SHATTER: Control and Defense-Aware Attack Analytics for Activity-Driven Smart Home Systems

Nur Imtiazul Haque*, Maurice Ngouen*, Mohammad Ashiqur Rahman*, Selcuk Uluagac†, and Laurent Njilla‡
*Analytics for Cyber Defense (ACyD) Lab, Florida International University, USA
†Cyber-Physical Systems Laboratory (CPSLab), Florida International University, USA
‡US Air Force Research Laboratory (AFRL), USA
*{nhaqu004, mngou002, marahman}@fiu.edu, †suluagac@fiu.edu, ‡laurent.njilla@us.af.mil

***Abstract*—Modern smart home control systems utilize real-time occupancy and activity monitoring to ensure control efficiency, occupants' comfort, and optimal energy consumption. Moreover, adopting machine learning-based anomaly detection models (ADMs) enhances security and reliability. However, sufficient system knowledge allows adversaries/attackers to alter sensor measurements through stealthy false data injection (FDI) attacks. Although ADMs limit attack scopes, the availability of information like occupants' location, conducted activities, and alteration capability of smart appliances increase the attack surface. Therefore, performing an attack space analysis of modern home control systems is crucial to design robust defense solutions. However, state-of-the-art analyzers do not consider contemporary control and defense solutions and generate trivial attack vectors. To address this, we propose a control and defense-aware novel attack analysis framework for a modern smart home control system, efficiently extracting ADM rules. We verify and validate our framework using a state-of-the-art dataset and a prototype testbed.**

***Index Terms*—Cyberattacks; smart home; HVAC control system; formal modeling; machine learning; threat analysis.**

I. Introduction

Contemporary home control systems use enormous remotely accessible and controllable internet-connected smart devices to ensure energy efficiency and occupantś comfort. The adoption of smart devices is increasingly growing due to their affordability, accuracy, interoperability, productivity, cost reduction, and so on. Smart home control systems are currently assisted with voice-controlled smart devices (e.g., turning on the bedroom light through a smartphone voice assistant) or self-learned automated closed-loop controllers (e.g., smart cooling controller self-adjusted based on the homeowners' schedule). The prevalence of occupancy sensors and tracking devices (e.g., through smartwatches or RFID sensors) accounts for improved accuracy and efficiency of the control systems through real-time occupants' location and activity identification.

Unfortunately, the widespread use of the internet of things (IoT) network in smart devices has left smart home control systems highly susceptible to multiple cyberattacks. Such devices possess restricted security capabilities, leaving them vulnerable to constantly evolving and sophisticated attacks due to their open network communication. Hence, millions of IoT devices are currently functioning without adequate security protection [1]. Since smart homes/buildings are susceptible to several well-known attacks such as ransomware, distributed denial of service (DDoS), and data manipulation, it is crucial to investigate the vulnerability of the heating, ventilation, and air conditioning (HVAC) system, which is a critical component of a home. Our security analysis considers false data injection (FDI) attacks on demand-controlled HVAC (DCHVAC) systems. We consider a sophisticated attacker having malicious intent to maximize the overall energy consumption. The attack motivation could be sabotage/rivalry/personal vendetta that projects financial loss to the home dwellers. While FDI attacks on smart homes are considered to be in the conceptual phase, instances of such attacks have been reported, as demonstrated by an attacker who boasted publicly of increasing a home's temperature by 20° F. [2].

The attack space analysis of a smart home control system is an active research area. In one of our existing works, we analyzed FDI attacks on an American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE)-based DCHVAC system (i.e., optimally mixes return and fresh air to meet energy efficiency and occupant's comfort) in the smart building context [3]. A limited set of verification rules like maximum capacity of the zones, IAQ measurement consistencies, occupants count consistencies throughout the zones with the entrance count, etc., were considered in BIoTA for assessing the attack space of the home/ building control system. However, most modern smart home/building control systems are quite different than the assumption made in the existing works. Modern smart home control systems often use machine learning (ML)-based anomaly detection model (ADM) for identifying measurement inconsistencies, smart appliances control through voice assistants (through dedicated and other IoT device controllers), and occupants' activity monitoring tool. The ML-based ADM has already been adopted in industrial automation. e.g., BuildingIQ offers an intelligent energy management system that includes occupancy sensors and can adjust HVAC settings based on occupancy and building usage patterns [4]. Although not implemented in the industrial application, the activity recognition-based DCHVAC system has also been adopted in research facilities like KTH Live-In Lab, CASAS, ARAS testbeds [5], [6], [7]. Hence, existing regulation-based approaches [8], [9], [10], formal security analyses [11], [12], ML-based approaches [13], and ML-model verification [14], [15], [16] tools are inapplicable

in such ADM-based smart home contexts since the ADMs learn the pattern of occupants' behavior, which makes the attacks considered in the existing works unstealthy. We propose **S**mart **H**ome **A**nalytics for **T**hreats **T**argeting **E**nergy **R**outine (SHATTER) framework that identifies critical threats of smart home control systems with ML-based ADM and activity identification modules. While the ADM limits the attack scope of SHATTER-identified attacks, the appliance-triggering attack utilizing the activity identification module increases the attack impact. Our evaluation shows that ML-based ADM reduces the attack impact by 50% while leveraging the activity identification modules; an attacker can increase the attack impact by 20% as compared to the state-of-the-art (i.e., BIoTA) framework. For formally modeling the ML-based ADM, we use a convex hull algorithm [17], where the constraint acquisition from the ML models is inspired by the SHChecker framework [18]. A satisfiability modulo theories (SMT)-based solver is used to identify optimal attack paths to launch stealthy FDI attacks in the considered smart home control system. We verify our proposed framework with two houses of state-of-the-art dataset naming Activity Recognition with Ambient Sensing (ARAS) [5] and our built prototype testbed. In summary, our contributions are as follows:

- We formally model a smart home HVAC control system with ML-based ADM and activity recognition module using first-order predicate logic by extracting constraints from the component models to analyze the system.
- We develop a threat analysis framework (SHATTER) to identify potential attack vectors in the smart home control system by formally modeling FDI attacks with variable attack attributes.
- We conduct experiments with our formal threat analysis framework on state-of-the-art datasets and a real prototype testbed to identify critical attack vectors and evaluate the tool's scalability in analyzing the attack vectors.

