Routing Over Low-Power and Lossy Networks
Internet-Draft
Intended status: Informational
Expires: April 23, 2014

T. Tsao
R. Alexander
Cooper Power Systems
M. Dohler
CTTC
V. Daza
A. Lozano
Universitat Pompeu Fabra
M. Richardson
Sandelman Software Works

October 20, 2013

A Security Threat Analysis for Routing over Low-Power and Lossy Networks
draft-ietf-roll-security-threats-05

Abstract

This document presents a security threat analysis 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. Applicable countermeasures are application specific and are addressed in relevant applicability statements. These assessments provide the basis of the security recommendations for incorporation into low-power, lossy network routing protocols.

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 [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/.

Copyright Notice

Table of Contents

1. 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 interfaces (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 threat analysis for securing Routing Over LLNs (ROLL) through an analysis that starts from the routing basics. The process requires two steps. First, the analysis will be used to identify pertinent security issues. The second step is to identify necessary countermeasures to secure the ROLL protocols. As there are multiple ways to solve the problem and the specific tradeoffs are deployment specific, the specific countermeasure to be used is detailed in applicatbility statements.

This document uses [IS07498-2] model, which includes Authentication, Access Control, Data Confidentiality, Data Integrity, and Non-Repudiation but to which Availability is added.

All of this document concerns itself with control plane traffic only.

2. Terminology

This document adopts the terminology defined in [RFC6550], in [RFC4949], and in [I-D.ietf-roll-terminology].

The terms control plane and forwarding plane are used consistently with section 1 of [RFC6192].

3. Considerations on ROLL Security

Routing security, in essence, ensures that the routing protocol operates correctly. It 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). State changes would thereby involve not only authorization of injector's actions, authentication of injectors, and potentially confidentiality of routing data, but also proper order of state changes through timeliness, since seriously delayed state changes, such as commands or updates of routing tables, may negatively impact system operation. A security assesment can therefore begin with a focus on the assets [RFC4949] 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.

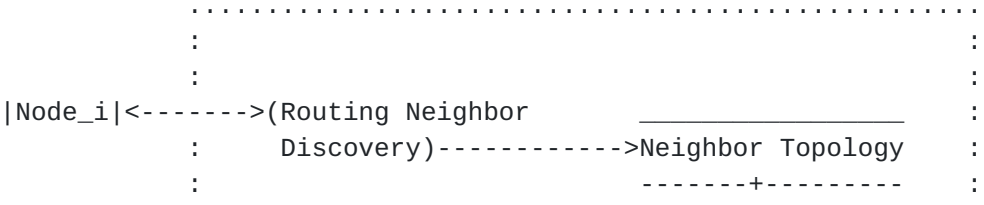
This section sets the stage for the development of the analysis by applying the systematic approach proposed in [Myagmar2005] to the routing security, while also drawing references from other reviews and assessments found in the literature, particularly, [RFC4593] and [Karlof2003]. The subsequent subsections 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 [ISO.7498-2.1988] 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.

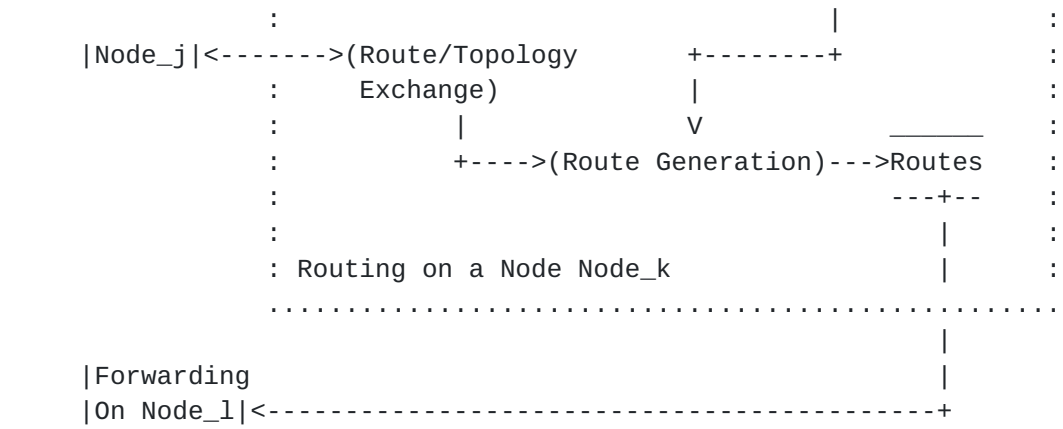
3.1. Routing Assets and Points of Access

An asset is an important system resource (including information, process, or physical resource), the access to, corruption or loss of which adversely affects the system. In the control plane context, an asset is information about the network, processes used to manage and manipulate this data, and the physical devices on which this data is stored and manipulated. The corruption or loss of these assets may adversely impact the control plane of the network. Within the same context, a point of access is an interface or protocol that facilitates interaction between control plane components. Identifying these assets and points of access will provide a basis for enumerating the attack surface of the control plane.

