Network Working Group
Internet Draft
Intended status: Standards Track
Expires: May 2014

Lan Zhang
Gang Feng
Shuang Qin
UESTC

November 27, 2013

Intrusion Detection System for Low-Power and Lossy Networks
draft-zhang-roll-rpl-intrusion-defence-00.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies intrusion detection systems (IDSs) as the second line of defence, to secure the Routing Protocol for Low-power and Lossy Networks (RPL).

Table of Contents

1. Introduction

With the advance of networked electronic devices and wireless communications, network can connect human-to-human, human-to-thing and even thing-to-thing. The network environment often consists of large quantities of devices, which usually have constrained resources such as limited processing capability, short battery life [Le2012]. As a consequence, the network links may have poor quality in transmitting packets. IETF ROLL working group was formed to specify routing protocol for such Low-Power and Lossy Networks (LLNs), and the working group defined a Routing Protocol for LLNs (RPL) [RFC6550]. Due to the salient features of LLNs devices and the inherent vulnerabilities of RPL, the security design to defence RPL intrusions is a significant challenge, especially for mission-critical applications such as military tasks and disaster recovery.

As a broad conception, intrusion generally refers to the unauthorized or unapproved actions that attempt to compromise the system. Intruders can usually be classified into external and internal intruders. External intruders have no right to access the network, which are outsiders with limited intrusion impact. Once they obtain the authorization to become internal intruders, they have more severe damage and as legitimate nodes they are hard to be detected. Usually, internal intruders pass the network access control mechanism by compromising a legitimate node or by deploying malicious nodes.

Security design to defence network intrusions involves three main components, including prevention, detection and mitigation [Farooqi2012]. Traditional cryptography technique is the typical intrusion prevention technique, as the first line of defence to prevent intrusions before their occurrence. However, the intruders may break the preventive security techniques. For example, external intruders compromise the encryption key to become internal. In this case, the intrusion detection technique as the second line of defence can be activated. Intrusion detection system (IDS) is designed to remedy the consequence of intrusions before the system resources are disclosed. IDSs also provide suspicious intrusion information, which might be useful in intrusion mitigation, the third line of defence. IDSs can be used to detect both internal and external intruders. Since RPL devices have weak security nature for tamper resistance, intrusions cannot be completedly solved by prevention techniques. Thus IDSs are of great significance for RPL security.

This document specifies IDSs for RPL, which is weak in defensing intrusions. This document is dedicated to analyzing the detection methodologies, system architectures, detection data and intrusion

response of IDSs with some available promotions in different scenarios.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

This document adopts the terminology defined in [RFC6550], and additionally uses terminology from [ROLL-TERMS], with the following introducing terminologies:

Node: An element of a low-power, lossy network that may be a router or a host.

Sink node: The root node of a Destination Oriented Directed Acyclic Graphs (DODAG). Usually, sink node is the LoWPAN Border Router (LBR), which connects to the internet.

Monitor node (MN): A special node type, which is in charge of monitoring job in IDSs. MNs can be LLNs devices or high-performance devices based on the design of IDSs.

3. Protocol Overview

RPL is a distance vector IPv6 routing protocol designed for LLNs [RFC6550]. Due to the special characteristics of LLNs, such as resource-constrained devices, poor link quality and unattended deployed environment, RPL mainly focuses on self-organizing capability, such as auto-optimized topology construction, self-repair and self-maintenance, etc.

RPL is composed of one or more DODAG. Each DODAG can be regarded as many nodes connected to an LBR, so as to minimize the cost from any node in the network to reach the LBR. LBRs are connected together and linked to the Internet through a backbone or transit link. The DODAG construction is based on Object Function (OF), which can minimize the particular metrics in different application scenarios. To construct the DODAG, RPL defines a set of new ICMPv6 messages, including DODAG Information Solicitation (DIS), DODAG Information Object (DIO), and Destination Advertisement Object (DAO) [RFC4443]. The sink node first broadcasts DIO messages with information related to the DODAG, such

as Rank (which is generally the distance to the backbone network), OF, DODAG-ID, etc. The parent nodes have lower Rank. After receiving DIO message, neighbors calculate their Rank and decide whether to join this DODAG. If a node joins this DODAG, it will send back a DAO message and broadcast DIO message with its rank, OF, the DODAG it belongs to, etc. Nodes can also ask for graph information by sending DIS messages. All nodes repeat this process until each node joins a DODAG, which means the auto-optimized topology construction is completed.

