2433
Email: kkim86@ajou.ac.kr

Wassim Michel Haddad
Ericsson
300 Holger Way
San Jose, CA 95134
US

Phone: +1 646 256 2030
Email: Wassim.Haddad@ericsson.com

Samita Chakrabarti
Ericsson
300 Holger Way
San Jose, CA
USA

Email: samita.chakrabarti@ericsson.com

Julien Laganier
Juniper
Sunnyvale, CA
USA

Email: Julien.ietf@laposte.net