A level-0 data flow diagram [Yourdon1979] is used here to identify the assets and points of access within a generic routing process. The use of a data flow diagram allows for a clear and concise model of the way in which routing nodes interact and process information, and hence provides a context for threats and attacks. The goal of the model is to be as detailed as possible so that corresponding assets, points of access, and process in an individual routing protocol can be readily identified.

Figure 1 shows that nodes participating in the routing process transmit messages to discover neighbors and to exchange routing information; routes are then generated and stored, which may be maintained in the form of the protocol forwarding table. The nodes use the derived routes for making forwarding decisions.





Notation:

(Proc) A process Proc

_____
topology A structure storing neighbor adjacency (parent/child)

_____
routes A structure storing the forwarding information base (FIB)

|Node_n| An external entity Node_n

-------> Data flow

Figure 1: Data Flow Diagram of a Generic Routing Process

It is seen from Figure 1 that

o Assets include

   * routing and/or topology information;

   * route generation process;

   * 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 of the security threat analysis is to be comprehensive. Hence, some of the discussion which follows is associated with assets and points of access that are not directly related to routing protocol design but nonetheless provided for reference since they do have direct consequences on the security of routing.

3.2. The ISO 7498-2 Security Reference Model

At the conceptual level, security within an information system in general and applied to ROLL in particular is concerned with the primary issues of authentication, access control, data confidentiality, data integrity, and non-repudiation. In the context of ROLL

Authentication
: Authentication involves the mutual authentication of the routing peers prior to exchanging route information (i.e., peer authentication) as well as ensuring that the source of the route data is from the peer (i.e., data origin authentication). [RFC5548] points out that LLNs can be drained by unauthenticated peers before configuration. [RFC5673] requires availability of open and untrusted side channels for new joiners, and it requires strong and automated authentication so that networks can automatically accept or reject new joiners.

Access Control
: Access Control provides protection against unauthorized use of the asset, and deals with the authorization of a node.

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 a 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 entails the protection of routing information and routing neighbor maintenance exchanges, as well as derived information maintained in the database, from unauthorized modification, insertions, deletions or replays. to be addressed beyond the routing protocol.

Non-repudiation
: Non-repudiation is the assurance that the transmission and/or reception of a message cannot later be denied. The service of non-repudiation applies after-the-fact and thus relies on the logging or other capture of on-going message exchanges and signatures. Applied to routing, non-repudiation is not an issue because it does not apply to routing protocols, which are machine-to-machine protocols. Further, with the LLN application domains as described in [RFC5867] and [RFC5548], proactive measures are much more critical than retrospective protections. Finally, given the significant practical limits to on-going routing transaction logging and storage and individual device digital signature verification for each exchange, non-repudiation in the context of routing is an unsupportable burden that bears no further considered as a ROLL security issue.

It is recognized that, besides those security issues captured in the ISO 7498-2 model, availability, is a security requirement:

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 should be emphasized here that for ROLL security the above requirements must be complemented by the proper security policies and enforcement mechanisms to ensure that security objectives are met by a given ROLL implementation.

3.3. Issues Specific to or Amplified in LLNs

The work [RFC5548], [RFC5673], [RFC5826], and [RFC5867] 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 study of trade-offs on which and what level of security services are to be afforded during the system design process. The chosen security mechanisms also needs to work within these constraints. Synchronization of security states with sleepy nodes is yet another issue.

Large scale of rolled out network
: The possibly numerous nodes to be deployed make manual on-site configuration unlikely. For example, an urban deployment can see several hundreds of thousands of nodes being installed by many installers with a low level of expertise. Nodes may be installed and not activated for many years, and additional nodes may be added later on, which may be from old inventory. The lifetime of the network is measured in decades, and this complicates the operation 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 complicating the operations of key management.

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 as a higher valued attack target. In fact, when Point-to-MultiPoint (P2MP) and MultiPoint-to-Point (MP2P) traffic represents a majority of the traffic, routing attacks consisting of advertising incorrect preferred routes can cause serious damage.

While it might seem that nodes higher up in the cyclic graph (i.e. those with lower rank) should be secured in a stronger fashion, it is not in general easy to predict which nodes will occupy those positions until after deployment. Issues of redundancy and inventory control suggests that any node might wind up in such a sensitive attack position, so all nodes need to be equally secure.

In addition, even if it were possible to predict which nodes will occupy positions of lower rank and provision them with stronger security mechanisms, in the absense of a strong authorization model, any node could advertise an incorrect preferred route.

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 limited 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.

Additionally nodes may appear to move from one side of a wall to another without any actual motion involved, the result of changes to electromagnetic properties, such as opening and closing of a metal door.

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 an LLN's physical constraints, size, operations, and variety of application areas may impact security. However, it is the combinations of these factors that particularly stress the security concerns. For instance, securing routing for a large number of autonomous devices that are left in unattended locations with limited physical security presents challenges that are not found in the common circumstance of administered networked routers. The following subsection sets up the security objectives for the routing protocol designed by the ROLL WG.

3.4. ROLL Security Objectives

This subsection applies the ISO 7498-2 model to routing assets and access points, taking into account the LLN issues, to develop a set of ROLL security objectives.

Since the fundamental function of a routing protocol is to build routes for forwarding packets, it is essential to ensure that:

- routing/topology information iintegrity remains intact during transfer and in storage;
- routing/topology information is used by authorized entities;
- routing/topology information is available when needed.

