Networking Working Group	T. Tsao
Internet-Draft	R. Alexander
Intended status: Informational	Cooper Power Systems
Expires: April 3, 2011	M. Dohler
	CTTC
	V. Daza
	A. Lozano
	Universitat Pompeu Fabra
	September 30, 2010

TOC

A Security Framework for Routing over Low Power and Lossy Networks
draft-ietf-roll-security-framework-01

Abstract

This document presents a security framework for routing over low power and lossy networks (LLN). The development builds upon previous work on routing security and adapts the assessments to the issues and constraints specific to low power and lossy networks. A systematic approach is used in defining and evaluating the security threats and identifying applicable countermeasures. These assessments provide the basis of the security recommendations for incorporation into low power, lossy network routing protocols. As an illustration, this framework is applied to IPv6 Routing Protocol for Low Power and Lossy Networks (RPL).

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119].

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 April 3, 2011.

Table of Contents

---

1. Terminology

TOC

This document adopts and conforms to the terminology defined in [I-D.ietf-roll-terminology] (Vasseur, J., "Terminology in Low power And Lossy Networks," September 2010.) and in [RFC4949] (Shirey, R., "Internet Security Glossary, Version 2," August 2007.), with the following addition:

> **Node** An element of a low power lossy network that may be a router or a host.

TOC

2. Introduction

In recent times, networked electronic devices have found an increasing number of applications in various fields. Yet, for reasons ranging from operational application to economics, these wired and wireless devices are often supplied with minimum physical resources; the constraints include those on computational resources (RAM, clock speed, storage), communication resources (duty cycle, packet size, etc.), but also form factors that may rule out user access interface (e.g., the housing of a small stick-on switch), or simply safety considerations (e.g., with gas meters). As a consequence, the resulting networks are more prone to loss of traffic and other vulnerabilities. The proliferation of these low power and lossy networks (LLNs), however, are drawing efforts to examine and address their potential networking challenges. Securing the establishment and maintenance of network connectivity among these deployed devices becomes one of these key challenges.

This document presents a framework for securing Routing Over LLNs (ROLL) through an analysis that starts from the routing basics. The objective is two-fold. First, the framework will be used to identify pertinent security issues. Second, it will facilitate both the assessment of a protocol's security threats and the identification of the necessary features for development of secure protocols for the ROLL Working Group.

The approach adopted in this effort proceeds in four steps, to examine security issues in ROLL, to analyze threats and attacks, to consider the countermeasures, and then to make recommendations for securing ROLL. The basis is found on identifying the assets and points of access of routing and evaluating their security needs based on the Confidentiality, Integrity, and Availability (CIA) model in the context of LLN. The utility of this framework is demonstrated with an application to IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) [I-D.ietf-roll-rpl] (Winter, T., Thubert, P., and R. Team, “RPL: IPv6 Routing Protocol for Low power and Lossy Networks,” July 2010.).

---

3. Considerations on ROLL Security

TOC

Security, in essence, entails implementing measures to ensure controlled state changes on devices and network elements, both based on external inputs (received via communications) or internal inputs (physical security of device itself and parameters maintained by the device, including, e.g., clock). A security assessment can therefore begin with a focus on the assets or elements of information that may be the target of the state changes and the access points in terms of interfaces and protocol exchanges through which such changes may occur. In the case of routing security the focus is directed towards the

elements associated with the establishment and maintenance of network connectivity.

This section sets the stage for the development of the framework by applying the systematic approach proposed in [Myagmar2005] (Myagmar, S., Lee, AJ., and W. Yurcik, “Threat Modeling as a Basis for Security Requirements,” Aug 29, 2005.) to the routing security problem, while also drawing references from other reviews and assessments found in the literature, particularly, [RFC4593] (Barbir, A., Murphy, S., and Y. Yang, “Generic Threats to Routing Protocols,” October 2006.) and [Karlof2003] (Karlof, C. and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” September 2003.); thus, the work presented herein may find use beyond routing for LLNs. The subsequent subsections begin with a focus on the elements of a generic routing process that is used to establish routing assets and points of access to the routing functionality. Next, the CIA security model is briefly described. Then, consideration is given to issues specific to or amplified in LLNs. This section concludes with the formulation of a set of security objectives for ROLL.

3.1. Routing Assets and Points of Access

TOC

An asset implies an important system component (including information, process, or physical resource), the access to, corruption or loss of which adversely affects the system. In network routing, assets lie in the routing information, routing process, and node's physical resources. That is, the access to, corruption, or loss of these elements adversely affects system routing. In network routing, a point of access refers to the point of entry facilitating communication with or other interaction with a system component in order to use system resources to either manipulate information or gain knowledge of the information contained within the system. Security of the routing protocol must be focused on the assets of the routing nodes and the points of access of the information exchanges and information storage that may permit routing compromise. The identification of routing assets and points of access hence provides a basis for the identification of associated threats and attacks.

This subsection identifies assets and points of access of a generic routing process with a level-0 data flow diagram [Yourdon1979] (Yourdon, E. and L. Constantine, “Structured Design,” 1979.) revealing how the routing protocol interacts with its environment. In particular, the use of the data flow diagram allows for a clear, concise model of the routing functionality; it also has the benefit of showing the manner in which nodes participate in the routing process, thus providing context when later threats and attacks are considered. The goal of the model is to be as detailed as possible so that corresponding components and mechanisms in an individual routing

protocol can be readily identified, but also to be as general as possible to maximize the relevancy of this effort for the various existing and future protocols. Nevertheless, there may be discrepancies, likely in the form of additional elements, when the model is applied to some protocols. For such cases, the analysis approach laid out in this document should still provide a valid and illustrative path for their security assessment.
Figure 1 (Data Flow Diagram of a Generic Routing Process) shows that nodes participating in the routing process transmit messages to discover neighbors and to exchange routing information; routes are then generated and stored. The nodes use the derived routes for making forwarding decisions.

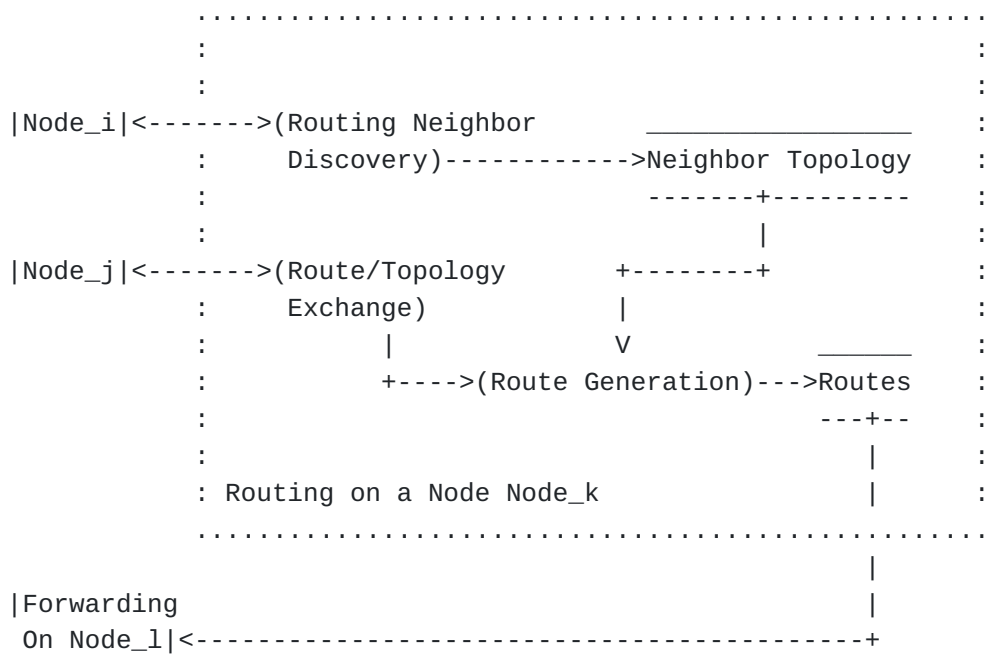

Figure 1: Data Flow Diagram of a Generic Routing Process

It is seen from Figure 1 (Data Flow Diagram of a Generic Routing Process) that

*Assets include

-routing and/or topology information;

-communication channel resources (bandwidth);

-node resources (computing capacity, memory, and remaining energy);

-node identifiers (including node identity and ascribed attributes such as relative or absolute node location).

*Points of access include

-neighbor discovery;

-route/topology exchange;

-node physical interfaces (including access to data storage).

A focus on the above list of assets and points of access enables a more directed assessment of routing security; for example, it is readily understood that some routing attacks are in the form of attempts to misrepresent routing topology. Indeed, the intention is to be comprehensive; nonetheless, the discussions to follow on physical related issues are not related to routing protocol design but provided for reference since they do have direct consequences on the security of routing.

3.2. The CIA Security Reference Model

TOC

At the conceptual level, security within an information system in general and applied to ROLL in particular is concerned with the primary issues of confidentiality, integrity, and availability. In the context of ROLL:

Confidentiality Confidentiality involves the protection of routing information as well as routing neighbor maintenance exchanges so that only authorized and intended network entities may view or access it. Because LLNs are most commonly found on publicly accessible shared medium, e.g., air or wiring in a building, and

sometimes formed ad hoc, confidentiality also extends to the neighbor state and database information within the routing device since the deployment of the network creates the potential for unauthorized access to the physical devices themselves.

Integrity Integrity, as a security principle, entails the protection of routing information and routing neighbor maintenance exchanges, as well as derived information maintained in the database, from misuse or unauthorized and improper modification. In addition, integrity also requires the authenticity of claimed identity in the origin and destination of a message, access and removal of data, execution of the routing process, and use of computing and energy resources.

