the benefit brought by the combination of the two, we build
missed instances should not impose hazards, as the events
two variants of HAWatcher: HAWatcher (Apps Only), which
are consistent with the fact that the residents are active dur-
extracts correlations from smart apps only, and HAWatcher
ing the time. Similarly, the 26 missed instances of Case 10
(Mining Only), which mines correlations without using apps.
are illuminance readings which have similar values with real
Detection Results of HAWatcher. As shown in Table 7,
readings at the time. For Case 9, two instances are missed
HAWatcher has an average detection precision of 97.83% and
because two residents are back home together when one of
a recall of 94.12% across the 24 diverse anomaly cases. For
their presence sensors' events get intercepted. In this situa-
18 out of 24 cases, HAWatcher successfully detects all the
tion, smart app R17 will be triggered without difference by
instances. Below we describe some examples to illustrate
the other presence sensor and no hazard is caused.
how HAWatcher detects anomalies.
Comparison. (1) As shown in Figure 8, HAWatcher achieves
Detecting Case 7. Residents entering/leaving the bedroom
the best performance across all the 24 cases. (2) HAWatcher
open the door, which is installed with an acceleration sen-
(Apps Only) merely obtains e2e correlations from smart apps,
sor C3, and cause the motion-active event of MS3. How-
and can only detect anomalies, such as Command Failures

ever, as motion-active events of MS3 are intercepted/lost,

(cyber)/Command Interceptions. It gets 16.67% for both the

the user activity e2e correlation C17 = acceleration(C3) active

average precision and recall. (3) HAWatcher (Mining Only)

motion(MS3)

Factive

> is violated and the anomaly is hence detected.

has the second best performance. On average, its precision

is 88.42% and recall 88.62%, showing the effectiveness and

Detecting Case 11. Ghost/Fake Commands that try to turn

importance of our mining approach. However, due to the

on P2 are detected due to a violation of the correlation

C30 = (Eon .switch(P2) SCO2(A) which is derived from the

lack of knowledge of smart apps, it misses many instances

of Cases 2, 11, 12, and 20. (4) The ARM-based detector has

smart app rule R14 and accepted by the hypothesis testing.

an average precision 2.03% and recall 7.79%. It fails to detect

The threshold 950 is easily extracted via semantic analysis

any anomaly instances for 17 of the 24 cases, as its rules

of apps, but it would be difficult, if not impossible, for pure

cover very few attributes (Section 6.2). (5) OCSVM performs

mining based approaches to learn it.

slightly better with precision 17.15% and recall 45.19%. It fails

Detecting Case 14. A stealthy command in Case 14 tries

for Cases 4, 9, 10, and 18, as events related to these cases do

to turn on the plug P2 to start the connected fan, which the

power(P2)

not fall inside the same input vector.

causes

event

However, Since the feedback

False Alarm Rate. We measure the false alarm rate of

.switch(P2)

event

Eon

is intercepted by attackers, the switch of P2

HAWatcher using the testing event logs (collected during the

is

still

at

the

state

switch(P2) Thus, the physical channel e2s

fourth week). We consider any alarms that are not due to our

correlation

Smitch(P2), is violated.

anomaly injection and cannot be categorized as any of the

Detecting Case 20. Command Failures (cyber)/Command

anomaly types listed in Section 3 as false alarms. HAWatcher

Interceptions are detected because of violation of the smart

reports totally 13 anomalies other than those injected by app channel e2e correlation C38 = motion(M2) \Smode home

us. Among them, six (6) are due to violations of correla-

tions C12, C13, C29, and C15, because of the large delays of

.switch(P4)

Eon

the commands are intercepted or not processed

some events from the illuminance sensors; three (3) are due

switch(P4

by the cyber part, so there are no feedback events Eon

to violations of correlations C20 and C21, because of the

In contrast, HAWatcher (Mining Only) cannot learn this cor-

large delays of some events from the acceleration sensors.

relation and thus misses all instances of this case.

Such anomalies are categorized as true positives due to Event

Detecting Case 21. L1 accepts the turning-on command

Losses or Large Delays (Section 3.1). They should be reported

and sends the feedback event, but due to a physical-part

to users, as the large delay may confuse users and even cause

failure or DoE, the light is not on. While most of the instances

undesired automation (e.g., an unlock-door command arrives

of Case 21 can be detected as violation of the correlation

late after the user has locked the door).

C24 = illuminance(MS1) switch(L1) (since the illuminance

The other four (4) are due to user behavioral deviations:

keeps low but the light-switch state is on), 3 instances are

two are due to violation of C4 and C5, because there is one missed, because the room has been brightened up by natural

time that the residents stayed outside the door for a while

light (hence, illuminance has already been high) when the

(longer than 60 seconds) before opening the front door; C11

anomaly arises.

and C18 each cause one false alarm, and the reason is that

For Cases 1, 3, 6, 9, and 10, some instances are missed,

the residents left the front door open for quite a while and

which should be attributed to imperfection of anomaly sim-

then closed it. While it is arguable whether anomalies due

ulation (rather than the inability of HAWatcher). For exam-

to user behavioral deviations should be categorized as false

ple, seven instances of Case 1 are missed, because the fake

alarms, we consider them false alarms, as they are not due

motion-active events of MS1 happen to be injected during

to attacks or device malfunctions.

the time when there are real events of active ,motion(MS1) ; such

In total, HAWatcher reports four (4) false alarms from 9,756