RPL has local repair mechanism to achieve self-healing. Any inconsistency between the routing decision for a packet and the rank relationship between the two nodes indicates a possible loop. On receiving such a packet, a node can institutes a local repair operation, [RFC6550] which can be operated by poisoning mechanism or the change of DODAG ID.

RPL also has timer trickle mechanism, which enables the self-healing and self-maintenance in a highly robust, energy efficient, simple and scalable manner. Each node has a timer to trigger its DIO messages, which increases exponentially. RPL sets the smallest and the biggest possible interval separately. Once network topology fluctuation exists, such as the parent node is unreachable, the timer is reset to the minimized interval value [RFC6206].

The self-organizing capability of RPL makes it more vulnerable to internal intrusions. Many strict rules, which help to maintain optimal RPL network state, may be utilized by the intruders. Neighbors are unaware of the inside process changes of the compromised nodes and continue to communicate as normal. Thus the RPL self-optimized state can be broken.

4. Detection methodologies

Functionally, IDSs have three detection methodologies, which are signature-based, anomaly-based and specification-based. This section details the detection methodologies, analyzes their advantages and disadvantages, and then gives some promotions.

- Signature-based detection: In this methodology, previously known intrusions are profiled as a reference, and the data is matched with the known intrusion signatures with a low false alarm rate. The disadvantage of this detection type is that it cannot be applicable to detect novel intrusions without well-defined [Tseng2003].

- Anomaly-based detection: This detection methodology is based on statistical behavior, which focuses on normal network behaviors rather than intrusion behaviors with a defined threshold to distinguish the compromised nodes. It can detect new intrusions without well-defined. However, the profiled normal behaviors must be updated, which may increase the load of nodes. Moreover the dynamic system may emerge legitimate but previously unseen behavior, which can produces a high degree of false alarms. According to the behavioral model processing nature, G Teodoro et al. [Garcia2009] further divide anomaly-based IDS into three categories, namely statistical based, knowledge based and machine learning based, which may be included in the future documents.

- Specification-based detection: This methodology also detects attacks by comparing network behavior deviations. It can detect new intrusions. Rather than previous network behaviors in anomaly-based detection, it needs to manually extract and craft to characterize legitimate system behavior, so as to avoid high degree of false alarms. But the development of specifications might be time-consuming. Specification-based IDS has been applied to privileged programs, applications, and several network protocols [Tseng2003].

Comparing the above three detection methodologies, the third one has advantages in LLNs. This document promotes specification-based detection methodology to deal with RPL intrusions. But in case of constrined time, the other two methodologies can also be applied. Thus the applied detection methodology can be adjusted based on the application scenarios.

5. System architectures of IDSs

System architecture [Farooqi2012] is crucial to optimize each module of IDSs, and it also directly affects the performance of IDSs. Thus this document pays more attention to the analysis of IDS system architecture. This section specifies three types of system architecture for RPL in different application scenarios.

5.1. Stand-alone IDS

The basic idea of stand-alone IDS is that each MN independently completes intrusion detection based on information collected by its own. In stand-alone IDS, MNs can be classified into centralized and distributed. The following part in this section will discuss the two types of stand-alone IDS.

5.1.1. Centralized MN

In stand-alone IDS with centralized MN, each RPL node is viewed as an MN. The network nodes perform RPL as well as monitoring. Watchdog machine [Shakshuki2011] is a typical centralized MN machine.

This kind of architecture scheme obviously aggravates the load of RPL nodes, which seriously affects the lifetime of RPL node. Due to the resource-constrained RPL characteristics, this kind of system architecture should be applied with caution.