Availability Availability ensures that routing information exchanges and forwarding services need to be available when they are required for the functioning of the serving network. Availability will apply to maintaining efficient and correct operation of routing and neighbor discovery exchanges (including needed information) and forwarding services so as not to impair or limit the network's central traffic flow function.

It is noted that, besides those captured in the CIA model, assurance of no denial of the transmission and/or reception of a message, i.e., non-repudiation, is a security interest under certain circumstances. With respect to routing, non-repudiation will involve providing some ability to allow traceability or network management review of participants of the routing process including the ability to determine the events and actions leading to a particular routing state. Non-repudiation implies after the fact and thus relies on the logging or other capture of on-going routing exchanges and signatures. Given the limited resources of a node and potentially the communication channel, and considering the operating mode associated with LLNs, routing transaction logging or auditing process communication overhead will not be practical; as such, non-repudiation in the context of routing is not further considered as a ROLL security issue.

3.3. Issues Specific to or Amplified in LLNs

TOC

The work [RFC5548] (Dohler, M., Watteyne, T., Winter, T., and D. Barthel, “Routing Requirements for Urban Low-Power and Lossy Networks,” May 2009.) and [RFC5673] (Pister, K., Thubert, P., Dwars, S., and T. Phinney, “Industrial Routing Requirements in Low-Power and Lossy Networks,” October 2009.), [RFC5826] (Brandt, A., Buron, J., and G. Porcu, “Home Automation Routing Requirements in Low-Power and Lossy Networks,” April 2010.), and [RFC5867] (Martocci, J., De Mil, P., Riou, N., and W. Vermeylen, “Building Automation Routing Requirements in Low-

Power and Lossy Networks," June 2010.) have identified specific issues and constraints of routing in LLNs for the urban, industrial, home automation, and building automation application domains, respectively. The following is a list of observations and evaluation of their impact on routing security considerations.

Limited energy, memory, and processing node resources As a consequence of these constraints, there is an even more critical need than usual for a careful trade study on which and what level of security services are to be afforded during the system design process. In addition, the choices of security mechanisms are more stringent. Synchronization of security states with sleepy nodes is yet another issue.

Large scale of rolled out network The possibly numerous nodes to be deployed, e.g., an urban deployment can see several hundreds of thousands of nodes, as well as the generally low level of expertise expected of the installers, make manual on-site configuration unlikely. Prolonged rollout and delayed addition of nodes, which may be from old inventory, over the lifetime of the network, also complicate the operations of key management.

Autonomous operations Self-forming and self-organizing are commonly prescribed requirements of LLNs. In other words, a routing protocol designed for LLNs needs to contain elements of ad hoc networking and in most cases cannot rely on manual configuration for initialization or local filtering rules. Network topology/ ownership changes, partitioning or merging, as well as node replacement, can all contribute to key management issues.

Highly directional traffic Some types of LLNs see a high percentage of their total traffic traverse between the nodes and the Lln Border Routers (LBRs) where the LLNs connect to non-LLNs. The special routing status of and the greater volume of traffic near the LBRs have routing security consequences. In fact, when Point-to-MultiPoint (P2MP) and MultiPoint-to-Point (MP2P) traffic represents a majority of the traffic, routing attacks consisting of advertising low route cost may cause serious damages.

Unattended locations and limited physical security Many applications have the nodes deployed in unattended or remote locations; furthermore, the nodes themselves are often built with minimal physical protection. These constraints lower the barrier of accessing the data or security material stored on the nodes through physical means.

Support for mobility On the one hand, only a number of applications require the support of mobile nodes, e.g., a home LLN that includes nodes on wearable health care devices or an industry LLN

> that includes nodes on cranes and vehicles. On the other hand, if a routing protocol is indeed used in such applications, it will clearly need to have corresponding security mechanisms.
>
> **Support for multicast and anycast** Support for multicast and anycast is called out chiefly for large-scale networks. Since application of these routing mechanisms in autonomous operations of many nodes is new, the consequence on security requires careful consideration.

The above list considers how a LLN's physical constraints, size, operations, and varieties of application areas may impact security. The following subsection sets up the security objectives for the routing protocol designed by the ROLL WG.

3.4. ROLL Security Objectives

TOC

This subsection applies the CIA model to the routing assets and access points, taking into account the LLN issues, to develop a set of ROLL security objectives.
Since the fundament function of a routing protocol is to build routes for forwarding packets, it is essential to ensure that

- routing/topology information is not tampered during transfer and in storage;
- routing/topology information is not misappropriated;
- routing/topology information is available when needed.

In conjunction, it is necessary to be assured of

- the authenticity and legitimacy of the participants of the routing neighbor discovery process;
- the routing/topology information received was faithfully generated according to the protocol design.

However, when trust cannot be fully vested through authentication of the principals alone, i.e., concerns of insider attack, assurance of the truthfulness and timeliness of the received routing/topology information is necessary. With regard to confidentiality, protecting the routing/topology information from eavesdropping or unauthorized exposure is in itself less pertinent in general to the routing function.
One of the main problems of synchronizing security states of sleepy nodes, as listed in the last subsection, lies in difficulties in

authentication; these nodes may not have received in time the most recent update of security material. Similarly, the issues of minimal manual configuration, prolonged rollout and delayed addition of nodes, and network topology changes also complicate key management. Hence, routing in LLNs needs to bootstrap the authentication process and allow for flexible expiration scheme of authentication credentials.
The vulnerability brought forth by some special-function nodes, e.g., LBRs, requires the assurance, particularly in a security context,

- of the availability of communication channels and node resources;
- that the neighbor discovery process operates without undermining routing availability.

There are other factors which are not part of a ROLL protocol but directly affecting its function. These factors include weaker barrier of accessing the data or security material stored on the nodes through physical means; therefore, the internal and external interfaces of a node need to be adequate for guarding the integrity, and possibly the confidentiality, of stored information, as well as the integrity of routing and route generation processes.
Each individual system's use and environment will dictate how the above objectives are applied, including the choices of security services as well as the strengths of the mechanisms that must be implemented. The next two sections take a closer look at how the ROLL security objectives may be compromised and how those potential compromises can be countered.

---

4. Threats and Attacks

TOC

This section outlines general categories of threats under the CIA model and highlights the specific attacks in each of these categories for ROLL. As defined in [RFC4949] (Shirey, R., “Internet Security Glossary, Version 2,” August 2007.), a threat is "a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm." An attack is "an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system."
The subsequent subsections consider the threats and their realizing attacks that can cause security breaches under the CIA model to the assets identified in Section 3.1 (Routing Assets and Points of Access). The analysis steps through the security concerns of each routing asset and looks at the attacks that can exploit points of access. The manifestation of the attacks is assumed to be from either inside or

outside attackers, whose capabilities may be limited to node-equivalent or more sophisticated computing platforms.

4.1. Threats and Attacks on Confidentiality

TOC

The assessment in Section 3.2 (The CIA Security Reference Model) indicates that information assets are exposed to confidentiality threats from all points of access.

4.1.1. Routing Exchange Exposure

TOC

Routing exchanges include both routing information as well as information associated with the establishment and maintenance of neighbor state information.
The exposure of routing information exchanged will allow unauthorized sources to gain access to the content of the exchanges between communicating nodes. The exposure of neighbor state information will allow unauthorized sources to gain knowledge of communication links between routing nodes that are necessary to maintain routing information exchanges.
The forms of attack that allow unauthorized access or exposure of routing exchange information, as reported in the literature, include

- *Deliberate exposure;
- *Sniffing;
- *Traffic analysis.

4.1.2. Routing Information (Routes and Network Topology) Exposure

TOC

Routes and neighbor topology information are the products of the routing process that are stored within the node device databases.
The exposure of this information will allow unauthorized sources to gain direct access to the configuration and connectivity of the network thereby exposing routing to targeted attacks on key nodes or links.
Since routes and neighbor topology information is stored within the node device, threats or attacks on the confidentiality of the information will apply to the physical device including specified and unspecified internal and external interfaces.

The forms of attack that allow unauthorized access or exposure of the routing information (other than occurring through explicit node exchanges) will include

- *Physical device compromise;
- *Remote device access attacks (including those occurring through remote network management or software/field upgrade interfaces).

More detailed descriptions of the exposure attacks on routing exchange and information will be given in Section 5 (Countermeasures) together with the corresponding countermeasures.

4.2. Threats and Attacks on Integrity

TOC

The assessment in Section 3.2 (The CIA Security Reference Model) indicates that information and identity assets are exposed to integrity threats from all points of access.

4.2.1. Routing Information Manipulation

TOC

Manipulation of routing information will allow unauthorized sources to influence the operation and convergence of the routing protocols and ultimately impact the forwarding decisions made in the network. Manipulation of topology and reachability information will allow unauthorized sources to influence the nodes with which routing information is exchanged and updated. The consequence of manipulating routing exchanges can thus lead to sub-optimality and fragmentation or partitioning of the network by restricting the universe of routers with which associations can be established and maintained. For example, being able to attract network traffic can make a blackhole attack more damaging.
The forms of attack that allow manipulation to compromise the content and validity of routing information include

- *Falsification, including overclaiming and misclaiming;
- *Routing information replay;
- *Byzantine (internal) attacks that permit corruption of routing information in the node even where the node continues to be a validated entity within the network;
- *Physical device compromise.

4.2.2. Node Identity Misappropriation

TOC

Falsification or misappropriation of node identity between routing participants opens the door for other attacks; it can also cause incorrect routing relationships to form and/or topologies to emerge. Routing attacks may also be mounted through less sophisticated node identity misappropriation in which the valid information broadcast or exchanged by a node is replayed without modification. The receipt of seemingly valid information that is however no longer current can result in routing disruption, and instability (including failure to converge). Without measures to authenticate the routing participants and to ensure the freshness and validity of the received information the protocol operation can be compromised. The forms of attack that misuse node identity include

*Identity attacks, including Sybil attacks in which a malicious node illegitimately assumes multiple identities;

*Routing information replay.