All implementation and evaluation results are reproducible with the source code on GitHub [19]. The rest of the paper is organized as follows: we provide an overview of the considered smart home system and its components in Section II. We provide a formal description of the problem domain and considered the attack model in Section III. In the following section, we present the technical details of the proposed SHATTER framework. We provide case studies to give insights about our proposed framework's working principle and capabilities in Section V. Then, we show the validation of the SHATTER framework with a real prototype testbed. We evaluate SHATTER using state-of-the-art datasets in Section VII. A comprehensive literature review is presented in Section VIII. We conclude the paper in Section IX.

II. Smart Home Control System

We present a comprehensive but simplistic overview of the smart home control system considered in this work considering a DCHVAC system that can supply the optimal air to meet occupants' comfort and energy efficiency. Our considered smart home control system can track/locate the occupants in

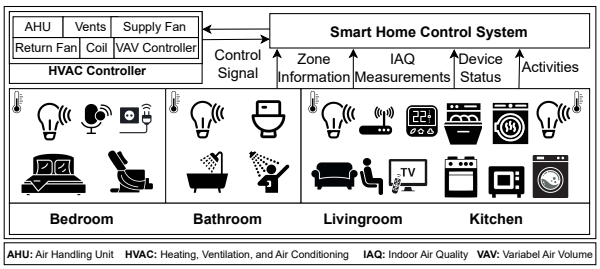


Fig. 1. Smart home system with HVAC controller.

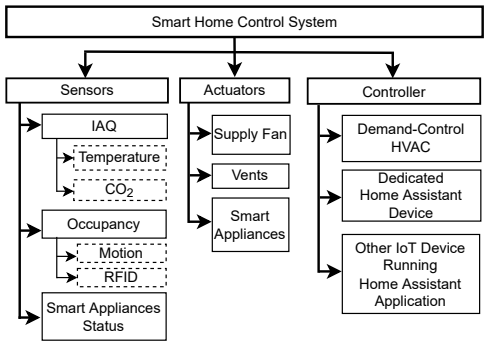


Fig. 2. Components of smart home control systems.

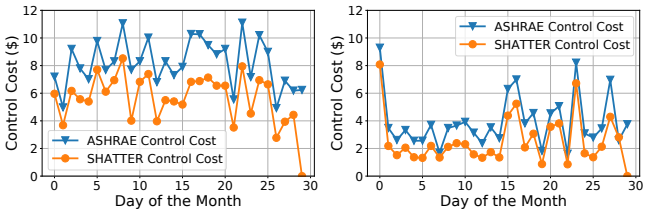


Fig. 3. Comparison between ASHRAE and proposed Control Cost ($) for (a) ARAS House-A (b) ARAS House-B.

different zones and their conducted activities that allow predicting/estimating the IAQ (i.e., temperature and air pollutants) and hence the cooling/heating/ventilation demand. The close approximation of demand enables the calculation of optimal actuation of the control system. Figure 1 shows the architecture of the considered home control system, where the system acquires various IoT-based sensor information to estimate the smart home state (i.e., occupants' location, activity, and appliance status). The HVAC controller, which is the core controller of our considered control system, generates the optimal control signal to actuate the supply fan, return fan, and vents. We consider that all the appliances in the home are smart IoT devices and can be accessed, triggered, or actuated by the dedicated device or application-controlled voice assistants. The status of the smart appliances can be identified by the sensor installed on the appliances or the appliance control applications. Figure 2 shows the hierarchy of the control system's different components.

Although we adopt the DCHVAC controller based on ASHRAE standards, some variations in our considered controller made it more efficient. Figure 3 shows the control cost comparison (the proposed DCHVAC controller is 48.2% efficient for ARAS house-A, while 53.35% efficient for house-B). It is to be noted that the purpose of this work is not

to develop an efficient controller. However, the adoption of a sophisticated controller helps us identify critical attack vectors. The efficiency of the proposed controller is due to the following 3 reasons.

(1) **Activity-Based Actuation** We consider an occupant activity-based DCHVAC controller, unlike the ASHRAE-based control model, which considers an average change in IAQ by the occupants. However, research by Persily et al. [20] shows that the level of physical activities of the occupants impacts the metabolic rate, in turn, the IAQ of the home.

(2) **Activity-Appliance Relationship** The ASHRAE standard considers an average load (i.e., appliances) for the HVAC control system estimated by studying historical data. However, the estimated load is not good for meeting instantaneous demand. For instance, a person studying in the living room does not interact with any appliances and the control system with average load modeling will supply more air, thus will create discomfort for that person. Hence unlike BIoTA, we relate the appliances with conducted activity (i.e., appliance accessing information is used for activity recognition).

(3) **Occupants tracking** Another factor that contributed to developing an efficient controller is that the considered control system is continuously tracking zone-wise occupants through RFID sensors. Persily et al. [20] also identified that the occupant demographics influence the heat and pollutant generation in the zones. For instance, a middle-aged man generates twice as much air pollutants compared to an infant.

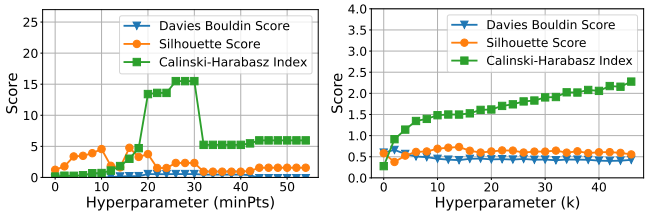
The considered controller integrates an ML-based ADM for detecting sensor measurement inconsistencies, which is detailed in the following section.

III. Problem Definition and Attack Model

This section provides a formal definition of the assumed home control system and a summary of the attack model.