5.1.2. Distributed MN

Distributed MNs are designed for intrusion detection for a certain monitor area. This kind of IDS architecture deploys multiple MNs to cover the network. The proper backbone of MNs should be accomplished with minimal MNs, and each RPL node should be in the range of at least one MN.
Distributed MN with FSM is first proposed by University of California, which is promoted for stand-alone IDS with distributed MN in this document. An FSM is implemented in each MN, which is designed based on the intrusion detection. MNs passively listen to RPL packets and extract information to store in their monitor lists. Each MN has a monitor list, which is updated dynamically. MNs apply the FSM to monitor the behavior flow of nodes in its monitoring area by analyzing data recorded on their monitor list.

Considering the resource-constrained RPL characteristics, the additional monitoring job may incurr big processing cost. Distributed MN device can be designed to high-performance device or LLNs device, and the MNs using LLNs devices can also be RPL node or another special kind of node. Thus there exist three types of distributed MN as follows.

1. As LLNs devices, this type of MN also works as normal RPL nodes. They perform RPL as well as monitor tasks. As battery powered LLNs devices, it is hard to replenish once the energy runs out. This can leads to the network malfunctioning earlier. But this scheme can decrease the network cost to a great extent. Moreover unlike traditional security mechanism, MN does not require any harsh encryption algorithm or operation. This scheme is promoted to be applied to applications with simple security problems, such as simple civil scenarios.
2. As LLNs devices, this type of MN does not perform any RPL operation. As another special kind of node, it only monitors the network security, and it can be applied to defense some

complicated attacks by the complex algorithm. The disadvantages are that the additional nodes increase network cost and the interferences among nodes are also increased. This scheme can be applied to applications with high security requirements or potential security issues, such as military scenarios.

3. As the high-performance device, this kind of MN can detect intrusions without limitations of resource constraints. It is benefitial to detect intrusions effectively, with the most expensive cost. Also the special devices may lead to more intrusions to them. But it is still a useful scheme for some serious mission-task scenarios.

5.1.3. Estimation of stand-alone IDS

The advantage of stand-alone IDS is robust, since each MN can complete intrusion detection independently. When some MNs become invalid, others can operate as normal. This system architecture is relatively simple, which is easy for deployment and implementation. The stand-alone IDS with distributed MN also considers the energy consuming problem of RPL. Three kind of schemes to different application scenarios are designed.

The stand-alone IDS architecture also has some disadvantages. The MNs do not cooperate or share information with others, which limits the detection efficiency. Moreover, since the MNs are equal and operate their IDS dependently, the detection results might have some collisions.

5.2. Distributed and Cooperative IDS

In distributed and cooperative IDS, intrusion detection is accomplished by the cooperation of MNs. Each MN runs an IDS agent to participate in the intrusion detection and response to the overall network. This kind of IDS applies two levels coordinate architecture with neighbor-agent and local-agent. The deployment of agents and the agent device type can refer to stand-alone IDS (in 5.1).

When a local-agent detects an intrusion with sufficient evidence, it can alert intrusion independently. While the local-agent detects an intrusion with weak or inconclusive evidence, it can initiate a global detection procedure by interactive connection with neighbor-agents. With the exchanges of data and responses, the globe response will be delivered to each agent.

The distributed and cooperative IDS is suitable to the flat network infrastructures, such as a DODAG in RPL. Thus, it can be applied to small-scale network. The distributed and cooperative IDS solves the low detection efficiency problem in stand-alone IDS, but with a more complicated architecture.

5.3. Distributed and Hierarchical IDS

In large-scale RPL network, the network topology is usually composed of several DODAGs, and the sink node of each DODAG connects together to the internet. Thus RPL can be regarded as a multi-layer network. The distributed and hierarchical IDS is promoted for such clustering network. This IDS is of two level architecture. As the cluster heads (CH), sink nodes are CH-agents. And the local-agents are deployed and designed according to stand-alone IDS (in 5.1).

Each local-agent operates independently, and reports the detection results to CH-agents. CH-agents are responsible to monitor the member nodes and make the global intrusion detection decisions. CH-agents complete the association and aggregation of alerts in the DODAG, and the neighbor CH-agents can coordinate to complete the cross-DODAG intrusion detection.