In conjunction, it is necessary to be assured that

- authorized peers authenticate themselves during the routing neighbor discovery process;
- the routing/topology information received is 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 unauthorized exposure may be desirable in certain cases but 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. Threat Sources

[RFC4593] provides a detailed review of the threat sources: outsiders and byzantine. ROLL has the same threat sources.

5. Threats and Attacks

This section outlines general categories of threats under the ISO 7498-2 model and highlights the specific attacks in each of these categories for ROLL. As defined in [RFC4949], 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 the attacks that can cause security breaches under the ISO 7498-2 model to the routing

assets and via the routing points of access identified in Section 3.1. The assessment steps through the security concerns of each routing asset and looks at the attacks that can exploit routing points of access. The threats and attacks identified are based on the routing model analysis and associated review of the existing literature. The source of the attacks is assumed to be from either inside or outside attackers. The capability these attackes may be limited to node-equivalent, but also to more sophisticated computing platforms.

5.1. Threats due to failures to Authenticate

5.1.1. Node Impersonation

If an attacker can join a network with any identify, then it may be able to assume the role of a legitimate (and existing node). It may be able to report false readings (in metering applications), or provide inappropriate control messages (in control systems involving actuators) if the security of the application is leveraged from the security of the routing system.

In other systems where there is separate application layer security, the ability to impersonate a node would permit an attacker to direct traffic to itself, which facilitates on-path attacks including replaying, delaying, or duplicating control messages.

5.1.2. Dummy Node

If an attacker can join a network with any identify, then it can pretend to be a legitimate node, receiving any service legitimate nodes receive. It may also be able to report false readings (in metering applications), or provide inappropriate authorizations (in control systems involving actuators), or perform any other attacks that are facilitated by being able to direct traffic towards itself.

5.1.3. Node Resource Spam

If an attacker can join a network with any identify, then it can continously do so, draining down the resources of the network to store identity and routing information, potentionally forcing legitimate nodes of the network.

5.2. Threats and Attacks on Confidentiality

The assessment in Section 3.2 indicates that there are threat actions against the confidentiality of routing information at all points of access. The confidentiality threat consequences is disclosure, see Section 3.1.2 of [RFC4593]. For ROLL this is the disclosure of

routing information either by evesdropping on the communication exchanges between routing nodes or by direct access of node's information.

5.2.1. Routing Exchange Exposure

Routing exchanges include both routing information as well as information associated with the establishment and maintenance of neighbor state information. As indicated in Section 3.1, the associated routing information assets may also include device specific resource information, such as memory, remaining power, etc., that may be metrics of the routing protocol.

The routing exchanges will contain reachability information, which would identify the relative importance of different nodes in the network. Nodes higher up in the DODAG, to which more streams of information flow, would be more interesting targets for other attacks, and routing exchange exposures can identify them.

5.2.2. Routing Information (Routes and Network Topology) Exposure

Routes (which may be maintained in the form of the protocol forwarding table) 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 attachers 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 disclosure 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).

Both of these attack vectors are considered a device specific issue, and are out of scope for the RPL protocol to defend against. In some applications, physical device compromise may be a real threat and it may be necessary to provide for other devices to react quickly to exclude a compromised device.

6. Threats and Attacks on Integrity

The assessment in Section 3.2 indicates that information and identity assets are exposed to integrity threats from all points of access. In other words, the integrity threat space is defined by the potential for exploitation introduced by access to assets available through routing exchanges and the on-device storage.

6.1. Routing Information Manipulation

Manipulation of routing information that range from neighbor states to derived routes 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.

A sub-optimal network may use too much power and/or may congest some routes leading to premature failure of a node, and a denial of service on the entire network.

In addition, 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 (see, for example, [RFC4593] for further discussions on Byzantine attacks);
- Physical device compromise or remote device access attacks.

6.2. Node Identity Misappropriation

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.

7. Threats and Attacks on Availability

The assessment in Section 3.2 indicates that the process and resources assets are exposed to threats against availability; attacks in this category may exploit directly or indirectly information exchange or forwarding (see [RFC4732] for a general discussion).

7.1. Routing Exchange Interference or Disruption

Interference is the threat action and disruption is threat consequence that allows attackers to influence the operation and convergence of the routing protocols by impeding the routing information exchange.

The forms of attack that allow interference or disruption of routing exchange include:

- Routing information replay;
- ACK spoofing;
- Overload attacks. (Section 8.3.2)

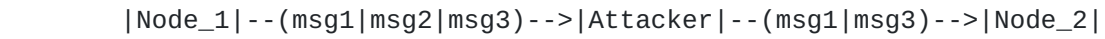
In addition, attacks may also be directly conducted at the physical layer in the form of jamming or interfering.

7.2. Network Traffic Forwarding Disruption

The disruption of the network traffic forwarding capability will undermine the central function of network routers and the ability to handle user traffic. This affects the availability of the network because of the potential to impair the primary capability of the network.