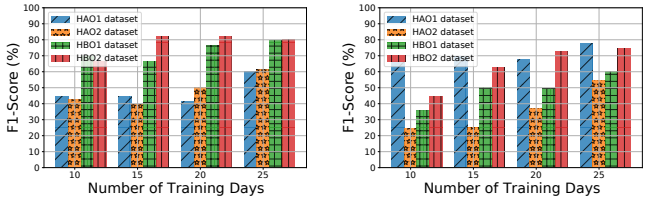
A. Problem Definition

We consider a smart home, $\mathbb{H}$ with smart sensors $\mathcal{S}$ and actuators $\mathcal{A}$, which are triggered by a control system $\mathbb{C}$. Both automated (e.g., HVAC controller) and manual controllers (e.g., smartphone sending voice commands to trigger a microwave in the kitchen) are part of $\mathbb{C}$. Different activities $\mathcal{D}$ of occupants, $\mathcal{O}$ residing in different zones, $\mathcal{Z}$ of $\mathbb{H}$ are constantly monitored through some $\mathcal{S}$ (e.g., RFID, photocell, contact, sonar distance sensors). The use of RFID sensor devices allows tracking the specific occupant/s residing in different $\mathcal{Z}$. The instantaneous activity information of $\mathcal{O}$ at different $\mathcal{Z}$ helps build a more energy-efficient HVAC controller (i.e., a component of $\mathcal{C}$) since different human activity correlates to different metabolic rates that directly control the IAQ of the zones. Other than the HVAC controller, our problem scope considers a smart home automation controller, which triggers smart devices (e.g., smart lights, smart kitchen utensils) throughout different $\mathcal{Z}$



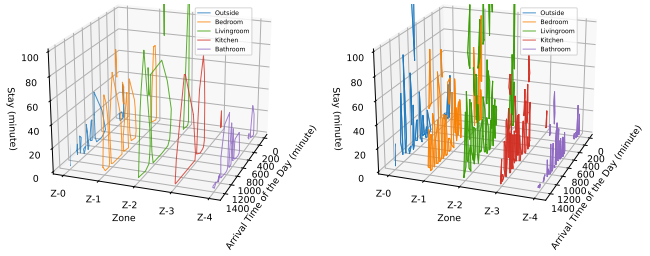
(a) (b)

Fig. 4. Hyperparameter tuning of (a) DBSCAN and (b) K-Means clustering-based ADM for ARAS HAO1 dataset.



(a) (b)

Fig. 5. Progressive incremental performance visualization for (a) DBSCAN and (b) K-Means clustering-based ADM based on F1-score.



(a) (b)

Fig. 6. Cluster visualizations of (a) DBSCAN-based ADM and (b) K-Means clustering-based for ARAS HAO1 dataset.

using dedicated home assistant devices (e.g., Amazon Alexa) or other IoT device (e.g., smartphone) controller applications.

An ML-based (combined with some verification rule) ADM $\mathbb{E}$ checks the measurement consistencies at different timestamps. However, with the knowledge of $\mathcal{C}$ and $\mathbb{E}$, an attacker can still launch a stealthy FDI attack through intelligently crafting different $\mathcal{S}$. Suppose, there is only one occupant in $\mathbb{H}$, and he/she is staying in the bedroom zone. The occupant doing some chores will be alarmed if the washer or dryer is turned on through adversarial attempts, although unwanted turning on of the oven or microwave in the kitchen zone will be unnoticeable to the occupant. However, if the occupant is sleeping deeply and the bedroom door is closed, she will most likely be unaware of the adversarial activation of the washer or dryer. Hence, we consider an occupant activity model that learns the temporal behavioral and activity patterns. For example, if the occupant enters the bathroom at 2.00 pm, he/she is taking a shower for 20 minutes to 30 minutes, or if the occupant goes into the bedroom zone at 10 pm, he/she sleeps for 6 to 8 hours.

Anomaly Detection Model (ADM) We consider ARAS datasets for evaluating our work, which captures every minute data of 27 different occupant activities from 4 zones of 2 homes (2 occupants each) over a month period [5]. The

dataset is used to train two different clustering-based ADMs-DBSCAN and K-Means clustering [21], [22]. For training the ADMs, we consider four datasets, which we name HAO1 (i.e., a dataset containing information about one occupant of house A), HAO2, HBO1, and HBO2 datasets, and use the names throughout the write-up. The hyperparameter of the ADMs are optimized using Davies-Bouldin Index (DBI), Silhouette Coefficient (SC), and Calinski-Harabasz Index (CHI) since the ground truth of the clusters are not known [23]. The higher values of SC and CHI and the lower value of DBI yield better performance. Figure 4 shows the performance of the ADMs based on different hyperparameters for HAO1. The optimal DBSCAN hyperparameter minPts (i.e., the minimum number of points for cluster forming) is found to be 30, where the optimal K-means clustering hyperparameter k (number of clusters) is 29. The other hyperparameter for DBSCAN (i.e., maximum distance in between within cluster samples) is considered to be 3 (i.e., the minimum number of points to create a convex hull). Since the datasets lack adequate samples, the ADMs' performance is not significant. However, the progressive learning capability for both ADMs (i.e., linearized with convex hull) shown in Figure 5 suggests that after learning a few more days/months of data, the ADM will fully learn the occupants' behavioral patterns. To evaluate the performance of the ADMs, we generated attack samples using the BIoTA framework [3]. We use the F1-score (i.e., the harmonic mean of precision and recall) for the performance evaluation since the datasets are imbalanced datasets. The HAO1 dataset has 12.4%, 12.1%, 13.6%, and 14.3% attack data compared to the benign data for 10, 15, 20, and 25 days of training samples(out of 30 days), respectively. For the HAO2 dataset, the ratios are 3.6%, 3.61%, 3.73%, and 3.71%, respectively. Similarly, for HBO1 and HBO2 datasets, the ratios are around 7%. The ADM clusters visualized in Figure 6 show that the clusters from K-means clustering cover a larger area than DBSCAN clustering. The main reason is that the K-means clustering algorithm clusters every sample in training sets into benign samples (i.e., no benign or outlier samples). Here we mainly discuss the choice of ADMs and their hyperparameters. The performance of ADMs is evaluated, reasoned, and discussed more through the SHATTER framework in section VII.

B. Attack Model

The attack model is used to generate parameterized attack procedures and functions that target a specific cyber-physical system (CPS), in our case, a smart home. In this section, we provide a summarized version of the attack model, which is detailed and formally analyzed in Section IV.

1) Attack Assumptions: The proposed framework considers a set of assumptions.