4.3. Threats and Attacks on Availability

TOC

The assessment in Section 3.2 (The CIA Security Reference Model) indicates that the process and resources assets are exposed to availability threats; attacks of this category may exploit directly or indirectly information exchange or forwarding.

4.3.1. Routing Exchange Interference or Disruption

TOC

Interference or disruption of routing information exchanges will allow unauthorized sources to influence the operation and convergence of the routing protocols by impeding the regularity of routing information exchange.
The forms of attack that allow interference or disruption of routing exchange include

*Routing information replay;

*HELLO flood attacks and ACK spoofing;

*Overload attacks.

4.3.2. Network Traffic Forwarding Disruption

TOC

The disruption of the network traffic forwarding capability of the network will undermine the central function of network routers and the ability to handle user traffic. This threat and the associated attacks affect the availability of the network because of the potential to impair the primary capability of the network.
The forms of attack that allows disruption of network traffic forwarding include [Karlof2003] (Karlof, C. and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” September 2003.)

*Selective forwarding attacks;

*Wormhole attacks;

*Sinkhole attacks.

For reference, Figure 2 (Selective Forwarding, Wormhole, and Sinkhole Attacks) depicts the aforementioned three types of attacks.

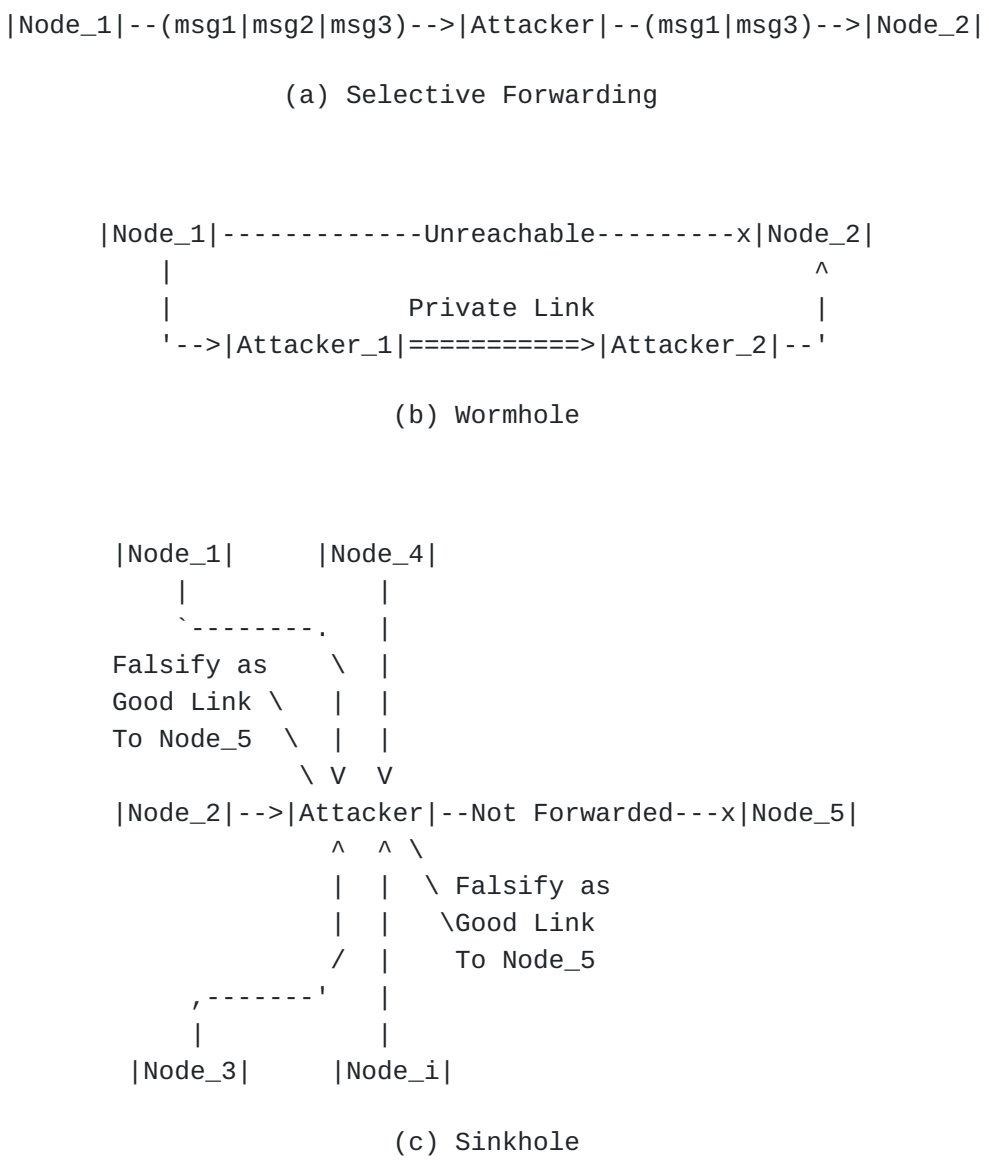

Figure 2: Selective Forwarding, Wormhole, and Sinkhole Attacks

---

4.3.3. Communications Resource Disruption

TOC

Attacks mounted against the communication channel resource assets needed by the routing protocol can be used as a means of disrupting its operation. However, while various forms of Denial of Service (DoS) attacks on the underlying transport subsystem will affect routing protocol exchanges and operation (for example physical layer RF jamming

in a wireless network or link layer attacks), these attacks cannot be countered by the routing protocol. As such, the threats to the underlying transport network that supports routing is considered beyond the scope of the current document. Nonetheless, attacks on the subsystem will affect routing operation and so must be directly addressed within the underlying subsystem and its implemented protocol layers.

4.3.4. Node Resource Exhaustion

TOC

A potential security threat to routing can arise from attempts to exhaust the node resource asset by initiating exchanges that can lead to the undue utilization of exhaustion of processing, memory or energy resources. The establishment and maintenance of routing neighbors opens the routing process to engagement and potential acceptance of multiple neighboring peers. Association information must be stored for each peer entity and for the wireless network operation provisions made to periodically update and reassess the associations. An introduced proliferation of apparent routing peers can therefore have a negative impact on node resources.
Node resources may also be unduly consumed by the attackers attempting uncontrolled topology peering or routing exchanges, routing replays, or the generating of other data traffic floods. Beyond the disruption of communications channel resources, these threats may be able to exhaust node resources only where the engagements are able to proceed with the peer routing entities. Routing operation and network forwarding functions can thus be adversely impacted by node resources exhaustion that stems from attacks that include

- *Identity (including Sybil) attacks;
- *Routing information replay attacks;
- *HELLO flood attacks and ACK spoofing;
- *Overload attacks.

---

5. Countermeasures

TOC

By recognizing the characteristics of LLNs that may impact routing and identifying potential countermeasures, this framework provides the basis for developing capabilities within ROLL protocols to deter the identified attacks and mitigate the threats. The following subsections

consider such countermeasures by grouping the attacks according to the classification of the CIA model so that associations with the necessary security services are more readily visible. However, the considerations here are more systematic than confined to means available only within routing; the next section will then distill and make recommendations appropriate for a secured ROLL protocol.

5.1. Confidentiality Attack Countermeasures

TOC

Attacks on confidentiality may be mounted at the level of the routing information assets, at the points of access associated with routing exchanges between nodes, or through device interface access. To gain access to routing/topology information, the attacker may rely on a compromised node that deliberately exposes the information during the routing exchange process, may rely on passive sniffing or analysis of routing traffic, or may attempt access through a component or device interface of a tampered routing node.

5.1.1. Countering Deliberate Exposure Attacks

TOC

A deliberate exposure attack is one in which an entity that is party to the routing process or topology exchange allows the routing/topology information or generated route information to be exposed to an unauthorized entity during the exchange.

A prerequisite to countering this type of confidentiality attacks associated with the routing/topology exchange is to ensure that the communicating nodes are authenticated prior to data encryption applied in the routing exchange. Authentication ensures that the nodes are who they claim to be even though it does not provide an indication of whether the node has been compromised.

To prevent deliberate exposure, the process that communicating nodes use for establishing communication session keys must be symmetric at each node so that neither node can independently weaken the confidentiality of the exchange without the knowledge of its communicating peer. A deliberate exposure attack will therefore require more overt and independent action on the part of the offending node.

Note that the same measures which apply to securing routing/topology exchanges between operational nodes must also extend to field tools and other devices used in a deployed network where such devices can be configured to participate in routing exchanges.

TOC

5.1.2. Countering Sniffing Attacks

A sniffing attack seeks to breach routing confidentiality through passive, direct analysis and processing of the information exchanges between nodes. A sniffing attack in an LLN that is not based on a physical device compromise will rely on the attacker attempting to directly derive information from the over-the-shared-medium routing/ topology communication exchange (neighbor discovery exchanges may of necessity be conducted in the clear thus limiting the extent to which the information can be kept confidential).

Sniffing attacks can be directly countered through the use of data encryption for all routing exchanges. Only when a validated and authenticated node association is completed will routing exchange be allowed to proceed using established session confidentiality keys and an agreed confidentiality algorithm. The level of security applied in providing confidentiality will determine the minimum requirement for an attacker mounting this passive security attack. The possibility of incorporating options for security level and algorithms is further considered in Section 6.5 (Consideration on Matching Application Domain Needs). Because of the resource constraints of LLN devices, symmetric (private) key session security will provide the best tradeoff in terms of node and channel resource overhead and the level of security achieved. This will of course not preclude the use of asymmetric (public) key encryption during the session key establishment phase.

