Poster: State of the Art IDS Design for IoT

Ahmet Aris and Sema F. Oktug
Faculty of Computer and Informatics
Istanbul Technical University, Turkey
{arisahmet, oktug}@itu.edu.tr

Abstract

This paper summarizes the ongoing work of us which aims to protect Internet-of-Things networks against Denial-of-Service attacks. The attacks that our anomaly-based Intrusion Detection System targets can be insider or outsider attacks. The system we are proposing can be thought of as an improved version of SVELTE IDS which successfully solves the problem of detection system components' placement within the low power and lossy network. Similar to the reference work, we place the monitoring part of the detection system to the resource constrained devices and the detection part to the border router. In addition to this, we consider extended 6LoWPAN networks and incorporate the cooperative autonomous detection model so that multiple IoT networks sharing the same DODAG ID cooperate and get stronger against coordinated attacks.

1 Introduction

Internet of Things (IoT) is a network of sensors, actuators and various devices that can connect to Internet. IETF and IEEE proposed several standards [4] in order to enable nodes to form an energy-efficient IoT network and connect to the Internet by means of Internet Protocol (IP). Although cryptography-based security solutions were suggested by the standardization authorities [6], IoT networks are still vulnerable to the attacks called as Denial of Service (DoS) attacks [1].

In this ongoing work, we aim to design an anomaly-based Intrusion Detection System (IDS) which is capable of protecting the IoT network from both insider and outsider attackers. As devices in IoT are resource-constrained and anomaly-based IDS requires computationally intensive operations, placement of IDS modules in IoT network becomes a critical issue. SVELTE [5] comes up with a very handy solution where the monitoring part of the IDS that is computationally lightweight is placed onto resource-constrained nodes and the resource-intensive part is placed onto the Border Router (BR). This separation removes the burden of attack detection from IoT nodes and provides the necessary monitoring data to the BR. Although SVELTE seems to be a perfect match in terms of IDS tailored for IoT, it does not consider coordinated attackers. It also targets only routing attacks and actually a portion of routing attacks. We believe that an IDS for IoT networks should consider coordinated attackers and also should cover most of the insider D/DoS attacks. In order to protect IoT from coordinated attackers, IDSs have to cooperate and share information with each other. Therefore, we employ the idea of Cooperative Autonomous Attack Detection (CATS) [2] so as to cooperate IDSs with each other. As a result, we came up with an IDS which benefits from SVELTE and CATS and proposes a DDoS protection system that can detect the majority of insider attacks; can cooperate with other IDSs sharing the same RPL Instance IDs to protect IoT from coordinated attackers.

2 State-of-the-Art Intrusion Detection System for Internet-of-Things

In this section, we will summarize SVELTE and CATS which are the basis of our proposal.

SVELTE proposes an IDS which is tailored for the needs of IoT networks. It targets routing attacks, namely sinkhole and selective forwarding attacks. The main contribution of SVELTE is that, it places lightweight IDS modules to resource-constrained nodes and resource-hungry anomaly detection module to the BR. Each IDS module in nodes periodically send node ID, DODAG ID, version, rank, parent and neighbor information to the main module on BR. Main module detects the anomalies by means of the inconsistencies in the DODAG. Main module also includes a firewall, that aims to protect the IoT network from known outsider attacks. White list approach is used to mitigate the effects of the attacker within the network.

CATS separates the network monitoring from the attack detection and tries to make use of distributed nature where distributed detection systems share information with each other but make decisions independently. It employs both anomaly-based and knowledge-based detection techniques. Monitoring part of the IDS provides monitored data to the detection module and also exports the monitored data to other distributed detection modules. Detection module on

International Conference on Embedded Wireless Systems and Networks (EWSN) 2017
20–22 February, Uppsala, Sweden