(a) **Assumption I:** Attacker has complete knowledge of the zone properties, smart home control algorithm, and ADM. Moreover, the parameters considered in the zone, appliance, and activity modeling are known to the attacker.

(b) **Assumption II:** We assume each zone of our considered smart home accommodates only single measurements for measuring the IAQ.

(c) **Assumption III:** We consider the attacker having access to sensor measurement (IAQ, occupancy, and appliances' status) can read and alter the measurement, while access to an appliance indicates the feasibility of activation of an unacitvated appliance.

(d) **Assumption IV:** All actuation devices cannot be altered or activated similar to smart appliances. For instance, cooling/heating fans and vents are out of the attack scope.

(e) **Assumption V:** The controller and communication between the controller to the actuator is out of attack scope. Since the controllers are high computation devices they are hard and expensive parts to be compromised. Furthermore, the HVAC controllers and actuators are physically connected through a wired medium, which makes them sturdy against attackers' manipulation [24].

2) Attack technique: In our formal threat analysis framework, we are considering FDI or measurement manipulation attacks. Altering the sensor measurements, an attacker can lead the $\mathbb{E}$ to make an erroneous system state, thus making the $\mathbb{C}$ send an improper control signal, resulting in actuating the $\mathcal{A}$ differently than required. The measurement alternations are considered to be performed intelligently to evade the $\mathbb{E}$. The proposed framework finds out only those attack vectors (each contains the false values to be injected in different sensor measurements) that are attainable with the attacker's capability. It is to be noted that inaudible voice commands are also considered FDI in the attack model and are part of the attack vector. The $\mathbb{H}$ can be attacked with FDI attacks in different ways. For instance, an attacker can leverage physical interaction features on IoT devices to conduct a stealthy attack against IoT systems. The attacks are primarily launched using an app or environment where an attacker seeks to exploit aphysical channels [25]. The SHATTER-considered attacks can be broadly classified into two categories- sensor measurement acquisition and alteration as detailed followingly.

Measurement acquisition through physical sensing The occupants' location (i.e., within $\mathcal{Z}$) can be sniffed by RF signals as depicted in [26]. The Access point, along with the $\mathcal{S}$ emits RF that constantly reflects on the occupant's body and, therefore, sends out the information about the occupant's location in the building. Here, the adversary uses commodity and low-cost sniffers to conduct a covert reconnaissance attack that can continually monitor and pinpoint human activity within a particular location in a home or an office without having any physical or remote access to the WiFi devices.

Measurement acquisition through eavesdropping communication packets In an IoT network, nodes generally send, forward, or collect packets along with evaluating the routing consistency of each path [27]. The attacker's access to the router can act as a man-in-the-middle and sniff the communication packets through packet capture and analysis tools.

Measurement alteration through packet crafting Through man-in-the-middle attack, the attacker can not only eavesdrop

on packets but also alter/craft packet information utilizing ARP poisoning and IP/MAC addressing spoofing attack. The goal is to alter the measurement information sent by specific sensors. Through this approach, the attacker can modify all the sensor measurements and appliances' statuses. Such alterations are hardly detected by the control system.

Activation of Appliances through inaudible voice commands Smart IoT devices require charging whenever the battery becomes low in other to function appropriately. A recent attack has shown the feasibility of sending inaudible voice commands from smartphones through malicious charging plugs [28]. To perform this attack, the occupant must charge their device. Moreover, inaudible voice commands can be transmitted through other approaches as identified by the existing works – Backdoor [29], DolphinAttack [30], LipRead [31], SurfingAttack [32], etc. These attacks allow an adversary to send inaudible voice commands to the voice assistants and stealthily activate the appliances.

3) Attack Goal: The SHATTER framework's primary goal is to increase the energy consumption of the home through stealthy FDI attacks. The attack demands alteration of the necessary sensor measurements to maximize the overall energy consumption in $\mathcal{H}$ by forcing $\mathcal{C}$ to flow more air (i.e., both fresh and return air) through the supply air duct in different $\mathcal{Z}$. To launch stealthy attacks, the attacker needs to bypass:

ADM: Inconsistencies in the occupancy or IAQ measurement from the learned occupant's behavioral pattern will be recognized as an anomalous event.

Occupants: Turning on the washer in the kitchen while an occupant is cooking will lose the attack's stealthiness.

4) Attacker's Attributes: For modeling the attack, we consider variable accessibility and resource constraints for the attacker. This work considers a knowledgeable attacker aware of the surrounding weather pattern, smart home zone attributes, occupancy information, underlying control, and defense mechanisms (i.e., ADM) of the smart home control system. It is unreasonable to assume that the attacker has access accessibility to all of the resources (i.e., sensor devices) to initiate a stealthy FDI attack. The attack model specifies access to sensor measurements (i.e., IAQ/occupancy/appliances' status measurement), and access to appliances (i.e., appliances that can be triggered by inaudible voice commands). The major differences between BIoTA and SHATTER frameworks are illustrated in Table I.

TABLE I
PRIMARY DIFFERENCES BETWEEN BIOTA AND SHATTER FRAMEWORK.

Criteria	BIoTA	SHATTER
Application Domain	Smart building/ homes	Smart homes
Number of Occupants	∼(10-1000)	∼(1-10)
Anomaly Detection Model	Rule-based	ML-based
Occupant's Activity Tracking	Not considered	Considered
Appliance Modeling	Fixed load at every control cycle	Dynamic load modeling
Attack Constraints	Stealthy bypass control system	Deceive both control system and occupants
Attack Technique	Greedy FDI attack	Dynamic FDI attack

IV. TECHNICAL DETAILS OF THE SHATTER FRAMEWORK

In this section, we provide a detailed overview of the SHATTER framework. SHATTER formally models the smart home control systems, ADM, and the attack model using the Z3 tool that leverages SMT [33]-based solver and optimizer to identify stealthy attack vectors that can optimally increase the energy consumption of the home. Table II demonstrates the modeling notations.

A. Formal Modeling of the smart home control system

For the HVAC control system, we mainly consider temperature, occupancy, and CO_2 concentration as measurement values. Because building occupants are the primary source of continuous heat and CO_2 generation, accurately measuring the number of people in real-time utilizing different building sensor systems is critical for computing energy efficiency and occupant comfort.