As with the key establishment process, data encryption must include an authentication prerequisite to ensure that each node is implementing a level of security that prevents deliberate or inadvertent exposure. The authenticated key establishment will ensure that confidentiality is not compromised by providing the information to an unauthorized entity (see also [Huang2003] (Huang, Q., Cukier, J., Kobayashi, H., Liu, B., and J. Zhang, “Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks,” Sept. 19 2003.)).

Based on the current state of the art, a minimum 128-bit key length should be applied where robust confidentiality is demanded for routing protection. This session key shall be applied in conjunction with an encryption algorithm that has been publicly vetted and where applicable approved for the level of security desired. Algorithms such as the Advanced Encryption Standard (AES) [FIPS197] (, “Federal Information Processing Standards Publication 197,” Nov. 26 2006.), adopted by the U.S. government, or Kasumi-Misty [Kasumi3gpp] (, “3GPP TS 35.202 Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification,” 2009.), adopted by the 3GPP 3rd generation wireless mobile consortium, are examples of symmetric-key algorithms capable of ensuring robust confidentiality for routing exchanges. The key length, algorithm and mode of operation will be selected as part of the overall security tradeoff that also achieves a balance with the level of confidentiality afforded by the physical device in protecting the routing assets (see Section 5.1.4 (Countering Physical Device Compromise) below).

As with any encryption algorithm, the use of ciphering synchronization parameters and limitations to the usage duration of established keys should be part of the security specification to reduce the potential for brute force analysis.

5.1.3. Countering Traffic Analysis

TOC

Traffic analysis provides an indirect means of subverting confidentiality and gaining access to routing information by allowing an attacker to indirectly map the connectivity or flow patterns (including link-load) of the network from which other attacks can be mounted. The traffic analysis attack on a LLN, especially one founded on shared medium, may be passive and relying on the ability to read the immutable source/destination routing information that must remain unencrypted to permit network routing. Alternatively, attacks can be active through the injection of unauthorized discovery traffic into the network. By implementing authentication measures between communicating nodes, active traffic analysis attacks can be prevented within the LLN thereby reducing confidentiality vulnerabilities to those associated with passive analysis.

One way in which passive traffic analysis attacks can be muted is through the support of load balancing that allows traffic to a given destination to be sent along diverse routing paths. Where the routing protocol supports load balancing along multiple links at each node, the number of routing permutations in a wide area network surges thus increasing the cost of traffic analysis. Network analysis through this passive attack will require a wider array of analysis points and additional processing on the part of the attacker. In LLNs, the diverse radio connectivity and dynamic links (including potential frequency hopping), or a complex wiring system hidden from sight, will help to further mitigate traffic analysis attacks when load balancing is implemented.

The only means of fully countering a traffic analysis attack is through the use of tunneling (encapsulation) where encryption is applied across the entirety of the original packet source/destination addresses. With tunneling there is a further requirement that the encapsulating intermediate nodes apply an additional layer of routing so that traffic arrives at the destination through dynamic routes. For some LLNs, memory and processing constraints as well as the limitations of the communication channel will preclude both the additional routing traffic overhead and the node implementation required for tunneling countermeasures to traffic analysis.

TOC

5.1.4. Countering Physical Device Compromise

Section 4 (Threats and Attacks) identified that many threats to the routing functionality may involve compromised devices. For the sake of completeness, this subsection examines how to counter physical device compromise, without restricting the consideration to only those methods and apparatuses available to a LLN routing protocol.

Given the distributed nature of LLNs and the varying environment of deployed devices, confidentiality of routing assets and points of access may rely heavily on the security of the routing devices. One means of precluding attacks on the physical device is to prevent physical access to the node through other external security means. However, given the environment in which many LLNs operate, preventing unauthorized access to the physical device cannot be assured. Countermeasures must therefore be employed at the device and component level so that routing/topology or neighbor information and stored route information cannot be accessed even if physical access to the node is obtained.

With the physical device in the possession of an attacker, unauthorized information access can be attempted by probing internal interfaces or device components. Device security must therefore move to preventing the reading of device processor code or memory locations without the appropriate security keys and in preventing the access to any information exchanges occurring between individual components. Information access will then be restricted to external interfaces in which confidentiality, integrity and authentication measures can be applied.

To prevent component information access, deployed routing devices must ensure that their implementation avoids address or data buses being connected to external general purpose input/output (GPIO) pins. Beyond this measure, an important component interface to be protected against attack is the Joint Test Action Group (JTAG) interface used for component and populated circuit board testing after manufacture. To provide security on the routing devices, components should be employed that allow fuses on the JTAG interfaces to be blown to disable access. This will raise the bar on unauthorized component information access within a captured device.

At the device level a key component information exchange is between the microprocessor and it associated external memory. While encryption can be implemented to secure data bus exchanges, the use of integrated physical packaging which avoids inter-component exchanges (other than secure external device exchanges) will increase routing security against a physical device interface attack. With an integrated package and disabled internal component interfaces, the level of physical device security can be controlled by managing the degree to which the device packaging is protected against expert physical decomposition and analysis.

The device package should be hardened such that attempts to remove the integrated components will result in damage to access interfaces, ports

or pins that prevent retrieval of code or stored information. The degree of Very Large Scale Integration (VLSI) or Printed Circuit Board (PCB) package security through manufacture can be selected as a tradeoff or desired security consistent with the level of security achieved by measures applied for other routing assets and points of access. With package hardening and restricted component access countermeasures, the security level will be raised to that provided by measures employed at the external communications interfaces.

Another area of node interface vulnerability is that associated with interfaces provided for remote software or firmware upgrades. This may impact both routing information and routing/topology exchange security where it leads to unauthorized upgrade or change to the routing protocol running on a given node as this type of attack can allow for the execution of compromised or intentionally malicious routing code on multiple nodes. Countermeasures to this device interface confidentiality attack needs to be addressed in the larger context of node remote access security. This will ensure not only the authenticity of the provided code (including routing protocol) but that the process is initiated by an authorized (authenticated) entity.

The above identified countermeasures against attacks on routing information confidentiality through internal device interface compromise must be part of the larger LLN system security as they cannot be addressed within the routing protocol itself. Similarly, the use of field tools or other devices that allow explicit access to node information must implement security mechanisms to ensure that routing information can be protected against unauthorized access. These protections will also be external to the routing protocol and hence not part of ROLL.

5.1.5. Countering Remote Device Access Attacks

TOC

Where LLN nodes are deployed in the field, measures are introduced to allow for remote retrieval of routing data and for software or field upgrades. These paths create the potential for a device to be remotely accessed across the network or through a provided field tool. In the case of network management a node can be directly requested to provide routing tables and neighbor information.

To ensure confidentiality of the node routing information against attacks through remote access, any device local or remote requesting routing information must be authenticated to ensure authorized access. Since remote access is not invoked as part of a routing protocol security of routing information stored on the node against remote access will not be addressable as part of the routing protocol.

TOC

5.2. Integrity Attack Countermeasures

Integrity attack countermeasures address routing information manipulation, as well as node identity and routing information misuse. Manipulation can occur in the form of falsification attack and physical compromise. To be effective, the following development considers the two aspects of falsification, namely, the tampering actions and the overclaiming and misclaiming content. The countering of physical compromise was considered in the previous section and is not repeated here. With regard to misuse, there are two types of attacks to be deterred, identity attacks and replay attacks.

5.2.1. Countering Tampering Attacks

TOC

Tampering may occur in the form of altering the message being transferred or the data stored. Therefore, it is necessary to ensure that only authorized nodes can change the portion of the information that is allowed to be mutable, while the integrity of the rest of the information is protected, e.g., through well-studied cryptographic mechanisms.
Tampering may also occur in the form of insertion or deletion of messages during protocol changes. Therefore, the protocol needs to ensure the integrity of the sequence of the exchange sequence.
The countermeasure to tampering needs to

- implement access control on storage;
- provide data integrity service to transferred messages and stored data;
- include sequence number under integrity protection.

5.2.2. Countering Overclaiming and Misclaiming Attacks

TOC

Both overclaiming and misclaiming aim to introduce false routes or topology that would not be generated by the network otherwise, while there is not necessarily tampering. The requisite for a counter is the capability to determine unreasonable routes or topology.
The counter to overclaiming and misclaiming may employ

- comparison with historical routing/topology data;
- designs which restrict realizable network topologies.

5.2.3. Countering Identity (including Sybil) Attacks

TOC

Identity attacks, sometimes simply called spoofing, seek to gain or damage assets whose access is controlled through identity. In routing, an identity attacker can illegitimately participate in routing exchanges, distribute false routing information, or cause an invalid outcome of a routing process.

A perpetrator of Sybil attacks assumes multiple identities. The result is not only an amplification of the damage to routing, but extension to new areas, e.g., where geographic distribution is explicit or implicit an asset to an application running on the LLN, for example, the LBR in a P2MP or MP2P LLN.

The countering of identity attacks need to ensure the authenticity and liveliness of the parties of a message exchange. The means may be through the use of shared key or public key based authentication scheme. On the one hand, the large-scale nature of the LLNs makes the network-wide shared key scheme undesirable from a security perspective; on the other hand, public-key based approaches generally require more computational resources. Each system will need to make trade-off decisions based on its security requirements. As an example, [Wander2005] (Wander, A., Gura, N., Eberle, H., Gupta, V., and S. Shantz, “Energy analysis of public-key cryptography for wireless sensor networ,” March 8-12 2005.) compared the energy consumption between two public-key algorithms on a low-power microcontroller, with reference to a symmetric-key algorithm and a hash algorithm.

5.2.4. Countering Routing Information Replay Attacks

TOC

In routing, message replay can result in false topology and/or routes. The counter of replay attacks need to ensure the freshness of the message. On the one hand, there are a number of mechanisms commonly used for countering replay, e.g., with a counter. On the other hand, the choice should take into account how a particular mechanism is made available in a LLN. For example, many LLNs have a central source of time and have it distributed by relaying, such that secured time distribution becomes a prerequisite of using timestamping to counter replay.

