Ad Hoc Networks 11 (2013) 2661–2674

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

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

SVELTE: Real-time intrusion detection in the Internet of Things

Shahid Raza [a,*], Linus Wallgren [a], Thiemo Voigt [a,b]

[a] SICS Swedish ICT, Stockholm, Sweden
[b] Department of Information Technology, Uppsala University, Sweden

ARTICLE INFO

Article history:
Available online 17 May 2013

Keywords:
Intrusion detection
Internet of Things
6LoWPAN
RPL
IPv6
Security
Sensor networks

ABSTRACT

In the Internet of Things (IoT), resource-constrained things are connected to the unreliable and untrusted Internet via IPv6 and 6LoWPAN networks. Even when they are secured with encryption and authentication, these things are exposed both to wireless attacks from inside the 6LoWPAN network and from the Internet. Since these attacks may succeed, Intrusion Detection Systems (IDS) are necessary. Currently, there are no IDSs that meet the requirements of the IPv6-connected IoT since the available approaches are either customized for Wireless Sensor Networks (WSN) or for the conventional Internet.

In this paper we design, implement, and evaluate a novel intrusion detection system for the IoT that we call SVELTE. In our implementation and evaluation we primarily target routing attacks such as spoofed or altered information, sinkhole, and selective-forwarding. However, our approach can be extended to detect other attacks. We implement SVELTE in the Contiki OS and thoroughly evaluate it. Our evaluation shows that in the simulated scenarios, SVELTE detects all malicious nodes that launch our implemented sinkhole and/or selective forwarding attacks. However, the true positive rate is not 100%, i.e., we have some false alarms during the detection of malicious nodes. Also, SVELTE's overhead is small enough to deploy it on constrained nodes with limited energy and memory capacity.

1. Introduction

With IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) [1,2] it is possible to connect resource constrained devices, such as sensor nodes, with the global Internet using the standardized compressed IPv6 protocol. These networks of resource constrained devices, also called 6LoWPAN networks, and the conventional Internet form the Internet of Things or strictly speaking the IP-connected Internet of Things (IoT). A 6LoWPAN Border Router (6BR) is an edge node that connects 6LoWPAN networks with the Internet. Due to the resource constrained nature of the devices or *things*, 6LoWPAN networks mostly use IEEE 802.15.4 as link and physical layer protocol.

Unlike typical wireless sensor networks (WSN), 6LoWPAN networks or IP-connected WSN are directly connected to the untrusted Internet and an attacker can get access to the resource-constrained *things* from anywhere on the Internet. This global access makes the *things* vulnerable to intrusions from the Internet in addition to the wireless attacks originating inside 6LoWPAN networks. Potential applications of the IoT are smart metering, home or building automation, smart cities, logistics monitoring and management, etc. These applications and services are usually charged and the revenue is based on data or services used. Hence, the confidentiality and integrity of the data and timely availability of services is very important.

Researchers have already investigated message security for the IoT using lightweight DTLS [3], IPsec [4], and IEEE 802.15.4 link-layer security [5]. Even with message security that enables encryption and authentication, networks are vulnerable to a number of attacks aimed to disrupt the network. Hence, an Intrusion Detection System (IDS)

* Corresponding author.
E-mail addresses: shahid@sics.se (S. Raza), linus@sics.se (L. Wallgren), thiemo@sics.se (T. Voigt).

1570-8705/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2013.04.014

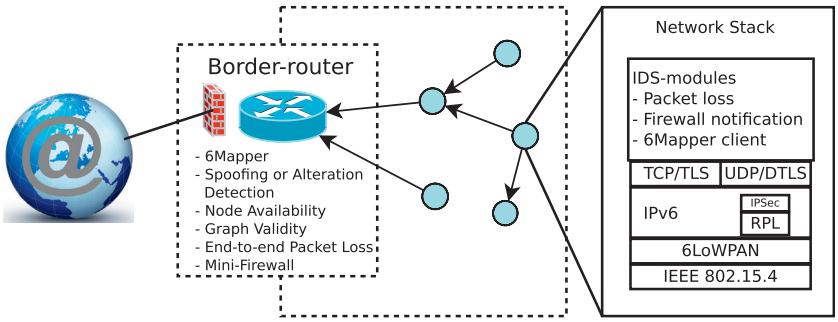

Fig. 1. An IoT setup where IDS modules are placed in 6BR and also in individual nodes.

is necessary to detect intruders that are trying to disrupt the network.