Ventilation Control Constraints: The HVAC control system adds optimal fresh outside air to the supply air for maintaining the CO_2 concentration in occupants' comfort range. The ventilation requirement depends on CO_2 emitted by the occupants, which varies based on the metabolic rate (depending on the occupants' age and levels of conducted physical activities).

$$\forall_{t\in\mathcal{T}}\forall_{z\in\mathcal{Z}} \quad \frac{\mathcal{S}^{OE}_{t,z}\times\mathbb{P}^{CE}_{o,z,a=\mathcal{A}_{t,o,z}}\times\Delta t}{\mathbb{P}^{V}_{z}} = \mathbb{P}^{CS}_{t,z} - \left(1-\frac{\mathcal{Q}_{t,z}}{\mathbb{P}^{V}_{z}}\right)\times\mathcal{S}^{C}_{t,z} - \frac{\mathcal{Q}_{t,z}\times\Delta t}{\mathbb{P}^{V}_{z}}\times\mathbb{P}^{OC}_{t} \tag{1}$$

Temperature Control Constraints: The HVAC control system optimizes the usage of zone return air to the supply air for quickly meeting the zones' setpoint temperature and minimizing the home's energy consumption. The cooling demand is dependent on the appliances' heat radiation and the occupants' metabolic rate. In this work, we consider the load demand based on the appliances' status, unlike the control rules of BIoTA (constant load demand). The factor 0.3167 in Equation 2 is used since it does not vary significantly with the parameters change. We multiply a factor ($\mathbb{P}^{HRF}_{d}$) with total energy consumption for all devices to calculate sensible heat gain (e.g., LED lights radiate 12% heat [34]).

$$\forall_{t\in\mathcal{T}}\forall_{z\in\mathcal{Z}}\forall_{d\in\mathcal{D}} \quad \mathcal{Q}_{t,z}\times(\mathbb{P}^{TS}_{z,t}-\mathbb{P}^{TSP}_{z,t})\times 0.3167 = \mathcal{S}^{OE}_{t,z}\times\mathbb{P}^{HR}_{o,z,a=\mathcal{A}_{t,o,z}} + \mathcal{S}^{D}_{t,z,d}\times\mathbb{P}^{PC}_{d}\times\mathbb{P}^{HRF}_{d} \tag{2}$$

Equations 1 and 2 constraint the airflow requirement in the zones and account for optimal estimation of airflow to satisfy both occupant's comfort and energy savings needs.

HVAC Control Cost Calculation: The HVAC cost calculation mainly depends on the air quality in the mixed air chamber. The air handling unit (AHU) optimally mixes the fresh and return air to meet the zone's IAQ demand. The air mixing chamber of the HVAC controller mixes both outside

TABLE II
MODELING NOTATIONS

Type of Notation	Notation	Description	Data Type
General	$\mathcal{Z}$	Set of all zones	Set
	$\mathcal{O}$	Set of all occupants in a multi-occupant setup	Set
	$\mathcal{D}$	Set of all appliances	Set
	$\mathcal{T}$	Set of all timeslots in a day at each sampling time	Set
	$\mathcal{A}$	Set of all activities	Set
	$\mathcal{D}_{z,d}$	d-th appliance at zone, z	Integer
	$\mathcal{A}_{t,o,z}$	Activity conducted by o-th occupant at t-th timeslot in z-th zone	Integer
	Δt	Sampling time of the controller	Integer
Sensor Measurements	$\mathcal{S}$	Set of all sensor measurements	Set
	$\mathcal{S}^{OE}_{t,z}$	Occupancy estimation measurement (occupants count) at t-th timeslot in z-th zone	Integer
	$\mathcal{S}^{OT}_{t,o,z}$	Tracking presence of o-th occupant at t-th timeslot in z-th zone	Boolean
	$\mathcal{S}^{C}_{t,z}$	CO_2 sensor measurement at t-th timeslot in z-th zone	Real
	$\mathcal{S}^{T}_{t,z}$	Temperature ($^\circ$ F) sensor measurement at t-th timeslot in z-th zone	Real
	$\mathcal{S}^{D}_{t,z,d}$	d-th appliance's status (on/off) at t-th timeslot in z-th zone	Boolean
Actuation Measurements	$\mathcal{Q}$	Set of all airflow (cfm) measurements	Set
	$\mathcal{Q}_{t,z}$	Airflow based at t-th timeslot in z-th zone	Real
Variable Parameters	$\mathbb{P}^{OT}_{t}$	Outdoor temperature at timeslot, t	Real
	$\mathbb{P}^{OC}_{t}$	Outdoor CO_2 concentration at t-th timeslot	Real
	$\mathbb{P}^{CS}_{t,z}$	CO_2 setpoint at t-th timeslot in z-th zone	Real
	$\mathbb{P}^{TSP}_{t,z}$	Temperature of supply air at t-th timeslot in z-th zone	Real
	$\mathbb{P}^{TS}_{t,z}$	Temperature setpoint at t-th timeslot in z-th zone	Real
	$\mathbb{P}^{TM}_{t,z}$	Temperature of mixed air at t-th timeslot in z-th zone	Real
	$\mathbb{P}^{TEC}_{t}$	Total energy consumption (kWh) at t-th timeslot	Real
Fixed Parameters	$\mathbb{P}^{CE}_{o,z,a}$	CO_2 emission per person per minute for occupant o at z-th zone performing activity, a	Real
	$\mathbb{P}^{HR}_{o,z,a}$	Heat radiation per person per minute for o-th occupant at z-th zone performing a-th activity	Real
	$\mathbb{P}^{V}_{z}$	Volume (ft^3) of zone, z	Real
	$\mathbb{P}^{PC}_{d}$	Power consumption (Watt) of the d-th appliance if it is turned on	Real
	$\mathbb{P}^{HRF}_{d}$	Heat radiation factor of d-th appliance that nees to be multiplied by power consumption (Watt) to obtain the heat radiation (kWh) from appliance	Real
	$\mathbb{P}^{COP}_{t}$	Off-peak hour energy cost ($/kWh)	Real
	$\mathbb{P}^{CP}_{t}$	Peak hour energy cost ($/kWh)	Real
	$\mathbb{P}^{BS}$	Battery total storage (kWh) that is charged at off peak hours and used at peak hour to reduce peak hour energy cost	Real
Attack Vector	$\delta^{C}_{t,z}$	False measurement to be added in CO_2 sensor measurements in zone, z at timeslot t	Real
	$\delta^{T}_{t,z}$	False measurement to be added in temperature sensor measurementat t-th timeslot in z-th zone	Real
	$\delta^{O}_{t,o,z}$	False measurement to be multiplied with occupancy sensor measurements for o-th occupant at t-th timeslot in z-th zone	Boolean
	$\delta^{D}_{t,z,d}$	False measurement to be multiplied with d-th appliance sensor measurements at t-th timeslot in z-th zone	Boolean
	$\mathcal{I}$	Attack optimization window	Integer

fresh air and recirculating return air optimally to meet energy efficiency and occupants' comfort.

