Table 8: The number of false alarms caused by smart app changes.

Original Rule

Type

Rule after change

HAWatcher

OCSVM

ARM

R3

Action change

If MS1(active), then L2(on) and L1(on)

0

14

0

R5

New rule

If MS2(active) B2(click), then L3(on) L3(toggle)

0

10

0

R8

Condition change

If MS3(inactive) for 5 15 minutes, then L4(off)

0

30

67

R10

Condition change

If MS4(inactive) for 15 30 minutes, then L5(off)

0

17

75

R14

Trigger change

If A(CO2 > 950 1000), then P2(on) for 15 minutes

0

17

0

8

Limitations and Future Work

9 Conclusion

While the evaluation results are very promising, we consider

In an appified smart home, there exists rich semantic infor-

this work a first step towards semantics-aware anomaly de-

mation, such as smart apps, configurations, device types, and

tection in appified smart homes. HAWatcher has some limi-

installation locations. It is a promising direction to combine

tations that we plan to address.

such semantic information with mining for anomaly detec-

tion. We presented a viable and effective approach in this

User Activity Deviations. Correlations due to the user ac-

direction: it exploits semantics on different channels (smart-

tivity channel are useful for detecting anomalies, but they

can cause false alarms when there are user-activity devia-

app, physical, and user-activity) to propose explainable hy-

tions. We already find such cases during our evaluation (see

pothetical correlations, which are tested using event logs and

False Alarm Rate in Section 6.4), although they occur rarely.

refined by smart apps. We built a prototype HAWatcher and

Some alarms help remind users of unusual situations (e.g.,

evaluated it on four real-world testbeds against various (to-

the front door is left open), while others may be annoying.

tally 62) anomaly cases, demonstrating its high accuracy and

For example, one day a resident wants to read a book in her

low false alarm rate. We view this work as a first step, rather

than the final solution, in the direction of semantics-aware

bedroom and turns on extra lights, which causes illuminance

high. If this never or rarely occurs during training, it can

anomaly detection for appified smart homes.

cause a false alarm. One potential solution is to ask for users'

Acknowledgement

feedback when raising alarms, and deactivate or re-test cor-

relations that have caused negative feedback. Generally, how

We thank the reviewers for their invaluable suggestions. This

to continuously update correlations to adapt to changes of

work was supported in part by the US National Science Foun-

IoT devices and user activities is an important problem.

dation (NSF) under grants CNS-1828363, CNS-1564128, CNS-

1824440, CNS-2016589, CNS-1856380 and CNS-2016415.

Long-term Correlations. HAWatcher can only mine correlations whose anterior and posterior events arise within short intervals. Long-interval correlations, such as the relation between turning on AC and temperature events, cannot be mined yet. We can annotate the corresponding cells in the adjacency table with long intervals and use the information during hypothesis testing.

Attackers with More Knowledge. An attacker who knows the correlations may construct attacks that do not violate any correlations in order to evade detection. The bottom line of running HAWatcher is that it imposes extra constraints on attackers. In Testbe 1, each attribute is involved in at least four (4) correlations and has an average of 10.5 correlations (Section 6.2). It is a barrier to attack an device without violating

References

[1] Smartapp execution scheduling. https://docs.smartthings.com/en/latest/ref-docs/smartapp-ref.html#smartapp-run-in.

[2] Lights follows me, 2015. https://github.com/SmartThingsCommunity/SmartThingsPublic/tree/master/smartapps/smartthings/light-follows-me.src.

[3] Door knocker going crazy, 2016. https://community.smartthings.com/t/door-knocker-going-crazy/55570.

[4] Tons of issues with smartthings, 2016.

https:

any of the correlations. For example, given the correlation

www.reddit.com/r/SmartThings/comments/

unlocked

ck(frontdoor) Spresence (i.e., the front door unlock event

4463eo/anyone_else_having_tons_of_issues_with_

can only arise when the presence sensor is on), if an attacker

smartthings/.

has compromised the door lock, an alarm will be triggered if

the attacker unlocks the door when nobody is home.

[5] When st glitches become major safety fire haz-

ard, 2016. https://community.smartthings.com/t/

Sparsely Deployed IoT Devices. Some IoT devices might

when-st-glitches-become-major-safety-fire-hazard/

be sparsely deployed, and physical-channel correlations

43109.

among them might be very few. A promising solution is

to explore the correlations in the entire home, rather than

[6] Are

the

poltergeists

back?,

2017.

in separate rooms, which can hopefully derive more correla-

https://community.smartthings.com/t/october-

tions among devices. Moreover, it is a trend that IoT devices

2017-are-the-poltergeists-back-devices-randomly-

are deployed with increasing density.

turning-on/101402.