The available IDSs for WSNs could be used in the IoT. However, most of these approaches are built on the assumptions that (i) there is no central management point and controller, (ii) there exists no message security, and (iii) nodes cannot be identified globally. The IoT has a novel architecture where the 6BR is assumed to be always accessible, end-to-end message security is a requirement [5], and sensor nodes are globally identified by an IP address. Besides these opportunistic features, an IDS for the IoT is still challenging since the *things* (i) are globally accessible, (ii) are resource constrained, (iii) are connected through lossy links, and (iv) use recent IoT protocols such as CoAP [6], RPL [7], or 6LoWPAN [2]. Therefore, it is worth investigating and providing an IDS for the IoT exploiting these opportunities and threats.

To this end, we design, implement, and evaluate a novel Intrusion Detection system for the IoT that we call SVELTE.[1] To the best of our knowledge this is the first attempt to develop an IDS specifically designed for the IoT. Network layer and routing attacks are the most common attacks in low power wireless networks [8], and in this paper we primarily target these attacks. SVELTE is also inherently protected against sybil and clone ID attacks; we discuss these attacks in Section 3.2.5. We evaluate SVELTE against sinkhole and selective-forwarding attacks. Our approach is, however, extensible and can be used to detect other attacks as we discuss in Section 7.

The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) [7] is a novel standardized routing protocol primarily designed to meet the specific routing requirements of the IoT. SVELTE uses RPL as a routing protocol. It has two main components: the 6LoWPAN Mapper (6Mapper), and intrusion detection modules. The 6Mapper reconstructs RPL's current routing state, i.e., its directed acyclic graph, at the 6BR and extends it with additional intrusion detection parameters.

One of the important decisions in intrusion detection is the placement of the IDS in the network. We use a hybrid approach, see Section 3, and place the processing intensive SVELTE modules in the 6BR and the corresponding lightweight modules in the constrained nodes. Fig. 1 presents an overview of our IDS that we explain in more detail in Section 3. One of our main design goals is that the IDS should be lightweight and comply with the processing capabilities of the constrained nodes.

In addition to the 6Mapper and the intrusion detection techniques, we also propose and implement a distributed mini-firewall to protect 6LoWPAN networks against global attackers from Internet. We implement SVELTE in the Contiki operating system [9].

The main contributions of this paper are:

- We present SVELTE, a novel IDS with an integrated mini-firewall for the IP-connected IoT that uses RPL as a routing protocol in 6LoWPAN networks.
- We implement SVELTE and thoroughly evaluate it for 6LoWPAN networks that consist of resource-constrained *things* and have lossy communication links.

The next section of this paper gives an overview of the technologies used in SVELTE. Section 3 describes SVELTE that includes 6Mapper, the actual intrusion detection techniques, and the firewall. In Section 4 we detail SVELTE's implementation for the Contiki OS. Section 5 presents our detailed performance evaluation of SVELTE. We highlight the current IDSs and their applicability in the IoT in Section 6. Section 7 discusses the possible extensions in SVELTE, and finally we conclude the paper in Section 8.

2. Background

In this section we briefly discuss the technologies involved in SVELTE for the IoT.

2.1. The Internet of Things

The Internet of Things (IoT) or strictly speaking IP-connected IoT is a hybrid network of tiny devices, typically WSNs, and the conventional Internet. Unlike typical WSN where devices are mostly resource constrained and unlike in the Internet where devices are mostly powerful, the nodes or *things* in the IoT are heterogeneous devices. An IoT device can be a light bulb, a microwave, an electricity meter, an automobile part, a smartphone, a PC or a laptop, a powerful server machine or a cloud, or potentially anything. Hence the number of potential devices that can be connected to the IoT are in hundreds of billion. IPv6's huge address space has been designed to address this issue.

[1] SVELTE literary means *elegantly slim*.