$$\forall_{t\in\mathcal{T}}\mathbb{P}^{TEC}_{t} = \sum_{z\in\mathcal{Z}} \mathcal{Q}_{t,z}\times(\mathbb{P}^{TM}_{z,t}-\mathbb{P}^{TSP}_{z,t})\times 0.3167 \times\frac{\Delta t}{60000}+\sum_{z\in\mathcal{Z},d\in\mathcal{D}}\mathcal{S}^{D}_{t,z,d}\times\mathbb{P}^{PC}_{d} \quad (3)$$

$$\mathcal{G}^{\mathcal{S}} = \sum_{t_1\in\mathcal{T}^{OP}\vee(t_1\in\mathcal{T}^{P}\wedge\sum_{t=\mathcal{T}^{P}_{0}}^{t_1}\mathbb{P}^{TEC}_{t}\leq\mathbb{P}^{BS})} \mathbb{P}^{TEC}_{t_1}\times\mathbb{P}^{COP}_{t_1} + \sum_{(t_2\in\mathcal{T}^{P}\wedge\sum_{t=\mathcal{T}^{P}_{0}}^{t_2}\mathbb{P}^{TEC}_{t_2}>\mathbb{P}^{BS})} \mathbb{P}^{TEC}_{t_2}\times\mathbb{P}^{CP}_{t_2} \quad (4)$$

The instantaneous power consumption considers both HVAC and appliance-induced consumption as shown in Equation 3. We assume that the home has battery storage that is charged at the off-peak hour and discharged at the peak hour to meet its energy demand and thus reduce the household energy cost. The energy pricing is taken from PG&E electricity rate plans [35]. For brevity, we consider that the battery storage is always charged the full during off-peak hours. Hence, during off-peak hours and a portion of peak hours (i.e., until the battery is fully discharged), the residential loads operate at off-peak hour costing as shown in Equation 4.

B. Formal Modeling of the Anomaly Detection Model (ADM)

The SHATTER framework also extracts formal constraints from the ADM to generate stealthy attack vectors. We consider a clustering-based anomaly detection approach in this work, which continuously checks the duration of stay for an occupant in a particular zone based on the arrival time of that occupant. The considered ADM uses a clustering technique to attain the valid pairs of (arrival time and duration of staying). The hypothesis of choosing this approach is that occupants converge to a set of actions (i.e., moving from one zone to another, doing household chores) after habit formation. In the following write-up, we formally model the ADM after providing an intuitive explanation of the ADM using a toy example. We consider that ADM always checks the duration of staying, t_2, at a particular zone, while the occupant has entered the zone at the time, t_1, with a pre-trained model. The pre-trained model comes up with several clusters. If the point (t_1, t_2) is not within any of the clusters, the controller raises the alarm.

Figure 7 shows two clusters ($\mathcal{C}_{o,z,1}$ and ($\mathcal{C}_{o,z,2}$) in a 2D data plane where $\mathcal{C}_{o,z,1}$ consists of seven line segments ($\mathcal{K}_{o,z,1}$, $\mathcal{K}_{o,z,2}$, …, $\mathcal{K}_{o,z,7}$) and $\mathcal{C}_{o,z,2}$ consists of three line segments ($\mathcal{K}_{o,z,8}$, $\mathcal{K}_{o,z,9}$, and $\mathcal{K}_{o,z,10}$). We denote the end points of any line segment ($\mathcal{K}_{o,z,i}$) are ($\mathcal{X}_{o,z,i}, \mathcal{Y}_{o,z,i}$) and ($\mathcal{X}_{o,z,i}, \mathcal{Y}_{o,z,i}$), where $\mathcal{Y}_{o,z,i} \geq \mathcal{Y}_{o,z,i}$.

(a) $leftOfLineSegment(t_1, t_2, \mathcal{K}_{o,z,i})$: This function checks if the point (t_1, t_2) is on the left side of the line segment, $\mathcal{K}_{o,z,i}$.

(b) $withinCluster(t_1, t_2, \mathcal{C}_{o,z,k})$: This function returns $True$ if the data point (t_1, t_2) is within the cluster, $\mathcal{C}_{o,z,k}$. The point is considered to be within a cluster if it is $leftOfLineSegment$ of all the clusters.

A new set of formal modeling notations- $\mathcal{E}^{A}_{t_1,o,z}$, $\mathcal{E}^{E}_{t_1,o,z}$, and $\mathcal{E}^{S}_{t_1,o,z}$ derived from the occupancy sensor measurements for modeling the ADM. As the name suggests, $\mathcal{E}^{A}$ and $\mathcal{E}^{E}$

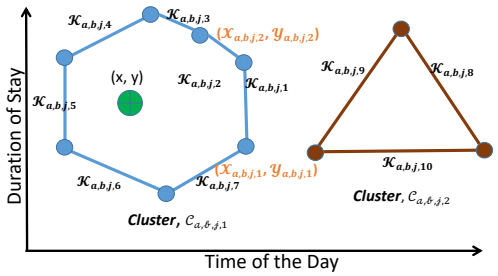


Fig. 7. Sample convex hull representation of the ADM cluster with formal notations.

respectively denote the arrival and exit events of all zones and for all occupants.