Since local-agent and CH-agent coordinate architecture does not need the coordination of neighbor-agents, it decreases the risk of eavesdropping. But the globe response by CH-agents might cause a long delay.

5.4. Mobile Agent IDS

Mobile agent [Li2012] is assigned to perform monitoring task in a selected node, based on specific tasks. The mobile agents cooperatively perform the intrusion detection. And the selection of agents might be changed after the task is completed or after a certain time period. The movement of agents is usually evolved from RPC methods through data duplication. The mobile agent saves its own state, transfers the saved state to the new node, and resumes execution from the saved state. The mobile agent is characterized by the following attributes.

- o Mobility: Mobile agents can actively migrate between nodes for asynchronous execution at any time during their execution. This makes them powerful to deal with distributed RPL applications. Also the mobility characterize can increase the efficiency of IDS.

- o Autonomy: Mobile agents operate independently without any manual intervention, and use preprogrammed knowledge in order to execute general tasks. They are also expected to be able to analyze the changes of a network and take intuitive action accordingly.

The above attributes virtually improve the function of IDS in RPL. However the mobile agent IDS architecture also has several disadvantages, and this document only gives some sketchy introduction, the detailed discussion may be included in the future. The main disadvantages are listed below.

- Resource consumption: The IDSs may consist of a large amount of codes, which might be very time-consuming for transfering codes between agent nodes. Moreover the additional codes will cause a resource overhead. Since all nodes are prepared to serve as a mobile agent, the additional processes increase energy consumption. The resource consumption problem must be effectively solved in RPL before its application.

- Decisional confliction: Since the mobile agents usually have equal status, the confliction is still hard to avoid.

- Security: The mobility and autonomy characteristics of mobile agent also make it unsecure from intrusions.

6. Detection data

In aformentioned system architecture of IDSs, MNs defense intrusions by detecting system data. This section mainly discusses the source of data and the data detection frequency.

6.1. Detection source location

The source of detection data can be classified into three groups, including host-based, network-based and hybrid.

- Host-based IDS: When the IDS only concern events on the host, the source of detection data is host-based. This kind of detection can be achieved in application or system log files on the host.

- Network-based IDS: The IDS places sniffers on interconnection equipment, captures and examines the transmitting packets. It can detect packets, payload or other information within the packet.

- Hybrid IDS: The hybrid IDS is a combination of host-based and network-based IDS.

6.2. Collection frequency

Considering the resource-constrained characteristic of LLNs devices, data detection frequency can be adjusted according to different application scenarios. For real-time applications, MNs should detect

the data continuously or in a high frequency. In the contrary, in applications such as weather prediction, a proper detection interval is indispensable.

7. Intrusion response

As the second line of defence, IDSs do not do preventive tasks and the IDS reacts when an intrusion is detected. This document simply introduces the following intrusion response, and the detailed action can be discussed in future docuemnts.

o The system may generate an alarm to inform the administrator or the sink node, so as to decide the reaction to the intrusion.

o The system may react in the corrective action, such as designing a new rule in a firewall or disconnection of suspicious connections, which can prevent the identical future intrusions.

o A mitigation method may be induced as the third line of defence in a comprehensive system, and the mitigation detection can stop the intrusion with information provided by the IDS.

8. A general design of IDS for ETX intrusion detection

The above document analyzes several aspects of IDS with promotions based on different application scenarios. The self-organizing capability makes RPL be vulnerable to intrusions, especially the new type of internal intrusions. Thus this section gives an example of designing the IDS to defense ETX intrusion with single intruder, which is a new type of internal intrusion in RPL.

8.1. ETX intrusion

RPL constructs auto-optimized topology based on metric and constrains. In RPL with ETX metric[De2005], node chooses preferred parent based on integrated ETX value, which is composed by neighbor ETX value from received DIO messages and counted link ETX value to that neighbor. Usually, node selects neighbor with smaller integrated ETX value as preferred parent. ETX intrusion can be developed by single intruder or multiple collaborated intruders. This section only deals with ETX intrusion with single intruder.