TOC

5.2.5. Countering Byzantine Routing Information Attacks

Where a node is captured or compromised but continues to operate for a period with valid network security credentials, the potential exists for routing information to be manipulated. This compromise of the routing information could thus exist in spite of security countermeasures that operate between the peer routing devices. Consistent with the end-to-end principle of communications, such an attack can only be fully addressed through measures operating directly between the routing entities themselves or by means of external entities able to access and independently analyze the routing information. Verification of the authenticity and liveliness of the routing principals can therefore only provide a limited counter against internal (Byzantine) node attacks.

For link state routing protocols where information is flooded with areas (OSPF) or levels (ISIS), countermeasures can be directly applied by the routing entities through the processing and comparison of link state information received from different peers. By comparing the link information from multiple sources decisions can be made by a routing node or external entity with regard to routing information validity.

For distance vector protocols where information is aggregated at each routing node it is not possible for nodes to directly detect Byzantine information manipulation attacks from the routing information exchange. In such cases, the routing protocol must include and support indirect communications exchanges between non-adjacent routing peers to provide a secondary channel for performing routing information validation. S-RIP [Wan2004] (Wan, T., Kranakis, E., and PC. van Oorschot, “S-RIP: A Secure Distance Vector Routing Protocol,” Jun. 8-11 2004.) is an example of the implementation of this type of dedicated routing protocol security where the correctness of aggregate distance vector information can only be validated by initiating confirmation exchanges directly between nodes that are not routing neighbors.

Alternatively, an entity external to the routing protocol would be required to collect and audit routing information exchanges to detect the Byzantine attack. In the context of the current security framework, any protection against Byzantine routing information attacks will need to be directly included within the mechanisms of the ROLL routing protocol. This can be implemented where such an attack is considered relevant even within the physical device protections discussed in Section 5.1.4 (Countering Physical Device Compromise)

5.3. Availability Attack Countermeasures

TOC

As alluded to before, availability requires that routing information exchanges and forwarding mechanisms be available when needed so as to guarantee a proper functioning of the network. This may, e.g., include

the correct operation of routing information and neighbor state information exchanges, among others. We will highlight the key features of the security threats along with typical countermeasures to prevent or at least mitigate them. We will also note that an availability attack may be facilitated by an identity attack as well as a replay attack, as was addressed in Section 5.2.3 (Countering Identity (including Sybil) Attacks) and Section 5.2.4 (Countering Routing Information Replay Attacks), respectively.

5.3.1. Countering HELLO Flood Attacks and ACK Spoofing Attacks

TOC

HELLO Flood [Karlof2003] (Karlof, C. and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” September 2003.),[I-D.suhopark-hello-wsn] (Park, S., “Routing Security in Sensor Network: HELLO Flood Attack and Defense,” December 2005.) and ACK Spoofing attacks are different but highly related forms of attacking a LLN. They essentially lead nodes to believe that suitable routes are available even though they are not and hence constitute a serious availability attack.

The origin of facilitating a HELLO flood attack lies in the fact that many routing protocols require nodes to send HELLO packets either upon joining or in regular intervals so as to announce or confirm their existence to the network. Those nodes that receive the HELLO packet assume that they are indeed neighbors.

With this in mind, a malicious node can send or replay HELLO packets using, e.g., a higher transmission power. That creates the false illusion of being a neighbor to an increased number of nodes in the network, thereby effectively increasing its unidirectional neighborhood cardinality. The high quality of the falsely advertised link may coerce nodes to route data via the malicious node. However, those affected nodes, for which the malicious node is in fact unreachable, never succeed in their delivery and the packets are effectively dropped. The symptoms are hence similar to those of a sinkhole, wormhole and selective forwarding attack.

A malicious HELLO flood attack clearly distorts the network topology. It thus affects protocols building and maintaining the network topology as well as routing protocols as such, since the attack is primarily targeted on protocols that require sharing of information for topology maintenance or flow control.

To counter HELLO flood attacks, several mutually non-exclusive methods are feasible:

- *restricting neighborhood cardinality;
- *facilitating multipath routing;
- *verifying bidirectionality.

Restricting the neighborhood cardinality prevents malicious nodes from having an extended set of neighbors beyond some tolerated threshold and thereby preventing topologies to be built where malicious nodes have a false neighborhood set. Furthermore, as shown in [I-D.suhopark-hello-wsn] (Park, S., "Routing Security in Sensor Network: HELLO Flood Attack and Defense," December 2005.), if the routing protocol supports multiple paths from a sensing node towards several LBRs then HELLO flood attacks can also be diminished; however, the energy-efficiency of such approach is clearly sub-optimal. Finally, verifying that the link is truly bidirectional by means of, e.g., an ACK handshake and appropriate security measures ensures that a communication link is only established if not only the affected node is within range of the malicious node but also vice versa. Whilst this does not really eliminate the problem of HELLO flooding, it greatly reduces the number of affected nodes and the probability of such an attack succeeding.

As for the latter, the adversary may spoof the ACK messages to convince the affected node that the link is truly bidirectional and thereupon drop, tunnel or selectively forward messages. Such ACK spoofing attack is possible if the malicious node has a receiver which is significantly more sensitive than that of a normal node, thereby effectively extending its range. Since an ACK spoofing attack facilitates a HELLO flood attack, similar countermeasure are applicable here. Viable counter and security measures for both attacks have been exposed in [I-D.suhopark-hello-wsn] (Park, S., "Routing Security in Sensor Network: HELLO Flood Attack and Defense," December 2005.).

5.3.2. Countering Overload Attacks

TOC

Overload attacks are a form of DoS attack in that a malicious node overloads the network with irrelevant traffic, thereby draining the nodes' energy budget quicker, when the nodes rely on battery or energy scavenging. It thus significantly shortens the lifetime of networks of battery nodes and constitutes another serious availability attack. With energy being one of the most precious assets of LLNs, targeting its availability is a fairly obvious attack. Another way of depleting the energy of a LLN node is to have the malicious node overload the network with irrelevant traffic. This impacts availability since certain routes get congested which

- renders them useless for affected nodes and data can hence not be delivered;
- makes routes longer as shortest path algorithms work with the congested network;

*depletes battery and energy scavenging nodes quicker and thus shortens the network's availability at large.

Overload attacks can be countered by deploying a series of mutually non-exclusive security measures:

*introduce quotas on the traffic rate each node is allowed to send;

*isolate nodes which send traffic above a certain threshold based on system operation characteristics;

*allow only trusted data to be received and forwarded.

As for the first one, a simple approach to minimize the harmful impact of an overload attack is to introduce traffic quotas. This prevents a malicious node from injecting a large amount of traffic into the network, even though it does not prevent said node from injecting irrelevant traffic at all. Another method is to isolate nodes from the network at the network layer once it has been detected that more traffic is injected into the network than allowed by a prior set or dynamically adjusted threshold. Finally, if communication is sufficiently secured, only trusted nodes can receive and forward traffic which also lowers the risk of an overload attack.

5.3.3. Countering Selective Forwarding Attacks

TOC

Selective forwarding attacks are another form of DoS attack which impacts the routing path availability.
An insider malicious node basically blends neatly in with the network but then may decide to forward and/or manipulate certain packets. If all packets are dropped, then this attacker is also often referred to as a "black hole". Such a form of attack is particularly dangerous if coupled with sinkhole attacks since inherently a large amount of traffic is attracted to the malicious node and thereby causing significant damage. In a shared medium, an outside malicious node would selectively jam overheard data flows, where the thus caused collisions incur selective forwarding.
Selective Forwarding attacks can be countered by deploying a series of mutually non-exclusive security measures:

*multipath routing of the same message over disjoint paths;

*dynamically select the next hop from a set of candidates.

The first measure basically guarantees that if a message gets lost on a particular routing path due to a malicious selective forwarding attack,

there will be another route which successfully delivers the data. Such method is inherently suboptimal from an energy consumption point of view. The second method basically involves a constantly changing routing topology in that next-hop routers are chosen from a dynamic set in the hope that the number of malicious nodes in this set is negligible. A routing protocol that allows for disjoint routing paths may also be useful.

5.3.4. Countering Sinkhole Attacks

TOC

In sinkhole attacks, the malicious node manages to attract a lot of traffic mainly by advertising the availability of high-quality links even though there are none. It hence constitutes a serious attack on availability.
The malicious node creates a sinkhole by attracting a large amount of, if not all, traffic from surrounding neighbors by advertising in and outwards links of superior quality. Affected nodes hence eagerly route their traffic via the malicious node which, if coupled with other attacks such as selective forwarding, may lead to serious availability and security breaches. Such an attack can only be executed by an inside malicious node and is generally very difficult to detect. An ongoing attack has a profound impact on the network topology and essentially becomes a problem of flow control.
Sinkhole attacks can be countered by deploying a series of mutually non-exclusive security measures:

- *use geographical insights for flow control;
- *isolate nodes which receive traffic above a certain threshold;
- *dynamically pick up next hop from set of candidates;
- *allow only trusted data to be received and forwarded.

Whilst most of these countermeasures have been discussed before, the use of geographical information deserves further attention. Essentially, if geographic positions of nodes are available, then the network can assure that data is actually routed towards the intended destination and not elsewhere. On the other hand, geographic position is a sensitive information that may have security and/or privacy consequences.