$$\forall_{t_1 \in \mathcal{T}} \quad \mathcal{E}^A_{t_1,o,z} \rightarrow \mathcal{S}^{OT}_{t_1,O,z} \wedge \neg \mathcal{S}^{OT}_{t_1-1,O,z} \tag{5}$$

$$\forall_{t_2 \in \mathcal{T}} \quad \mathcal{E}^E_{t_2,o,z} \rightarrow \quad \mathcal{S}^{OT}_{t_2,o,z} \wedge \neg \mathcal{S}^{OT}_{t_2+1,o,z} \tag{6}$$

The stay duration for the occupants at a specific zone can be modeled using the arrival and exit events.

$$\forall_{t_1 \in \mathcal{T}} \quad \mathcal{E}^S_{t_1,o,z} = (t_2 - t_1) \rightarrow \mathcal{E}^A_{t_1,o,z} \wedge \mathcal{E}^E_{t_2 > t_1,o,z} \wedge \forall_{t_1 < t_3 < t_2 \in \mathcal{T}} \mathcal{S}^{OT}_{t_3,o,z} \tag{7}$$

The occupancy sensor measurements are considered to be benign if all the entering and leaving events of the occupants are consistent with the DBSCAN clusters.

$$consistent(\mathcal{S}^{OT}) \rightarrow \forall_{o \in \mathcal{O}} \forall_{z \in \mathcal{Z}} \forall_{t_1 \wedge \mathcal{E}^E_{t_1,o,z}} withinCluster(t_1, t_2 = \mathcal{E}^S_{t_1,o,z}, \mathcal{C}_{z,o}) \tag{8}$$

Here,

$$withinCluster(t_1, t_2, \mathcal{C}_{z,o}) \rightarrow \exists_{c \in \mathcal{C}_{z,o}} \forall_{k \in \mathcal{K}_{z,o} \wedge In(k,c)} \quad leftOfLineSegment(t_1, t_2, k) \tag{9}$$

$$leftOfLineSegment(t_1, t_2 = \mathcal{E}^S_{t_1,o,z}, \mathcal{K}_{z,o,i}) \rightarrow (t_1(\mathcal{Y}_{z,o,i,1} - \mathcal{Y}_{z,o,i,2}) - t_2(\mathcal{X}_{z,o,i,1} - \mathcal{X}_{z,o,i,2}) - (\mathcal{X}_{z,o,i,1}\mathcal{Y}_{z,o,i,2} - \mathcal{X}_{z,o,i,2}\mathcal{Y}_{z,o,i,1})) < 0 \tag{10}$$

The equations 9 and 10 say that the (t_1, t_2) pairs will be considered to be within the valid clusters if at least one cluster encloses the point. The condition of being in a cluster (i.e., convex hull) is that the point is the left-hand side of all that cluster line segments.

C. Formal Modeling of Attacks

The main goal of the attack is to maximize the energy cost by adding false measurements. The following three equations demonstrate the FDI attack in IAQ, occupancy, and appliance measurements, respectively.

(1) $\forall_{t \in \mathcal{T}^A} \forall_{z \in \mathcal{Z}^A} \forall_{p \in [C,T]} \bar{\mathcal{S}}^p_{t,z} = \mathcal{S}^p_{t,z} + \delta^p_{t,z}$
(2) $\forall_{t \in \mathcal{T}^A} \forall_{o \in \mathcal{O}^A} \forall_{z \in \mathcal{Z}^A} \bar{\mathcal{S}}^{OT}_{t,o,z} = \mathcal{S}^{OT}_{t,o,z} \times \delta^{OT}_{t,o,z}$
(3) $\forall_{t \in \mathcal{T}^A} \forall_{z \in \mathcal{Z}^A} \forall_{d \in \mathcal{D}^A} \bar{\mathcal{S}}^D_{t,z,d} = \mathcal{S}^D_{t,z,d} \times \delta^D_{t,z,d}$

Here, δ is the attack vector that denotes the required injection to accomplish the attack goal.

Attack Goal:

$$maximize \; \mathcal{G}^{\bar{\mathcal{S}}} \tag{11}$$

Attack Constraints:

$$consistent(\mathcal{S}^{OT} + \delta^{OT}) \tag{12}$$

$$\sum_{t \in \mathcal{T}^A, o \in \mathcal{O}^A, z \in \mathcal{Z}^A} \bar{\mathcal{S}}^{OT}_{t,o,z} = \sum_{t \in \mathcal{T}^A, o \in \mathcal{O}^A, z \in \mathcal{Z}^A} \mathcal{S}^{Occ}_{t,o,z} \tag{13}$$

$$\forall_{t \in \mathcal{T}^A} \forall_{o \in \mathcal{O}^A} \forall_{z \in \mathcal{Z}^A} \frac{\mathcal{S}^{OE}_{t-1,z} \times \mathbb{P}^{CE}_{o,z,a=\mathcal{A}_{t-1,o,z}} \times \Delta t}{\mathbb{P}^V_z} = \mathcal{S}^C_{t,z} - \left(1 - \frac{\mathcal{Q}_{t-1,z}}{\mathbb{P}^V_z}\right) \times \mathcal{S}^C_{t-1,z} - \frac{\mathcal{Q}_{t-1,z} \times \Delta t}{\mathbb{P}^V_z} \times \mathbb{P}^{OC}_{t-1} \tag{14}$$

$$\forall_{t \in \mathcal{T}^A} \forall_{z \in \mathcal{Z}^A} \forall_{d \in \mathcal{D}^A} \quad \mathcal{Q}_{t-1,z} \times (\mathcal{S}^T_{t,z} - \mathcal{S}^T_{t-1,z}) \times 0.3167 = \mathcal{S}^{OE}_{t,z} \times \mathbb{P}^{HR}_{o,z,a=\mathcal{A}_{t,o,z}} + \mathcal{S}^D_{t,z,d} \times \mathbb{P}^{PC}_d \times \mathbb{P}^{HRF}_d \tag{15}$$

$$\forall_{t \in \mathcal{T}^A} \forall_{z \in \mathcal{Z}^A} \forall_{d \in \mathcal{D}^A} \quad \bar{\mathcal{S}}^D_{t,z,d} = \neg \mathcal{S}^D_{t,z,d} \rightarrow \forall_{o \in \mathcal{O}} stealthy(d, o) \tag{16}$$

These are attack constraints, where Equation 12 demands that altered occupancy measurement should follow the clusters. Equations 14 and 15 are adopted from the BIoTA framework, which requires prediction made in the previous timeslot about sensor measurements and actuation should be consistent with the current timeslot. The constraint in Equation 16 says that inaudible voice command-based appliance activation is possible if the device is present in an unoccupied zone.