In addition to physical layer obstructions, the forms of attack that allows disruption of network traffic forwarding include [Karlof2003]

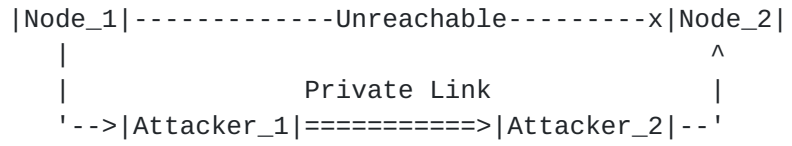
- Selective forwarding attacks;



(a) Selective Forwarding

Figure 2: Selective Forwarding

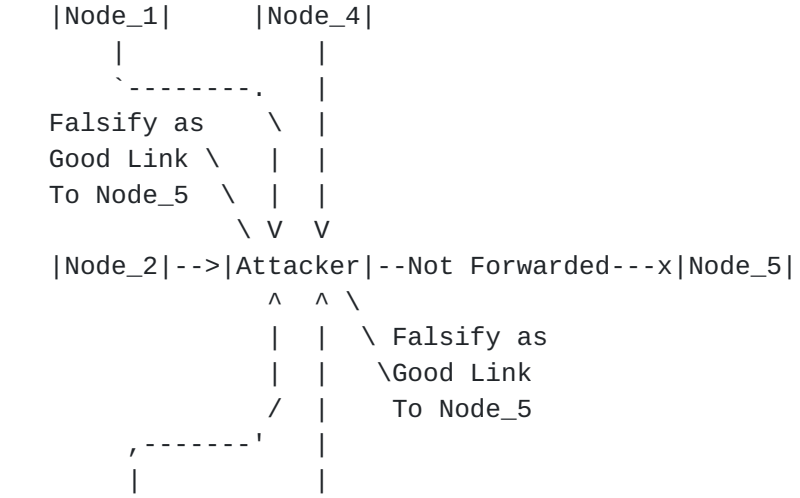
- Wormhole attacks;



(b) Wormhole

Figure 3: Wormhole Attacks

- Sinkhole attacks.



|Node_3| |Node_i|

(c) Sinkhole

Figure 4: Selective Forwarding, Wormhole, and Sinkhole Attacks

These attacks are generally done to both control plane and forwarding plane traffic. A system that prevents control plane traffic (RPL messages) from being diverted in these ways will also prevent actual data from being diverted.

7.3. Communications Resource Disruption

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.

7.4. Node Resource Exhaustion

A potential threat consequence can arise from attempts to overload the node resource asset by initiating exchanges that can lead to the 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 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 consequences 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;
- Overload attacks. (Section 8.3.2)

8. Countermeasures

By recognizing the characteristics of LLNs that may impact routing, this analysis 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 ISO 7498-2 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.

8.1. Confidentiality Attack Countermeasures

Attacks to disclosure routing information 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 wiretapping or traffic analysis, or may attempt access through a component or device interface of a tampered routing node.

8.1.1. Countering Deliberate Exposure Attacks

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.

A prerequisite to countering this attack 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 mitigate the risk of deliberate exposure, the process that communicating nodes use to establish session keys must be peer-to-peer (i.e., between the routing initiating and responding nodes).

This helps ensure that neither node is exchaning routing information with another peer without the knowledge of both communicating peerscan. For a deliberate exposure attack to succeed, the comprised node will need to more overt and take independent actions in order to disclose the routing information to 3rd party.

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.

8.1.2. Countering Passive Wiretapping Attacks

A passive wiretap attack seeks to breach routing confidentiality through passive, direct analysis and processing of the information exchanges between nodes.

Passive wiretap 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 keys and an agreed encryption algorithm. The strength of the encryption algorithm and session key sizes 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 9.5. Because of the resource constraints of LLN devices, symmetric (private) key encryption will provide the best trade-off 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]).

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], adopted by the U.S. government, or Kasumi-Misty [Kasumi3gpp], 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 trade-off that also achieves a balance with the level of confidentiality afforded by the physical device in protecting the routing assets.

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.

8.1.3. Countering Traffic Analysis

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 an LLN, especially one founded on shared medium, is passive and relies on the ability to read the immutable source/destination layer-3 routing information that must remain unencrypted to permit network routing.

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. ROLL does not generally support multi-path routing within a single DODAG. Multiple DODAGs are supported in the protocol, but few deployments will have space for more than half a dozen, and there are at present no clear ways to multiplex traffic for a single application across multiple DODAGs.

Another approach to countering passive traffic analysis could be for nodes to maintain constant amount of traffic to different destinations through the generation of arbitrary traffic flows; the drawback of course would be the consequent overhead.

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. Deployments which use layer-2 security that includes encryption already do this for all traffic.

8.1.4. Countering Remote Device Access Attacks

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 local or remote device 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.

8.2. 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 unauthorized modifications 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.

8.2.1. Countering Unauthorized Modification Attacks

Unauthorized modifications 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.

Unauthorized modifications 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 unauthorized modifications needs to:

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

8.2.2. Countering Overclaiming and Misclaiming Attacks

Both overclaiming and misclaiming aim to introduce false routes or topology that would not be generated by the network otherwise, while there are not necessarily unauthorized modifications to the routing messages or information. 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.

