Monitoring and Security for the Internet of Things

Anthéa Mayzaud, Rémi Badonnel, Isabelle Chrisment

Monitoring and Security for the Internet of Things

A. Mayzaud, R. Badonnel and I. Chrisment

Université de Lorraine, LORIA, UMR 7503, France
Inria Grand Est - Nancy, France

Abstract. The concept of Internet of Things involves the deployment of Low power and Lossy Networks (LLN) allowing communications amongst pervasive devices such as embedded sensors. A dedicated routing protocol called RPL has been designed to consider the constraints of these LLN networks. However, the RPL protocol remains exposed to many security attacks that can be very costly in time and energy. In this paper, we propose to exploit risk management methods and techniques to evaluate the potentiality of attacks and to dynamically reduce the exposure of the RPL protocol while minimizing resources consumption.

1 Introduction and Challenges

The growing interest for the Internet of Things has resulted in the large-scale deployment of Low power and Lossy Networks, such as wireless sensor networks and home automation systems. These networks have strong constraints in terms of resources (energy, memory, power) and their communication links are by nature characterized by a high loss rate and a low throughput. Moreover the traffic patterns are not simply point-to-point, but in many cases the devices communicate according to a point-to-multipoint or multipoint-to-point schema. Existing routing protocols for wired networks (OSPF, IS-IS) and for ad-hoc networks (AODV, OLSR) are not suitable to deal with all these requirements. The IETF ROLL[1] working group has proposed a new routing protocol called RPL (Routing Protocol for Low power and Lossy Networks) based on IPv6 and specifically designed for these environments [1]. These RPL-based networks may be exposed to a large variety of attacks [2], but the deployment of security mechanisms may also be quite expensive in terms of resources. In that context, we propose to exploit risk management methods and techniques to detect and prevent attacks while preserving resources in these networks. Risk management allows to dynamically adapt the selection of security countermeasures with respect to the observed threats. In the following of the paper, we will give an overview of the RPL protocol and its security issues, and then describe how risk management can be applied to these networks.

[1] Routing Over Low power and Lossy networks

2 RPL Protocol and its Security Issues

The RPL protocol is a distance-vector routing protocol based on IPv6, where devices are interconnected according to Destination Oriented Directed Acyclic Graphs (DODAG) [3]. An illustration of such a network is given in the lower plane of Figure 1. A network is composed of one or several DODAGs grouped into a RPL instance which is associated to an objective function. An objective function computes the best path for a set of metrics or constraints. A RPL node can join several instances at the same time but it can only join one DODAG per instance. For example in Figure 1, the node 11 is part of the RPL instances 1 and 2 in the DODAGs 2 and 3. These multiple instances enable the protocol to perfom different optimizations, such as quality-of-service. A set of ICMPv6 control messages is defined to exchange RPL routing information. A DODAG is built from a root which is the data sink of the graph. A rank is associated to each node and corresponds to its location in the graph with respect to the root. The node rank is always increasing in the downward direction, as illustrated in the DODAG 2 of Figure 1.

This procotol is exposed to multiple security attacks such as traffic interception, node resource exhaustion or denial of service [4]. For instance, a malicious node can voluntarily decrease its rank value to get closer to the root and intercept more traffic. A malicious node can also simply refuse to route messages, provide incorrect routing information data, or flood the network to perform denial of service. RPL already defines several mechanisms contributing to its security. It integrates local and global repair mechanisms to detect and avoid loops. It also considers two potential security modes. The pre-installed mode consists in having nodes with pre-installed keys in order to send secured messages. The authenticated mode considers that nodes with pre-installed keys can only join a DODAG as leaf, and must obtain a key from an authenticated authority to join the graph as a router. Complementary security mechanisms from regular protocols can also be envisioned to cover a larger variety of attacks, such as distributed denial-of-service attacks. The deployment of such security mechanisms (envisioned or not by the protocol) can be quite expensive in terms of network resources and may impact on the overall performances.

3 Risk Management applied to RPL-based Networks

Risk management offers new perspectives to dynamically activate or deactivate security mechanisms in RPL-based networks, in order to prevent attacks while maintaining network performances. We propose in this paper to investigate risk management methods and techniques for addressing the trade-off between security and cost in the Internet of Things. The risk level is traditionally defined as a combination of the probability of the attack and its consequences but may also be decomposed as given by Equation 1 [5].

$$\mathcal{R}(a) = P(a) \times E(a) \times C(a) \tag{1}$$

Let consider a security attack noted a. The risk level $R(a)$ depends on the potentiality $P(a)$ of the attack, the exposure $E(a)$ of the RPL network, and the consequences $C(a)$ on the network if the attack succeeds [6]. Risk management is a process consisting in monitoring, prioritizing and controlling risks [7]. For instance, when this process observes a high potentiality $P(a)$, it may activate security mechanisms (being aware of their costs) to reduce the exposure $E(a)$ and maintain the risk level $R(a)$ to a low value [8]. As depicted on the upper plane of