The intruder advertises DIO messages with fake ETX value, which misleads its neighbors to change preferred parents. It can form redundant route paths and break RPL auto-optimized topology, which degrades the network performance in many important QoS aspects, such as energy consumption, throughput and delay. The intruders only need

to ignore the legitimate ETX detection by itself, and then work as normal. Moreover, in LLNs devices, the cryptography techniques cannot be applied to examine DIO message, and thus neighbors cannot judge the legitimation of ETX value from received DIO messages. As a consequence, the ETX intrusion is easy to start and hard to detect.

8.2. Design of the IDS for ETX Intrusion

Assume that ETX intrusion with single intruder is happened in a stable network environment without other intrusions, and the network initialization is secure. The IDS to defense this intrusion is designed as follows.

- Detection methodology: The IDS applies specification-based detection methodology, which can detect novel intrusions with a lower false alarm rate.

- System architecture: The IDS applies stand-alone system architecture, which is simple and effective to defense single intruder without collaboration. Considering RPL resource-constrained characteristic, stand-alone IDS employs distributed MN with FSM architecture. Since the network environment is stable, MN devices employ RPL devices, which do RPL jobs as well as the monitoring work.

  The deployment of distributed MNs is accomplished with minimal MNs before network initialization, and each RPL node is in the range of at least one MN. Thus MNs can collect the complete information of neighbors to detect intrusions.

  In distributed MN with FSM, MNs passively listen to RPL packets, extract and record useful information in a dynamically updated list. The FSM operates the detection based on that list. Since specification-based IDSs detect intrusions by comparing network behavior deviations, before designing FSM, normal RPL behaviors should be discussed. In stable network environment, link ETX values are nearly the same, and the integrated ETX value is only depended on neighbor ETX value. Thus the selection of preferred parent is only decided on neighbor ETX value. In secure RPL environment, neighbor ETX values may change but without leading massive topology fluctuation. Thus, in a stable RPL environment, when a node broadcasts DIO message with decreased ETX value, the number of its child nodes might be increased. If the increase number of child nodes exceeds a threshold, that node must be an ETX intruder.

According to above discussions, the list of MNs should include useful information of all neighbors, including ETX value from DIO messages, preferred parent from DAO messages, and child node number counted by list item of preferred parent. There are six states in FSM, including the start when network initialize, the route path setup/change, the packets detection, the invalid route, the network fluctuation and the ETX intrusion alarm.

1. When MN first receives a DIO message, its state will move to topology setup/change state, in Step 2. The MN will record ETX value, and build an entry for that node in its list.

2. In topology setup/change state, when MN sniffs DIO or DAO message, its state is transited to packets detection state, in Step 3.

   When the list record shows that parent and child ETX relationship is broken (parent node has bigger ETX value), the state of FSM is transited to invalid route state, in Step 4.

   When the recorded ETX value is decreased, the FSM state is transited to network fluctuation state, in Step 5.

3. In packets detection state, if the node is new, MN will build an entry and record information of that node to its list. Otherwise the MN will update the corresponding ETX value from DIO message or preferred parent information from DAO message. Then the FSM state is transitted back to topology setup/change state, in Step 2.

4. In invalid route state, an RPL local repair mechanism is needed to recover the network topology.

5. In network fluctuation state, a time counter will be started for that node to examine asynchronously consequences. Before the timer expiration, if the number of child nodes increases to exceed a threshold, the FSM state will move to ETX intrusion alarm state, in Step 6. The threshold is depended on the network environment and the network scale.

6. In ETX intrusion alarm state, MN broadcasts ETX intrusion alarm packets. There might be a feedback mechanism to make sure that the intrusion is noted by all neighbors.

- o Detection data: The detection data is network-based, and the detection frequency is the same as data packet sending frequency.

- o Intrusion response: The IDS reacts in a corrective action. When ETX intrusion is detected, the MN will broadcast alarms. Nodes which receive the alarm will mark the intruder to avoid intrusion again, and then check their parent list. If the intruder exists in the parent list, it will delete the intruder and reselect its preferred parent immediately. In this way, the intruder cannot start ETX intrusions anymore.