8.2.3. Countering Identity (including Sybil) Attacks

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 explicitly or implicitly an asset to an application running on the LLN, for example, the LBR in a P2MP or MP2P LLN.

8.2.4. Countering Routing Information Replay Attacks

In many routing protocols, message replay can result in false topology and/or routes. This is often counted with some kind of counter to ensure the freshness of the message. Replay of a current, literal RPL message are in general idempotent to the topology. An older (lower DODAGVersionNumber) message, if replayed would be rejected as being stale. The trickle algorithm further dampens the affect of any such replay, as if the message was current, then it would contain the same information as before, and it would cause no network changes.

Replays may well occur in some radio technologies (not very likely, 802.15.4) as a result of echos or reflections, and so some replays must be assumed to occur naturally.

Note that for there to be no affect at all, the replay must be done with the same apparent power for all nodes receiving the replay. A change in apparent power might change the metrics through changes to the ETX and therefore might affect the routing even though the

contents of the packet were never changed. Any replay which appears to be different should be analyzed as a Selective Forwarding Attack, Sinkhole Attack or Wormhole Attack.

8.2.5. 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 entities can therefore only provide a limited counter against internal (Byzantine) node attacks.

For link state routing protocols where information is flooded with, for example, areas (OSPF [RFC2328]) or levels (ISIS [RFC1142]), 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; see Chapter 2 of [Perlman1988] for a discussion on flooding attacks.

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] 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 analysis, any protection against Byzantine routing information attacks will need to be directly included within the mechanisms of the ROLL routing protocol.

8.3. Availability Attack Countermeasures

As alluded to before, availability requires that routing information exchanges and forwarding mechanisms be available when needed so as to guarantee 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 8.2.3 and Section 8.2.4, respectively.

8.3.1. Countering HELLO Flood Attacks and ACK Spoofing Attacks

HELLO Flood [Karlof2003],[I-D.suhopark-hello-wsn] and ACK Spoofing attacks are different but highly related forms of attacking an LLN. They essentially lead nodes to believe that suitable routes are available even though they are not and hence constitute a serious availability attack.

A HELLO attack mounted against RPL would involve sending out (or replaying) DIO messages by the attacker. Lower power LLN nodes might then attempt to join the DODAG at a lower rank than they would otherwise.

The most effective method from [I-D.suhopark-hello-wsn] is the verify bidirectionality. A number of layer-2 links are arranged in controller/spoke arrangements, and continuously are validating connectivity at layer 2.

In addition, in order to calculate metrics, the ETX must be computed, and this involves, in general, sending a number of messages between nodes which are believed to be adjacent. [I-D.kelsey-intarea-mesh-link-establishment] is one such protocol.

In order to join the DODAG, a DAO message is sent upwards. In RPL the DAO is acknowledged by the DAO-ACK message. This clearly checks bidirectionality at the control plane.

As discussed in section 5.1, [I-D.suhopark-hello-wsn] a receiver with a sensitive receiver could well hear the DAOs, and even send DAO-ACKs as well. Such a node is a form of WormHole attack.

These attacks are also all easily defended against using either layer-2 or layer-3 authentication. Such an attack could only be made against a completely open network (such as might be used for provisioning new nodes), or by a compromised node.

8.3.2. Countering Overload Attacks

Overload attacks are a form of DoS attack in that a malicious node overloads the network with irrelevant traffic, thereby draining the nodes' energy store more quickly, when the nodes rely on batteries or energy scavenging. It thus significantly shortens the lifetime of networks of energy-constrained 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 an 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 more quickly 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.

Receiving nodes that validate signatures and sending nodes that encrypt messages need to be cautious of cryptographic processing usage when validating signatures and encrypting messages. Where

feasible, certificates should be validated prior to use of the associated keys to counter potential resource overloading attacks. The associated design decision needs to also consider that the validation process requires resources and thus itself could be exploited for attacks. Alternatively, resource management limits can be placed on routing security processing events (see the comment in Section 6, paragraph 4, of [RFC5751]).

8.3.3. Countering Selective Forwarding Attacks

Selective forwarding attacks are a form of DoS attack which impacts the availability of the generated routing paths.

A selective forwarding attack may be done by a node involved with the routing process, or it may be done by what otherwise appears to be a passive antenna or other RF feature or device, but is in fact an active (and selective) device. An RF antenna/repeater which is not selective, is not a threat.

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 selecting 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 a method is inherently suboptimal from an energy consumption point of view; it is also suboptimal from a network utilization perspective. 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.

8.3.4. Countering Sinkhole Attacks

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 [Karlof2003]. 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.

Some LLNs may provide for geolocation services, often derived from solving triangulation equations from radio delay calculations, such calculations could in theory be subverted by a sinkhole that transmitted at precisely the right power in a node to node fashion.

While geographic knowledge could help assure that traffic always went in the physical direction desired, it would not assure that the traffic was taking the most efficient route, as the lowest cost real route might be match the physical topology; such as when different parts of an LLN are connected by high-speed wired networks.

8.3.5. Countering Wormhole Attacks

In wormhole attacks at least two malicious nodes claim to have a short path between themselves [Karlof2003]. 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".