TOC

5.3.5. Countering Wormhole Attacks

In wormhole attacks at least two malicious nodes shortcut or divert the usual routing path by means of a low-latency out-of-band channel. This changes the availability of certain routing paths and hence constitutes a serious security breach.
Essentially, two malicious insider nodes use another, more powerful, transmitter to communicate with each other and thereby distort the would-be-agreed routing path. This distortion could involve shortcutting and hence paralyzing a large part of the network; it could also involve tunneling the information to another region of the network where there are, e.g., more malicious nodes available to aid the intrusion or where messages are replayed, etc. In conjunction with selective forwarding, wormhole attacks can create race conditions which impact topology maintenance, routing protocols as well as any security suits built on "time of check" and "time of use".
Wormhole attacks are very difficult to detect in general but can be mitigated using similar strategies as already outlined above in the context of sinkhole attacks.

---

6. ROLL Security Features

TOC

The assessments and analysis in Section 4 (Threats and Attacks) examined all areas of threats and attacks that could impact routing, and the countermeasures presented in Section 5 (Countermeasures) were reached without confining the consideration to means only available to routing. This section puts the results into perspective and provides a framework for addressing the derived set of security objectives that must be met by the routing protocol(s) specified by the ROLL Working Group. It bears emphasizing that the target here is a generic, universal form of the protocol(s) specified and the normative keywords are mainly to convey the relative level of importance or urgency of the features specified.
The first part of this section, Section 6.1 (Confidentiality Features) to Section 6.3 (Availability Features), is a prescription of ROLL security features of measures that can be addressed as part of the routing protocol itself. As routing is one component of a LLN system, the actual strength of the security services afforded to it should be made to conform to each system's security policy; how a design may address the needs of the urban, industrial, home automation, and building automation application domains also needs to be considered.
The second part of this section, Section 6.4 (Additional Related Features) and Section 6.5 (Consideration on Matching Application Domain Needs), discusses system security aspects that may impact routing but that also require considerations beyond the routing protocol, as well as potential approaches.

6.1. Confidentiality Features

TOC

With regard to confidentiality, protecting the routing/topology information from eavesdropping or unauthorized exposure is not directly essential to maintaining the routing function. Breaches of confidentiality may lead to other attacks or the focusing of an attacker's resources (see Section 4.1 (Threats and Attacks on Confidentiality)) but does not of itself directly undermine the operation of the routing function. However, to protect against, and improve vulnerability against other more direct attacks, routing information confidentiality should be protected. Thus, a secured ROLL protocol

- *SHOULD provide payload encryption;
- *MAY provide tunneling;
- *MAY provide load balancing;
- *SHOULD provide privacy when geographic information is used (see, e.g., [RFC3693] (Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, “Geopriv Requirements,” February 2004.)).

Where confidentiality is incorporated into the routing exchanges, encryption algorithms and key lengths need to be specified in accordance of the level of protection dictated by the routing protocol and the associated application domain transport network. In terms of the life time of the keys, the opportunity to periodically change the encryption key increases the offered level of security for any given implementation. However, where strong cryptography is employed, physical, procedural, and logical data access protection considerations may have more significant impact on cryptoperiod selection than algorithm and key size factors. Nevertheless, in general, shorter cryptoperiods, during which a single key is applied, will enhance security.
Given the mandatory protocol requirement to implement routing node authentication as part of routing integrity (see Section 6.2 (Integrity Features)), key exchanges may be coordinated as part of the integrity verification process. This provides an opportunity to increase the frequency of key exchange and shorten the cryptoperiod as a compliment to the key length and encryption algorithm required for a given application domain. For LLNs, the coordination of confidentiality key management with the implementation of node device authentication can thus reduce the overhead associated with supporting data confidentiality. A new ciphering key may therefore be concurrently

generated or updated in conjunction with the mandatory authentication exchange occurring with each routing peer association.

6.2. Integrity Features

TOC

The integrity of routing information provides the basis for ensuring that the function of the routing protocol is achieved and maintained. To protect integrity, a secured ROLL protocol

- *MUST verify message integrity;
- *MUST verify the authenticity and liveliness of both principals of a connection;
- *MUST verify message sequence.

Depending on the nature of the routing protocol, e.g., distance vector or link state, additional measures may be necessary when the validity of the routing information is of concern. Specifically, verification of routing peer authenticity and liveliness can be used to build a "chain of trust" along the path the routing information flows, such that network-wide information is validated through the concatenation of trust established at each individual routing peer exchange. This is particularly important in the case of distance vector-based routing protocols, where information is updated at intermediate nodes, In such cases, there are no direct means within routing for a receiver to verify the validity of the routing information beyond the current exchange; as such, nodes would need to be able to communicate and request information from non-adjacent peers (see [Wan2004] (Wan, T., Kranakis, E., and PC. van Oorschot, “S-RIP: A Secure Distance Vector Routing Protocol,” Jun. 8-11 2004.)) to provide information integrity assurances. With link state-based protocols, on the other hand, routing information can be signed at the source thus providing a means for validating information that originates beyond a routing peer. Therefore, where necessary, a secured ROLL protocol MAY use security auditing mechanisms that are external to routing to verify the validity of the routing information content exchanged among routing peers.

6.3. Availability Features

TOC

Availability of routing information is linked to system and network availability which in the case of LLNs require a broader security view beyond the requirements of the routing entities (see Section 6.5 (Consideration on Matching Application Domain Needs)). Where

availability of the network is compromised, routing information availability will be accordingly affected. However, to specifically assist in protecting routing availability

*MAY restrict neighborhood cardinality;

*MAY use multiple paths;

*MAY use multiple destinations;

*MAY choose randomly if multiple paths are available;

*MAY set quotas to limit transmit or receive volume;

*MAY use geographic insights for flow control.

6.4. Additional Related Features

TOC

If a LLN employs multicast and/or anycast, it MUST secure these mechanisms with the services listed in this sections. Furthermore, the nodes MUST provide adequate physical tamper resistance to ensure the integrity of stored routing information.
The functioning of the security services requires keys and credentials. Therefore, even though not directly a ROLL security requirement, a LLN must include a process for key and credential distribution; a LLN is encouraged to have procedures for their revocation and replacement.

6.5. Consideration on Matching Application Domain Needs

TOC

As routing is one component of a LLN system, the actual strength of the security services afforded to it should be made to conform to each system's security policy; how a design may address the needs of the urban, industrial, home automation, and building automation application domains is considered as part of the security architecture in Section 6.5.1 (Security Architecture).
The development so far takes into account collectively the impacts of the issues gathered from [RFC5548] (Dohler, M., Watteyne, T., Winter, T., and D. Barthel, “Routing Requirements for Urban Low-Power and Lossy Networks,” May 2009.), [RFC5673] (Pister, K., Thubert, P., Dwars, S., and T. Phinney, “Industrial Routing Requirements in Low-Power and Lossy Networks,” October 2009.), [RFC5826] (Brandt, A., Buron, J., and G. Porcu, “Home Automation Routing Requirements in Low-Power and Lossy Networks,” April 2010.), and [RFC5867] (Martocci, J., De Mil, P., Riou,

N., and W. Vermeylen, “Building Automation Routing Requirements in Low-Power and Lossy Networks,” June 2010.). The following two subsections first consider from an architectural perspective how the security design of a ROLL protocol may be made to adapt to the four application domains, and then examine mechanism and protocol operations issues.

6.5.1. Security Architecture

TOC

The first challenge for a ROLL protocol security design is to have an architecture that can adequately address a set of very diversified needs. It is mainly a consequence of the fact that there are both common and non-overlapping requirements from the four application domains, while, conceivably, each individual application will present yet its own unique constraints.

For a ROLL protocol, the security requirements defined in Section 6.1 (Confidentiality Features) to Section 6.4 (Additional Related Features) can be addressed at two levels: 1) through measures implemented directly within the routing protocol itself and initiated and controlled by the routing protocol entities; or 2) through measures invoked on behalf of the routing protocol entities but implemented within the part of the network over which the protocol exchanges occur. Where security is directly implemented as part of the routing protocol the security requirements configured by the user (system administrator) will operate independent of the lower layers. OSPFv2 [RFC2328] (Moy, J., “OSPF Version 2,” April 1998.) is an example of such an approach in which security parameters are exchanged and assessed within the routing protocol messages. In this case, the mechanism may be, e.g., a header containing security material of configurable security primitives in the fashion of OSPFv2 or RIPv2 [RFC2453] (Malkin, G., “RIP Version 2,” November 1998.). Where IPsec [RFC4301] (Kent, S. and K. Seo, “Security Architecture for the Internet Protocol,” December 2005.) is employed to secure the network, the included protocol-specific (OSPF or RIP) security elements are in addition to and independent of those at the network layer. In the case of LLNs or other networks where system security mandates protective mechanisms at other lower layers of the network, security measures implemented as part of the routing protocol will be redundant to security measures implemented elsewhere as part of the protocol stack.

Security mechanisms built into the routing protocol can ensure that all desired countermeasures can be directly addressed by the protocol all the way to the endpoint of the routing exchange. In particular, routing protocol Byzantine attacks by a compromised node that retains valid network security credentials can only be detected at the level of the information exchanged within the routing protocol. Such attacks aimed the manipulation of the routing information can only be fully addressed through measures operating directly between the routing entities

themselves or external entities able to access and analyze the routing information (see discussion in Section 5.2.5 (Countering Byzantine Routing Information Attacks)).

On the other hand, it is more desirable from a LLN device perspective that the ROLL protocol is integrated into the framework of an overall system architecture where the security facility may be shared by different applications and/or across layers for efficiency, and where security policy and configurations can be consistently specified. See, for example, considerations made in RIPng [RFC2080] (Malkin, G. and R. Minnear, “RIPng for IPv6,” January 1997.) or the approach presented in [Messerges2003] (Messerges, T., Cukier, J., Kevenaar, T., Puhl, L., Struik, R., and E. Callaway, “Low-Power Security for Wireless Sensor Networks,” Oct. 31 2003.).

