HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes

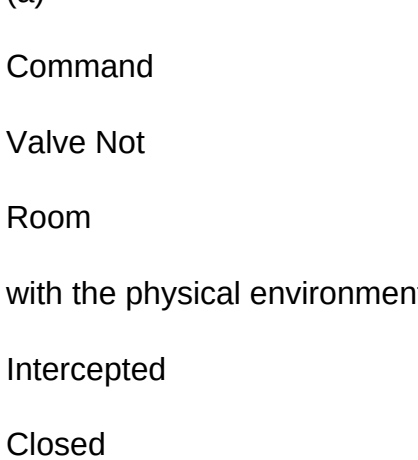
Chenglong Fu
Temple University
chenglong.fu@temple.edu

Qiang Zeng
University of South Carolina
zeng1@cse.sc.edu

Xiaojiang Du
Temple University
xjdu@temple.edu

Abstract

As IoT devices are integrated via automation and coupled with the physical environment, anomalies in an appified smart home, whether due to attacks or device malfunctions, may lead to severe consequences. Prior works that utilize data mining techniques to detect anomalies suffer from high false alarm rates and missing many real anomalies. Our observa-



Broken

Heater

Fire

Relay

Overheating

Hazard

tion is that data mining-based approaches miss a large chunk of information about automation programs (also called smart apps) and devices. We propose Home Automation Watcher (HAWatcher), a semantics-aware anomaly detection system

(c)

Spurious

Presence

Unlock

for appified smart homes. HAWatcher models a smart home's

Presence On

Unlock App

Front Door

normal behaviors based on both event logs and semantics. Given a home, HAWatcher generates hypothetical correla-

Figure 1: Examples of anomalies in a smart home.

tions according to semantic information, such as apps, device types, relations and installation locations, and verifies them

Despite advances in appified smart home, there are grow-

with event logs. The mined correlations are refined using

ing concerns about its safety and security [41]. First, IoT de-

correlations extracted from the installed smart apps. The
vices make it possible for cyber-space attacks to be extended
refined correlations are used by a Shadow Execution engine
to the physical world. As shown in Figure 1(a), the command
to simulate the smart home's normal behaviors. During run-
of "close the valve" is maliciously intercepted, which may
time, inconsistencies between devices' real-world states and
cause room flooding. Second, very often a device malfunc-
simulated states are reported as anomalies. We evaluate our
tion is hardly noticeable until certain consequences arise. As
prototype on the SmartThings platform in four real-world
shown in Figure 1(b), an electronic heater controlled by a
testbeds and test it against totally 62 different anomaly cases.
smart app "It's too cold" [15] could result in fires because of a
The results show that HAWatcher achieves high accuracy,
broken relay (an electronically operated switch), which pre-
significantly outperforming prior approaches.
vents the plug from shutting the power for the heater. Third,
as IoT devices are chained together via automation [28,29,39],
abnormal behaviors of one device might trigger undesired

1 Introduction

actions of another, which further exaggerates the impact of
anomalies. As shown in Figure 1(c), a smart lock that auto-
With the rapid growth of Internet of Things (IoT), smart
matically unlocks upon the resident's presence is unlocked
homes gain booming popularity. As predicted by Gartner,

due to a fake event of the presence sensor.

there will be more than 500 IoT devices deployed in a typical

To address these concerns, many anomaly detection sys-

household by 2022 [72]. IoT devices become increasingly in-

tems [30,35,54,56,60,68,76] utilize data mining techniques to

tegrated, thanks to IoT platforms such as $martThings [21],

profile the system's normal behaviors and report events that

Homekit [47], and OpenHAB [55]. These platforms provide

deviate from profiles as anomalies. However, these works

interoperability among home IoT devices by different ven-

usually take event logs as inputs without fully considering

dors, and allow them to work according to user-specified

each event's semantics, which actually may be acquired from

automation programs (also called smart apps).

smart apps, device types, and device functionalities. The lim-