A pure Wormhole attack is nearly impossible to detect. A wormhole which is used in order to subsequently mount another kind of attack would be defeated by defeating the other attack. A perfect wormhole, in which there is nothing adverse that occurs to the traffic, would be difficult to call an attack. The worst thing that a benign wormhole can do in such a situation is to cease to operate (become unstable), causing the network to have to recalculate routes.

A highly unstable wormhole is no different than a radio opaque (i.e. metal) door that opens and closes a lot. RPL includes hystersis in its objective functions [RFC6719] in an attempt to deal with frequent changes to the ETX between nodes.

9. ROLL Security Features

The assessments and analysis in Section 5 examined all areas of threats and attacks that could impact routing, and the countermeasures presented in Section 8 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.

In this view, 'MUST' is used to define the requirements that are specific to the routing protocol and that are essential for an LLN routing protocol to ensure that routing operation can be maintained. Adherence to MUST requirements is needed to directly counter attacks that can affect the routing operation (such as those that can impact maintained or derived routing/forwarding tables). 'SHOULD' is used to define requirements that counter indirect routing attacks where such attacks do not of themselves affect routing but can assist an attacker in focusing its attack resources to impact network operation (such as DoS targeting of key forwarding nodes). 'MAY' covers

optional requirements that can further enhance security by increasing the space over which an attacker must operate or the resources that must be applied. While in support of routing security, where appropriate, these requirements may also be addressed beyond the network routing protocol at other system communications layers.

The first part of this section, Section 9.1 to Section 9.3, 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 an 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 9.4 and Section 9.5, discusses system security aspects that may impact routing but that also require considerations beyond the routing protocol, as well as potential approaches.

If an LLN employs multicast and/or anycast, these alternative communications modes MUST be secured with the same routing security services specified in this section. Furthermore, irrespective of the modes of communication, nodes MUST provide adequate physical tamper resistance commensurate with the particular application domain environment to ensure the confidentiality, integrity, and availability of stored routing information.

9.1. Confidentiality Features

With regard to confidentiality, protecting the routing/topology information from unauthorized disclosure 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 5.2) but does not of itself directly undermine the operation of the routing function. However, to protect against, and reduce consequences from other more direct attacks, routing information should be protected. Thus, a secured ROLL protocol:

- MUST implement payload encryption;
- MAY provide tunneling;
- MAY provide load balancing.

Where confidentiality is incorporated into the routing exchanges, encryption algorithms and key lengths need to be specified in accordance with 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 9.2), 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 complement 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. If a new ciphering key is concurrently generated or updated in conjunction with the mandatory authentication exchange occurring with each routing peer association, signaling exchange overhead can be reduced.

9.2. Integrity Features

The integrity of routing information provides the basis for ensuring that the function of the routing protocol is achieved and maintained. To protect integrity, RPL must either run using only the Secure versions of the messages, or must run over a layer-2 that uses channel binding between node identity and transmissions. (i.e.: a layer-2 which has an identical network-wide transmission key can not defend against many attacks)

XXX. Logging is critical, but presently impossible.

9.3. Availability Features

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 9.5). 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 information for flow control.

9.4. Key Management

The functioning of the routing security services requires keys and credentials. Therefore, even though not directly a ROLL security requirement, an LLN MUST have a process for initial key and credential configuration, as well as secure storage within the associated devices. Anti-tampering SHOULD be a consideration in physical design. Beyond initial credential configuration, an LLN is also encouraged to have automatic procedures for the revocation and replacement of the maintained security credentials.

While RPL has secure modes, but some modes are impractical without use of public key cryptography believed to be too expensive by many. RPL layer-3 security will often depend upon existing LLN layer-2 security mechanisms, which provides for node authentication, but little in the way of node authorization.

9.5. Consideration on Matching Application Domain Needs

Providing security within an LLN requires considerations that extend beyond routing security to the broader LLN application domain security implementation. In other words, as routing is one component of an LLN system, the actual strength of the implemented security algorithms for the routing protocol MUST be made to conform to the system's target level of security. The development so far takes into account collectively the impacts of the issues gathered from [RFC5548], [RFC5673], [RFC5826], and [RFC5867]. 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 mechanisms and protocol operations issues.

9.5.1. Security Architecture

The first challenge for a ROLL protocol security design is to have an architecture that can adequately address a set of very diverse 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 9.1 to Section 9.4 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 independently of the lower layers. OSPFv2 [RFC2328] 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]. Where IPsec [RFC4301] 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 at 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 8.2.5).

On the other hand, it is more desirable from an 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] or the approach presented in [Messerges2003].

Where the routing protocol is able to rely on security measures configured within other layers of the protocol stack, greater system efficiency can be realized by avoiding potentially redundant security. Relying on an open trust model [Messerges2003], 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.

For example, where a given security encryption scheme is deemed the appropriate standard for network confidentiality of data exchanges at the link layer, that level of security is directly provided to routing protocol exchanges across the local link. Similarly, where a given authentication procedure is stipulated as part of the standard required for authenticating network traffic, that security provision can then meet the requirement needed for authentication of routing exchanges. In addition, in the context of the different LLN application domains, the level of security specified for routing can and should be consistent with that considered appropriate for protecting the network within the given environment.