Where the routing protocol is able to rely on security measures configured with other part of the protocol stack, greater system efficiency can be realized by avoiding potentially redundant security. Relying on an open trust model [Messerges2003] (Messerges, T., Cukier, J., Kevenaar, T., Puhl, L., Struik, R., and E. Callaway, “Low-Power Security for Wireless Sensor Networks,” Oct. 31 2003.), the security requirements of the routing protocol can be more flexibly met at different layers of the transport network; measures that must be applied to protect the communications network are concurrently able to provide the needed routing protocol protection.

In addition, in the context of the different application domains, it allows the level of security applied for routing to be consistent with that needed for protecting the network itself. For example, where a 128-bit AES (AES-128) is deemed the appropriate standard for network confidentiality of data exchanges at the link layer, that level of security is automatically afforded to routing protocol exchanges. Similarly, where the Secure Hash Algorithm, v. 1, (SHA-1) [FIPS180] (, “Federal Information Processing Standards Publication 180-1,” Apr. 17 1995.) is stipulated as the standard required for authenticating routing protocol peers, the use of SHA-1 at the network layer between communicating routing devices automatically meets the routing protocol security requirement within the context of open trust across layers within the device.

A ROLL protocol MUST be made flexible by a design that offers the configuration facility so that the user (network administrator) can choose the security settings that match the application's needs. Furthermore, in the case of LLNs that flexibility should extend to allowing the routing protocol security requirements to be met by measures applied at different protocol layers, provided the identified requirements are collectively met.

Since Byzantine attacks that can affect the validity of the information content exchanged between routing entities can only be directly countered at the routing protocol level, the ROLL protocol may support mechanisms for verifying routing data validity that extends beyond the chain of trust created through device authentication. This protocol-specific security mechanism should be made optional within the protocol

allowing it to be invoked according to the given routing protocol and application domain and as selected by the system user. All other ROLL security mechanisms needed to meet the above identified routing security requirements should be flexibly implemented within the transport network (at the IP network layer or higher or lower protocol layers(s)) according to the particular application domain and user network configuration.

Based on device capabilities and the spectrum of operating environments it would be difficult for a single fixed security design to be applied to address the diversified needs of the urban, industrial, home, and building ROLL application domains, and foreseeable others, without forcing a very low common denominator set of requirements. On the other hand, providing four individual domain designs that attempt to a priori match each individual domain is also very likely to provide a suitable answer given the degree of network variability even within a given domain; furthermore, the type of link layers in use within each domain also influences the overall security. Instead, the framework implementation approach recommended for optional, routing protocol-specific measures together with flexible transport network mechanisms can be the most effective. This approach allows countermeasures against internal attacks to be applied in environments where applicable threats exist. At the same time, it allows routing protocol security to be configured through measures implemented within the transport network that is commensurate and consistent with the level and strength applied in the particular application domain networks.

6.5.2. Mechanisms and Operations

TOC

With an architecture allowing different configurations to meet the application domain needs, the task is then to find suitable mechanisms. For example, one of the main problems of synchronizing security states of sleepy nodes, as listed in the last subsection, lies in difficulties in authentication; these nodes may not have received in time the most recent update of security material. Similarly, the issues of minimal manual configuration, prolonged rollout and delayed addition of nodes, and network topology changes also complicate security management. In such case the ROLL protocol may need to bootstrap the authentication process and allow for flexible expiration scheme of authentication credentials. This exemplifies the need for the coordination and interoperation between the requirements of the ROLL routing protocol and that of the system security elements.

Similarly, the vulnerability brought forth by some special-function nodes, e.g., LBRs requires the assurance, particularly, of the availability of communication channels and node resources, or that the neighbor discovery process operates without undermining routing availability.

There and other factors which are not part of a ROLL routing protocol can still affect its operation. This includes elements such as weaker barrier to accessing the data or security material stored on the nodes through physical means; therefore, the internal and external interfaces of a node need to be adequate for guarding the integrity, and possibly the confidentiality, of stored information, as well as the integrity of routing and route generation processes.
Figure 3 (LLN Device Security Model) provides an overview of the larger context of system security and the relationship between ROLL requirements and measures and those that relate to the LLN system.

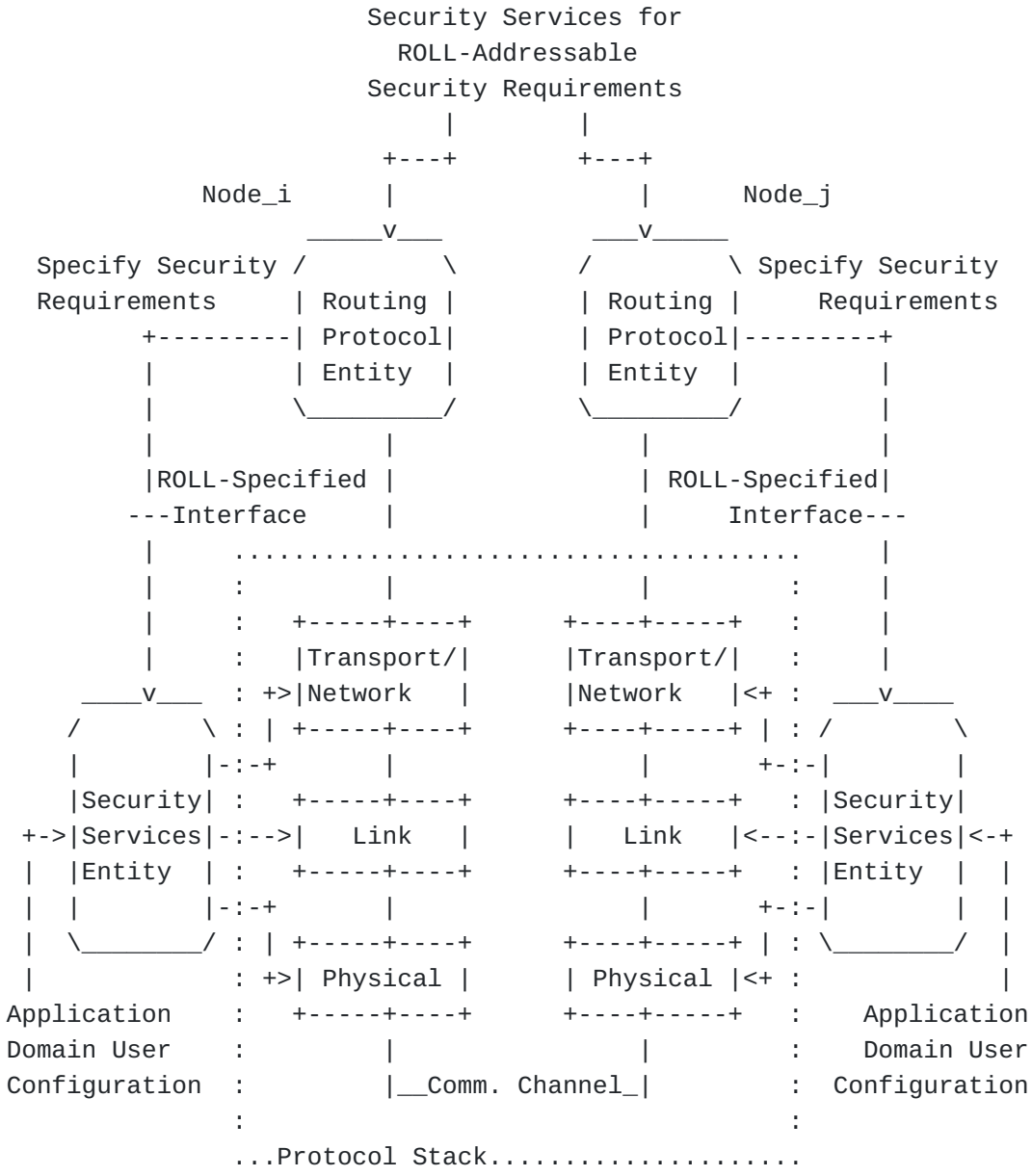

Figure 3: LLN Device Security Model

---

7. Application of ROLL Security Framework to RPL

TOC

This section applies the assessments given in Section 6 (ROLL Security Features) to RPL as an illustration of the application of the LLN security framework.

Specializing the approach used in Section 3.1 (Routing Assets and Points of Access), Figure 4 (Data Flow Diagram of RPL) gives a data flow diagram representation of RPL to show the routing "assets" and "points of access" that may be vulnerable and need to be protected.