9. Security Considerations

In RPL, the network security solution is largely limited by its resource-constrained characteristic. This document specifies IDSs as the second line to defence intrusions. However it does not take much consideration on the security of IDSs, since RPL nodes may do not have enough capability in using prevention detection methods to protect the IDS process.

This document proposes three type MN devices (in 5.1.2), and the latter two kinds may have the ability to adopt the prevention machine. Some simple security machines such as simple authentication, or other novel machines such as sequence authentication, can be considered to be applied to secure the IDSs.

10. IANA Considerations

This memo includes no request to IANA.

11. Conclusions

This document specifies IDSs as the second line of defence for RPL. Due to RPL self-organizing characteristics, it is necessary to design IDS to defence intrusions, especially the internal intrusions. This document first analyzes three type detection methodologies, and promotes the specification-based method to RPL. Then it mainly discusses the system architecture of IDSs. In stand-alone IDS, the distributed MN with FSM architecture is promoted with three types of MN device in different RPL applications. The distributed and cooperative IDS is promoted to flat network infrastructure, such as a DODAG. The distributed and hierarchical IDS is promoted in large-scale network with several DODAGs. And there are also some sketchy introductions on mobile agent IDS, which may be discussed in the future. The document also specifies detection data with data source and collection frequency. In addition, this document gives the intrusion responses to complete the IDS process. To explicitly show the design of IDSs, this document gives an example to apply IDS to defense ETX intrusion with single intruder, which is a novel internal

RPL intrusion. At last this document presents some security considerations for IDSs in RPL.

12. References

12.1. Normative References

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

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

[RFC4443] Conta, A., Deering, S., and Gupta, M., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

12.2. Informative References

[ROLL-TERMS]
Vasseur, JP., "Terminology in Low power And Lossy Networks", Work in Progress, March 2013.

[Farooqi2012] Farooqi, A. H., and Khan, F. A. "A survey of intrusion detection systems for wireless sensor networks", Proc. International Journal of Ad Hoc and Ubiquitous Computing 2012 PP. 69-83.

[Le2012] Le, A., Loo, J., Lasebae, A., Aiash, M., and Luo, Y. "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach", Proc. International Journal of Communication Systems 2012 pp. 1189-1212.

[Tseng2003] Tseng, C, Y., Balasubramanyam, P., Ko, C., Limprasittiporn, R., Rowe, J. and Levitt, K. "A specification-based intrusion detection system for AODV" Proc. the 1st ACM workshop on Security of ad hoc and sensor networks 2003 pp. 125-134.

[Shakshuki2011] Shakshuki, E., Kang, N., and Sheltami, T. "EAACK-A Secure Intrusion-Detection System for MANETs", Proc. Industrial ElectronicsIEEE Transactions 2013 pp. 1089-1098.

[Garcia2009]Garcia-Teodoro, P., Diaz-Verdejo, J., et al. "Anomaly-based network intrusion detection: Techniques, systems and challenges", Proc. computers & security 2009 PP. 18-28.

[Li2012] Li, Y., and Qian, Z. "Mobile agents-based intrusion detection system for mobile ad hoc networks", Proc. Innovative Computing & Communication 2010 Intl Conf on and Information Technology & Ocean Engineering, 2010 Asia-Pacific Conf 2010 pp. 145-148.

[De2005] De, Couto, D. S., Aguayo, D., Bicket, J., and Morris, R. "A high-throughput path metric for multi-hop wireless routing", Proc. Wireless Networks 2005 PP. 419-434.

13. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Lan Zhang, Gang Feng, Shuang Qin
National Key Laboratory of Science and Technology on Communications
UESTC (University of Electronic Science and Technology of China)
No.2006, Xiyuan Ave, West Hi-Tech Zone
Chengdu, Sichuan, P.R.China 611731

Phone: +86 151-9663-7390
Email: zhanglan_uestc@163.com
fenggang@uestc.edu.cn
blueqs@uestc.edu.cn