ISBN: 978-0-9949886-1-4

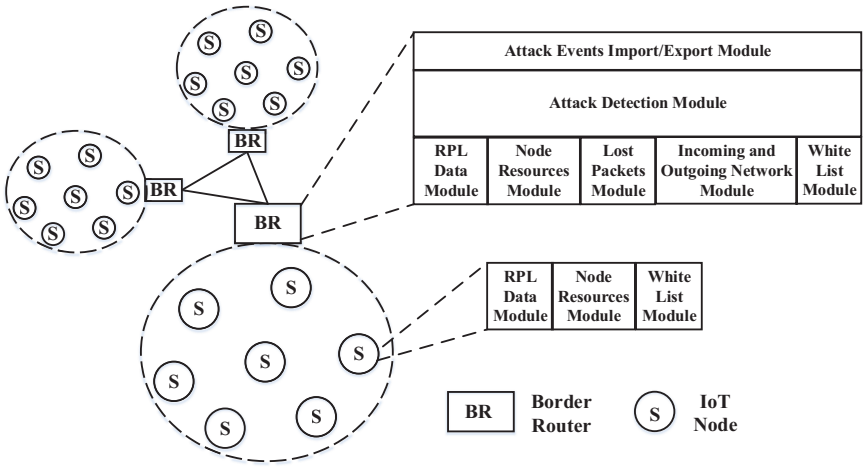

Figure 1. Proposed IDS Block Diagram.

the other hand, perform anomaly and signature/rule based detection and exports detected events to other distributed detection modules. By this way, each IDS strengthens its detection performance with the help of others.

2.1 Proposed Work

In this work, we wanted to benefit from both SVELTE and CATS in order to detect insider and outsider attackers efficiently in IoT networks. Based on these works, we came up with an IDS as shown in the Fig. 1. We followed the approach of SVELTE in which we place resource hungry modules to BRs and lightweight monitoring modules to nodes.

Every IoT node has RPL Data, Node Data and White List modules. RPL Data Module provides the same information SVELTE nodes provide but additionally provides RPL control message information logs to the BR. Node data module provides information about the node resources (e.g., remaining battery, RAM usage, CPU usage). White List Module deals with the white list information BR router disseminates in case of a detected attacker.

As depicted in the figure, BR accommodates RPL Data, Node Resources, Lost Packets, Incoming and Outgoing Network modules in order to get useful information for detection of insider and outsider attacks. Here, RPL Data Module collects the information that RPL Data Modules of IoT nodes provide. Node Resources Module collects the state information of every node in the network. BR keeps track of packets and finds out the lost/dropped packets. So, Lost Packets Module provides relevant information. Incoming and outgoing network is analyzed and regarding source, destination, port, protocol, and various connection information are collected and pre-processed in Incoming and Outgoing Network Module. All of the aforementioned modules provide useful information to Attack Detection Module which we think will be an anomaly-based detection engine. But it can be a hybrid engine as well (i.e., anomaly and signature based detection engine). It will incorporate the idea of [3] to determine the most appropriate features for attack detection. This module additionally generates a white list and sends it to White List Module which is responsible from the dissemination of the white list information through the network. Anomaly Detection Module also generates attack events data which is shared with other Attack Detection Modules in the nearby BRs having the same RPL Instance IDs. Attack Detection Module not only makes use of the monitoring information from its own network but also the attack events data it receives from other Attack Detection Modules via Attack Events Import/Export Module.

3 Conclusions

In this poster paper, we summarized our ongoing work that aims to propose a novel IDS for IoT. We expect slight increase in the complexity of the software running on nodes and in the energy consumption will pay back with a more efficient IDS for IoT networks.

4 Acknowledgments

This study was supported by the 2211C - Domestic Doctoral Scholarship Program Intended for Priority Areas, No. 1649B031503218 of the Scientific and Technological Research Council of Turkey (TUBITAK).

5 References

[1] A. Aris, S. Oktug, and S. Yalcin. Internet-of-things security: Denial of service attacks. In *Signal Processing and Communications Applications Conference (SIU), 2015 23th*, pages 903–906, May 2015.

[2] F. Dressler, G. Münz, and G. Carle. Attack Detection using Cooperating Autonomous Detection Systems (CATS). In *1st IFIP International Workshop on Autonomic Communication (WAC 2004), Poster Session*, Berlin, Germany, October 2004. IFIP.

[3] K. Kalkan and F. Alagoz. A distributed filtering mechanism against {DDoS} attacks: Scoreforcore. *Computer Networks*, 108:199 – 209, 2016.

[4] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler. Standardized Protocol Stack for the Internet of (Important) Things. *IEEE Communications Surveys Tutorials*, 15(3):1389–1406, Third 2013.

[5] S. Raza, L. Wallgren, and T. Voigt. Svelte: Real-time intrusion detection in the internet of things. *Ad Hoc Networks*, 11(8):2661 – 2674, 2013.

[6] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson. A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs). RFC 7416 (Informational), Jan. 2015.