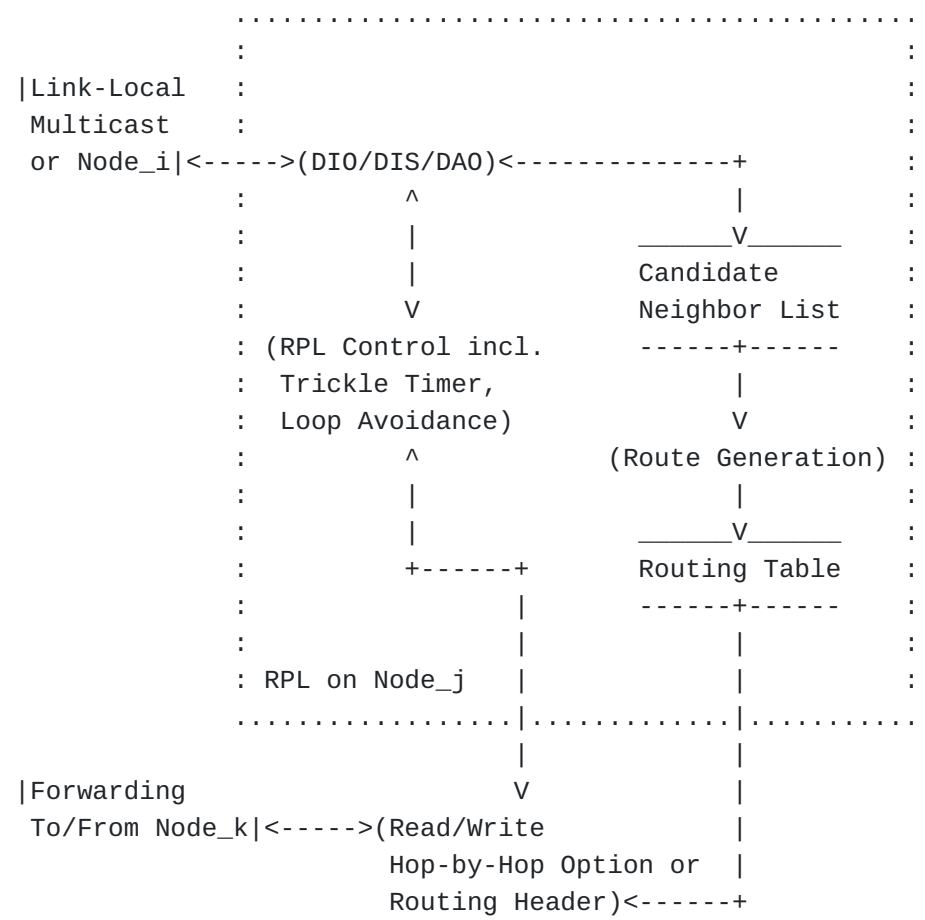

Figure 4: Data Flow Diagram of RPL

From Figure 4 (Data Flow Diagram of RPL), it is seen that threats to the proper operation of RPL are realized through attacks on its DIO, DIS, and DAO messages, as well as on the information the protocol places on the IPv6 Hop-by-Hop Option Header [I-D.ietf-6man-rpl-option] (Hui, J. and J. Vasseur, “RPL Option for Carrying RPL Information in Data-Plane Datagrams,” July 2010.)and Routing Header [I-D.ietf-6man-rpl-routing-header] (Hui, J., Vasseur, J., and D. Culler, “An IPv6 Routing Header for Source Routes with RPL,” July 2010.). As set forth in Section 6.1 (Confidentiality Features) to Section 6.4 (Additional Related Features), the base security

requirements concern message integrity, authenticity and liveliness of the principals of a connection, and protection against message replay; message encryption may be desirable. The security objectives for RPL are therefore to ensure that

1. participants of the DIO, DIS, and DAO message exchanges are authentic;

2. the received DIO, DIS, and DAO messages are not modified during transportation;

3. the received DIO, DIS, and DAO messages are not retransmissions of previous messages;

4. the content of the DIO, DIS, and DAO messages may be made legible to only authorized entities.

In meeting the above objectives, RPL also needs to provide tunable mechanisms both to allow matching the security afforded to the application domain requirements and to enable efficient use of system resources, as discussed in Section 6.5.1 (Security Architecture) and Section 6.5.2 (Mechanisms and Operations).
The functions of the different RPL messages, and the next hops information placed in the Routing Header and RPL option TLV carried in the Hop-by-Hop Option Header are factors that can be taken into account when deciding the optional security features and levels of strength to be afforded. For example, the DIO messages build routes to roots while the DAO messages support the building of downward routes to leaf nodes. Consequently, there may be application environments in which the directions of the routes have different importance and thus warrant the use of different security features and/or strength. In other words, it may be desirable to have an RPL security design that extends the tunability of the security features and strengths to message types. The use of a per-message security specification will allow flexibility in permitting application-domain security choices as well as overall tunability.

---

8. IANA Considerations

TOC

This memo includes no request to IANA.

TOC

9. Security Considerations

The framework presented in this document provides security analysis and design guidelines with a scope limited to ROLL. Security services are identified as requirements for securing ROLL. The results are applied to RPL, with consequent recommendations.

---

10. Acknowledgments

TOC

The authors would like to acknowledge the review and comments from Rene Struik.

---

11. References

TOC

11.1. Normative References

TOC

[FIPS180]	“Federal Information Processing Standards Publication 180-1,” US National Institute of Standards and Technology, Apr. 17 1995.
[FIPS197]	“Federal Information Processing Standards Publication 197,” US National Institute of Standards and Technology, Nov. 26 2006.
[I-D.ietf-6man-rpl-option]	Hui, J. and J. Vasseur, “RPL Option for Carrying RPL Information in Data-Plane Datagrams,” draft-ietf-6man-rpl-option-00 (work in progress), July 2010 (TXT).
[I-D.ietf-6man-rpl-routing-header]	Hui, J., Vasseur, J., and D. Culler, “An IPv6 Routing Header for Source Routes with RPL,” draft-ietf-6man-rpl-routing-header-00 (work in progress), July 2010 (TXT).
[I-D.ietf-roll-rpl]	Winter, T., Thubert, P., and R. Team, “RPL: IPv6 Routing Protocol for Low power and Lossy Networks,” draft-ietf-roll-rpl-11 (work in progress), July 2010 (TXT).
[Kasumi3gpp]	“3GPP TS 35.202 Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification,” 3GPP TSG SA3, 2009.
[RFC2080]	Malkin, G. and R. Minnear, “RIPng for IPv6,” RFC 2080, January 1997 (TXT).
[RFC2119]	

	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2328]	Moy, J., "OSPF Version 2," STD 54, RFC 2328, April 1998 (TXT, HTML, XML).
[RFC2453]	Malkin, G., "RIP Version 2," STD 56, RFC 2453, November 1998 (TXT, HTML, XML).
[RFC3693]	Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements," RFC 3693, February 2004 (TXT).
[RFC4301]	Kent, S. and K. Seo, "Security Architecture for the Internet Protocol," RFC 4301, December 2005 (TXT).

11.2. Informative References

TOC

[Huang2003]	Huang, Q., Cukier, J., Kobayashi, H., Liu, B., and J. Zhang, "Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks," in Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications, San Diego, CA, USA, pp. 141-150, Sept. 19 2003.
[I-D.ietf-roll-terminology]	Vasseur, J., "Terminology in Low power And Lossy Networks," draft-ietf-roll-terminology-04 (work in progress), September 2010 (TXT).
[I-D.suhopark-hello-wsn]	Park, S., "Routing Security in Sensor Network: HELLO Flood Attack and Defense," draft-suhopark-hello-wsn-00 (work in progress), December 2005 (TXT).
[Karlof2003]	Karlof, C. and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Elsevier AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2):293-315, September 2003.
[Messerges2003]	Messerges, T., Cukier, J., Kevenaar, T., Puhl, L., Struik, R., and E. Callaway, "Low-Power Security for Wireless Sensor Networks," in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, Fairfax, VA, USA, pp. 1-11, Oct. 31 2003.
[Myagmar2005]	Myagmar, S., Lee, AJ., and W. Yurcik, "Threat Modeling as a Basis for Security Requirements," in Proceedings of the Symposium on Requirements Engineering for Information Security (SREIS'05), Paris, France, pp. 94-102, Aug 29, 2005.

[RFC4593]	Barbir, A., Murphy, S., and Y. Yang, “Generic Threats to Routing Protocols,” RFC 4593, October 2006 (TXT).
[RFC4949]	Shirey, R., “Internet Security Glossary, Version 2,” RFC 4949, August 2007 (TXT).
[RFC5548]	Dohler, M., Watteyne, T., Winter, T., and D. Barthel, “Routing Requirements for Urban Low-Power and Lossy Networks,” RFC 5548, May 2009 (TXT).
[RFC5673]	Pister, K., Thubert, P., Dwars, S., and T. Phinney, “Industrial Routing Requirements in Low-Power and Lossy Networks,” RFC 5673, October 2009 (TXT).
[RFC5826]	Brandt, A., Buron, J., and G. Porcu, “Home Automation Routing Requirements in Low-Power and Lossy Networks,” RFC 5826, April 2010 (TXT).
[RFC5867]	Martocci, J., De Mil, P., Riou, N., and W. Vermeylen, “Building Automation Routing Requirements in Low-Power and Lossy Networks,” RFC 5867, June 2010 (TXT).
[Wan2004]	Wan, T., Kranakis, E., and PC. van Oorschot, “S-RIP: A Secure Distance Vector Routing Protocol,” in Proceedings of the 2nd International Conference on Applied Cryptography and Network Security, Yellow Mountain, China, pp. 103-119, Jun. 8-11 2004.
[Wander2005]	Wander, A., Gura, N., Eberle, H., Gupta, V., and S. Shantz, “Energy analysis of public-key cryptography for wireless sensor networ,” in the Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications pp. 324-328, March 8-12 2005.
[Yourdon1979]	Yourdon, E. and L. Constantine, “Structured Design,” Yourdon Press, New York, Chapter 10, pp. 187-222, 1979.

Authors' Addresses

TOC

	Tzeta Tsao
	Cooper Power Systems
	20201 Century Blvd. Suite 250
	Germantown, Maryland 20874
	USA
Email:	tzeta.tsao@cooperindustries.com
	Roger K. Alexander
	Cooper Power Systems

	20201 Century Blvd. Suite 250
	Germantown, Maryland 20874
	USA
Email:	roger.alexander@cooperindustries.com
	Mischa Dohler
	CTTC
	Parc Mediterrani de la Tecnologia, Av. Canal Olimpic S/N
	Castelldefels, Barcelona 08860
	Spain
Email:	mischa.dohler@cttc.es
	Vanesa Daza
	Universitat Pompeu Fabra
	P/ Circumval.lacio 8, Oficina 308
	Barcelona 08003
	Spain
Email:	vanesa.daza@upf.edu
	Angel Lozano
	Universitat Pompeu Fabra
	P/ Circumval.lacio 8, Oficina 309
	Barcelona 08003
	Spain
Email:	angel.lozano@upf.edu