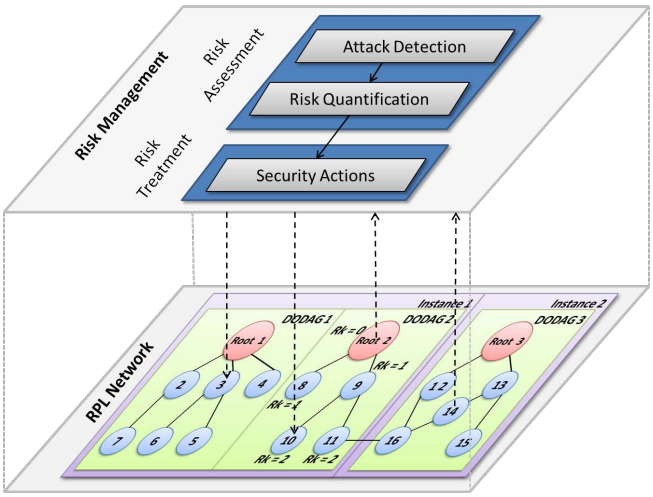

Fig. 1. Risk Management Applied to RPL Networks

Figure 1, the process is composed of two main activities: risk assessment and risk treatment. Risk assesment consists in quantifying the potentiality of attacks. For that, it is necessary to evaluate the performance of detection techniques (based on anomalies or known signatures) in these RPL environments, and to identify the network nodes able to perform this activity. Risk assessment aims also at quantifying the consequences of successful attacks. The objective is to assess the relative importance of nodes in the RPL network, and to analyze how the attack against a given node may impact on the functioning of the overall network. The risk treatment activity consists then in selecting and applying the security mechanisms that are needed. The activities of suspicious nodes can be mitigated, or the nodes can be (partially) excluded from the RPL network. For instance, the number of requests from them may be restricted over time, or the considered RPL nodes may not be allowed to act as routers anymore. The selection of countermeasures takes into account the costs induced by their activation on the RPL network. As previously mentioned, this cost is often not negligeable in such a critical environment. A typical illustration of this statement has been given in [9] where the authors showed that the traffic generated by a loop avoidance mechanism was higher than the one generated by the loops themselves most of the time.

4 Conclusions and Perspectives

The Internet of Things is typically based on the deployment of Low power and Lossy networks. Those ones have scarce resources in terms of energy, power and memory, and rely on limited communication links. Their development has led to the specification of a dedicated protocol, called RPL, by the IETF ROLL working group. These networks are exposed to multiple attacks. While security mechanisms are available or could be adapted, their activation may degrade the network performance. We propose to apply risk management methods in these networks in order to address the trade-off between security and cost. The objective is to dynamically adapt the network exposure with respect to the threat potentiality, through the activation or deactivation of dedicated countermeasures. As future work, we plan to classify the different security mechanisms available (or potentially applicable) for these networks and to analyze their cost and their coverage against current security attacks. We are also interested in other attacks such as diversion attacks. We will then work on the design, the implementation and the evaluation of our risk management strategy through proof-of-concept prototyping and simulations using Cooja or ns-3 [10].

Acknowledgements. This work was funded by Flamingo, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.

References

1. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J., Alexander, R.: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. Request for Comments 6550 (Proposed Standard), IETF (2012)
2. Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A.: Security Framework for Routing over Low power and Lossy Networks, IETF Requirement Draft for Routing over Low power and Lossy Networks (ROLL), Work in progress. (2012)
3. Gaddour, O., Koubâa, A.: RPL in a Nutshell: a Survey. Elsevier Journal Computer Networks (2012)
4. Boumessouer, M., Chrisment, I., Frikha, M.: Analysis of Vulnerabilities and Attacks in the RPL Routing Protocol, in French, Master Thesis Report, Supcom Engineering School (July 2012)
5. NIST: An Introduction to Computer Security: The NIST Handbook (1995)
6. Dabbebi, O., Badonnel, R., Festor, O.: Managing Risks at Runtime in VoIP Networks and Services. In: Proc. of the IFIP International Conference on Autonomous Infrastructure, Management and Security (IFIP AIMS'2010). (June 2010)
7. Bedford, T., Cooke, R.: Probabilistic Risk Analysis: Foundations and Methods. Cambridge University Press (2001)
8. Gehani, A., Kedem, G.: RheoStat : Real-Time Risk Management. In: Proc. of the 7th International Symposium RAID'2004. (2004)
9. Xie, W., Goyal, M., Hosseini, H., Martocci, J., Bashir, Y., Baccelli, E., Durresi, A.: Routing Loops in DAG-Based Low Power and Lossy Networks. In: Proc. of the 24th IEEE International Conference on Advanced Information Networking and Applications. AINA'10, Washington, USA, IEEE Computer Society (2010)
10. Bartolozzi, L., Pecorella, T., Fantacci, R.: ns-3 RPL Module: IPv6 Routing Protocol for Low Power and Lossy Networks. In: Proc. of the 5th International Conference on Simulation Tools and Techniques. SIMUTOOLS'12 (2012)