Journal of Information Security and Applications 61 (2021) 102939

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Multicast DIS attack mitigation in RPL-based IoT-LLNs

Faiza Medjek [a,b,*], Djamel Tandjaoui [a], Nabil Djedjig [a,b], Imed Romdhani [c]

[a] Research Centre on Scientific and Technical Information, 05, Rue des Trois Freres Aissou, Ben Aknoun, Algiers, Algeria
[b] Departement Informatique, Faculte des Sciences Exactes, Universite de Bejaia, 06000 Bejaia, Algeria
[c] Edinburgh Napier University, School of Computing, 10 Colinton Road, EH10 5DT, Edinburgh, UK

ARTICLE INFO

Keywords:
RPL
RPL security
Internet of Things
DIS attack
Routing attacks
Low Power and Lossy Networks

ABSTRACT

The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) was standardised by the IETF ROLL Working Group to address the routing issues in the Internet of Things (IoT) Low-Power and Lossy Networks (LLNs). RPL builds and maintains a Destination Oriented Directed Acyclic Graph (DODAG) topology using pieces of information propagated within the DODAG Information Object (DIO) control message. When a node intends to join the DODAG, it either waits for DIO or sends a DODAG Information Solicitation (DIS) control message Multicast to solicit DIOs from nearby nodes. Nevertheless, sending Multicast DIS messages resets the timer that regulates the transmission rate of DIOs to its minimum value, which leads to the network's congestion with control messages. Because of the resource-constrained nature of RPL-LLNs, the lack of tamper resistance, and the security gaps of RPL, malicious nodes can exploit the Multicast DIS solicitation mechanism to trigger an RPL-specification-based attack, named DIS attack. The DIS attack can have severe consequences on RPL networks, especially on control packets overhead and power consumption. In this paper, we use the Cooja–Contiki simulator to assess the DIS attack's effects on both static and dynamic PRL networks. Besides, we propose and implement a novel approach, namely RPL-MRC, to improve the RPL's resilience against DIS Multicast. RPL-MRC aims to reduce the response to DIS Multicast messages. Simulation results demonstrate how the attack could damage the network performance by significantly increasing the control packets overhead and power consumption. On the other hand, the RPL-MRC proposed mechanism shows a significant enhancement in reducing the control overhead and power consumption for different scenarios.

1. Introduction

In the Internet of Things (IoT) concept, all physical objects are identifiable, addressable, and interconnected with each other exploiting their standard underlying technologies such as ubiquitous and pervasive computing, embedded devices, communication technologies, sensor networks, and Internet protocols [1–3]. One of the main building blocks of the IoT is the Low-power and Lossy Networks (LLNs). LLNs are made of a collection of interconnected embedded resource-constrained devices, such as RFID and sensor nodes with low computational and storage capabilities and are often battery operated. In addition, communication technologies are subject to high packet loss, frame size limitations, low data rates, short communication ranges, and dynamically changing network topologies. Such limitations render the development of efficient routing solutions for LLNs crucial [4–6]. Several attempts have been proposed to handle these issues, like CTP [7], and Hydro [8]. Ultimately, the ROLL IETF Working Group has designed and standardised the Routing Protocol for LLNs, namely the Routing Protocol for Low-Power and Lossy Networks (RPL) [9,10]. These last years, several studies reported that RPL suffers from security limitations that harm its performances [11,12].

1.1. RPL overview

RPL [10] is a distance vector routing protocol that organises the physical network into a logical representation as a Directed Acyclic Graph (DAG) to route data packets. The DAG comprises one or multiple DODAGs (Destination Oriented DAGs) with one root per DODAG. Each root, called a border router (BR), is connected to the Internet, and other potential roots (BRs) via a backbone. Each node in the DODAG has many attributes such as an IPv6 address (ID), a list of parents with one preferred-parent, a list of discovered neighbours and a Rank. The Rank of a node identifies the node's position relative to the BR, respecting the rule that the parent has a lower Rank than the node itself. Specifically, the Rank values should increase from the BR towards the leaf nodes and decrease from the leaf nodes towards the BR. RPL

[*] Corresponding author at: Research Centre on Scientific and Technical Information, 05, Rue des Trois Freres Aissou, Ben Aknoun, Algiers, Algeria.
E-mail address: fmedjek@cerist.dz (F. Medjek).

https://doi.org/10.1016/j.jisa.2021.102939

Available online 27 July 2021