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 attackers 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 extend 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 can 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 unlikely 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 is for optional, routing protocol-specific measures that can be applied separately from, or together with, flexible transport network mechanisms. Protocol-specific measures include the specification of valid parameter ranges, increments and/or event frequencies that can be verified by individual routing devices. In addition to deliberate attacks this allows basic protocol sanity checks against unintentional mis-configuration. Transport network mechanisms would include out-of-band communications that may be defined to allow an external entity to request and process individual device information as a means to effecting an external verification of the derived network routing information to identify the existence of intentional or unintentional network anomalies.

This approach allows countermeasures against byzantine attackers to be applied in environments where applicable threats exist. At the same time, it allows routing protocol security to be supported through measures implemented within the transport network that are consistent with available system resources and commensurate and consistent with the security level and strength applied in the particular application domain networks.

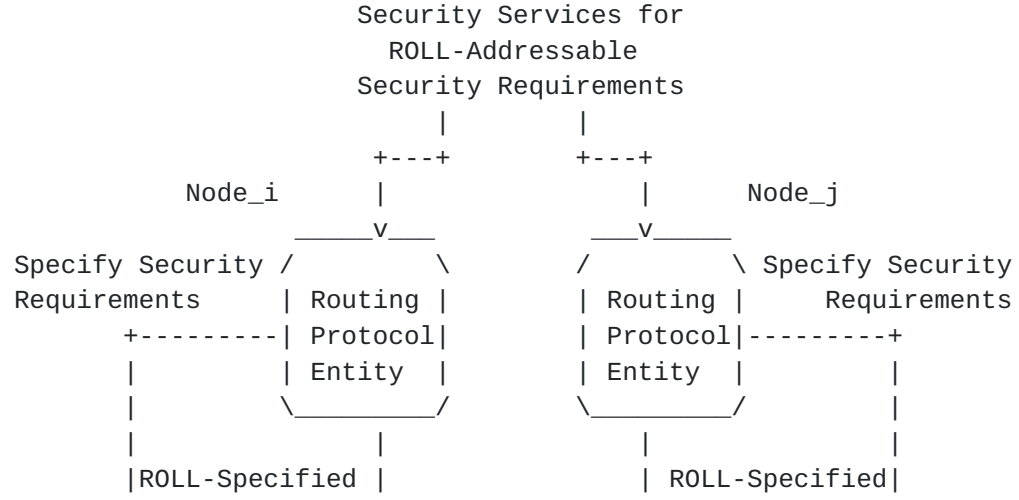
9.5.2. Mechanisms and Operations

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 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 many cases the ROLL protocol may need to bootstrap the authentication process and allow for a 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 are other factors which are not part of a ROLL routing protocol but which can still affect its operation. These include 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 5 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.



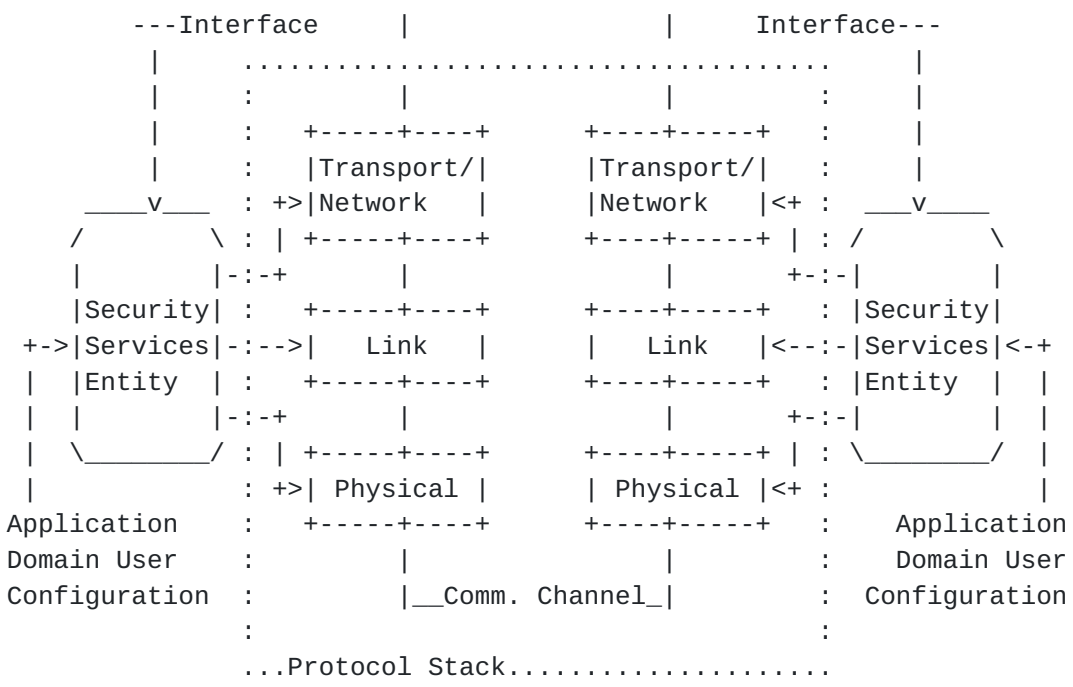


Figure 5: LLN Device Security Model

10. IANA Considerations

This memo includes no request to IANA.

11. Security Considerations

The analysis 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 specific mechanisms to be used to deal with each threat is specified in link-layer and deployment specific applicability statements.

12. Acknowledgments

The authors would like to acknowledge the review and comments from Rene Struik and JP Vasseur. The authors would also like to acknowledge the guidance and input provided by the ROLL Chairs, David Culler, and JP Vasseur, and the Area Director Adrian Farrel.

This document started out as a combined threat and solutions document. As a result of security review, the document was split up by ROLL co-Chair Michael Richardson and security Area Director Sean Turner as it went through the IETF publication process. The solutions to the threads are application and layer-2 specific, and have therefore been moved to the relevant applicability statements.

Ines Robles kept track of the many issues that were raised during the development of this document

13. References

13.1. Normative References

[I-D.ietf-roll-terminology]
Vasseur, J., "Terminology in Low power And Lossy Networks", draft-ietf-roll-terminology-04 (work in progress), September 2010.

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

[RFC4107] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", BCP 107, RFC 4107, June 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.

[RFC6719] Gnawali, O. and P. Levis, "The Minimum Rank with Hysteresis Objective Function", RFC 6719, September 2012.

13.2. Informative References

[FIPS197] , "Federal Information Processing Standards Publication 197: Advanced Encryption Standard (AES)", US National Institute of Standards and Technology, Nov. 26 2001.

[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.alexander-roll-mikey-lln-key-mgmt]
Alexander, R. and T. Tsao, "Adapted Multimedia Internet KEYing (AMIKEY): An extension of Multimedia Internet KEYing (MIKEY) Methods for Generic LLN Environments", draft-alexander-roll-mikey-lln-key-mgmt-04 (work in progress), September 2012.

[I-D.kelsey-intarea-mesh-link-establishment]
Kelsey, R., "Mesh Link Establishment", draft-kelsey-intarea-mesh-link-establishment-05 (work in progress), February 2013.

[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.

[IEEE1149.1]
, "IEEE Standard Test Access Port and Boundary Scan Architecture", IEEE-SA Standards Board, Jun. 14 2001.

[ISO.7498-2.1988]
International Organization for Standardization, "Information Processing Systems - Open Systems Interconnection Reference Model - Security Architecture", ISO Standard 7498-2, 1988.

[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.

[Kasumi3gpp]
, "3GPP TS 35.202 Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification", 3GPP TSG SA3, 2009.

[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.

[Perlman1988] Perlman, N., "Network Layer Protocols with Byzantine Robustness", MIT LCS Tech Report, 429, 1988.

[RFC1142] Oran, D., "OSI IS-IS Intra-domain Routing Protocol", RFC 1142, February 1990.

[RFC2080] Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC2453] Malkin, G., "RIP Version 2", STD 56, RFC 2453, November 1998.

[RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

[RFC4046] Baugher, M., Canetti, R., Dondeti, L., and F. Lindholm, "Multicast Security (MSEC) Group Key Management Architecture", RFC 4046, April 2005.

[RFC4593] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", RFC 4593, October 2006.

[RFC4732] Handley, M., Rescorla, E., IAB, "Internet Denial-of-Service Considerations", RFC 4732, December 2006.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC5055] Freeman, T., Housley, R., Malpani, A., Cooper, D., and W. Polk, "Server-Based Certificate Validation Protocol (SCVP)", RFC 5055, December 2007.

[RFC5197] Fries, S. and D. Ignjatic, "On the Applicability of Various Multimedia Internet KEYing (MIKEY) Modes and Extensions", RFC 5197, June 2008.

[RFC5548] Dohler, M., Watteyne, T., Winter, T., and D. Barthel, "Routing Requirements for Urban Low-Power and Lossy Networks", RFC 5548, May 2009.

[RFC5673] Pister, K., Thubert, P., Dwars, S., and T. Phinney, "Industrial Routing Requirements in Low-Power and Lossy Networks", RFC 5673, October 2009.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

[RFC5826] Brandt, A., Buron, J., and G. Porcu, "Home Automation Routing Requirements in Low-Power and Lossy Networks", RFC 5826, April 2010.

[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.

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

[RFC6192] Dugal, D., Pignataro, C., and R. Dunn, "Protecting the Router Control Plane", RFC 6192, March 2011.

[Szcze2008] Szczechowiak1, P., Oliveira, L., Scott, M., Collier, M., and R. Dahab, "NanoECC: testing the limits of elliptic curve cryptography in sensor networks", pp. 324-328, 2008, <http://www.ic.unicamp.br/~leob/publications/ewsn/NanoECC.pdf>.

[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

Tzeta Tsao
Cooper Power Systems
910 Clopper Rd. Suite 201S
Gaithersburg, Maryland 20878
USA

Email: tzeta.tsao@cooperindustries.com

Roger K. Alexander
Cooper Power Systems
910 Clopper Rd. Suite 201S
Gaithersburg, Maryland 20878
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

Michael Richardson (ed)
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z5V7
Canada

Email: mcr+ietf@sandelman.ca