Attacker's Property: An attacker may change a sensor measurement if he/she has the accessibility to that particular measurement. The attacker cannot inject false measurements into the inaccessible sensor measurements. The accessibility to zone, time-slots, devices, and occupants (RFID measurement) are modeled using $\mathcal{Z}^A$, $\mathcal{T}^A$, $\mathcal{D}^A$, and $\mathcal{O}^A$ respectively.

Attack Technique: The principal task of the proposed attack is to misinform the controller with tailored occupants' location and activity information. Hence, the attack can be considered as a scheduling problem, where the attacker will compute an optimal schedule of occupants (along with the activities) throughout different zones at different time instances that evade both the ADM and occupants. Eventually, the optimization objective defined in Equation 17 is an NP-hard problem (i.e., complexity $\mathcal{O}(|\mathcal{Z}|^{|\mathcal{T}|})$). Hence, it is not feasible to get the optimal attack vectors in a viable time. SHATTER aims at identifying sub-optimal solutions by optimizing the scheduling problem in a shorter time window ($\mathcal{I}$) and merging the results. We will consider the schedule as an attack schedule throughout the write-up.

(a) **Attack Schedule Generation:** In this process, the attacker pre-computes the attack schedule based on his knowledge of the control system and ADM. The goal of creating the attack schedule is to maximize the energy cost in the time horizon ($\mathcal{I}$), in which the optimization is feasible.

Attack Schedule Goal:

$$\forall_{t \in [1, |\mathcal{T}|, \mathcal{I}]} \quad maximize \sum_{t}^{t+\mathcal{I}} \mathcal{G}^{\bar{\mathcal{S}}}_t \tag{17}$$

However, the following attack constraints must be maintained to create the attack schedule.

$$\forall_{t\in\mathcal{T}^A}\forall_{o\in\mathcal{O}^A}\exists!_{z\in\mathcal{Z}^A} \quad \bar{\mathcal{S}}^{OT}_{t,o,z} \tag{18}$$

$$\forall_{t\in\mathcal{T}^A}\forall_{o\in\mathcal{O}^A}\forall_{z\in\mathcal{Z}^A} \quad \neg\bar{\mathcal{S}}^{OT}_{t,o,z} \rightarrow \bar{\mathcal{E}}^{A}_{t-m,o,z} \wedge m = maxStay(t,o,z) \tag{19}$$

$$\forall_{t\in\mathcal{T}^A}\forall_{o\in\mathcal{O}^A}\forall_{z\in\mathcal{Z}^A} \quad \bar{\mathcal{E}}^{E}_{t,o,z} \rightarrow \exists_{x\in\mathcal{T}} \quad inRangeStay(t,o,z,\bar{\mathcal{E}}^{S}_{t-x,o,z}) \tag{20}$$

Here, two functions are introduced. The maxStay(.) function outcomes the maximum valid stay duration (without alarming ADM) at a zone for an occupant given his/her arrival time. On the other hand, the inRangeStay(.) function checks whether staying at a zone for an occupant given his/her arrival time and stay duration is stealthy or not. The attack schedule can be derived from the attacked occupancy sensor measurements However, the attacker needs to make sure that the occupants are scheduled to a zone in every attack timeslot as shown in Equation 18. The equation 19 requires that the attacker must schedule an occupant to a different zone if keeping the occupant more will alarm the ADM. Other than that the occupant can only be scheduled to a different zone if the stay duration in the current zone based on the arrival time is within an ADM cluster as shown in Equation 20. Otherwise, scheduling the occupant in a different zone will alarm the ADM.

(b) **Real-timeAttack:** The pre-computed attack schedule can evade the ADM. However, to evade the occupants, the real-time measurement manipulation and appliance triggering decision need to be taken in real-time since the real-time occupant behavior will be different than the attack schedule. In real-time there will be two tasks - 1) using the attack schedule to measure manipulation and 2) appliance triggering attack. The former task requires misinforming the controller's IAQ and occupancy information according to the attack schedule. However, the attack can be carried out at a time-instances if the attacker has access to both the actual occupant zone and the zone from the attack schedule. The core idea behind the later task is that the appliances will be triggered based on the activity reported by the attack schedule, if and only if the occupant staying in the current zone has not exceeded the ADM reported minimum amount of time based on his/her arrival time. The algorithm of the appliance triggering process is shown in Algorithm 1, which sets a variable $trig$ to be $True$ when adversarial manipulation is possible. The minStay(.) function used in Algorithm 1outcomes the minimum valid stay duration (without alarming ADM) at a zone for an occupant given his/her arrival time.

Algorithm 1: Appliance Triggering Decision.

```
Function ApplianceTriggeringDecision(R):
    trig ← False;
    arrivalTime ← 0;
    thresh ← 0;
    Z ← set of all zones;
    for t in Range(T) do
        for o in Range(O) do
            zone ← ∃_{z∈Z} S̄t, o, z^OT;
            if Et, o, zone^A then
                thresh ← minStay(t, o, zone);
                arrivalTime ← t;
            end
            if t − arrivalTime ≤ thresh and ¬S^OT_{t,o,zone} then
                trig ← True;
            end
        end
    end
    return trig;
return
```

V. Case Study

In this section, we conduct empirical case studies to illustrate the working principle of the SHATTER framework in the case of identifying stealthy attack vectors and corresponding attack costs. To discuss the studies easily, we denote the two occupants of our considered home system as Alice and Bob and the intruder/attacker as Trudy. The occupancy/activity information of the home occupants is taken from the ARAS (Home A) dataset. The case study will be described using Table III. The actual occupancy information in the table is taken from day 4 (6 PM - 6:09 PM). We consider a greedy attack strategy (i.e., demonstrated in Algorithm 2.) as the baseline to compare the SHATTER-generated dynamic schedule. In the greedy strategy, we consider that the attacker will schedule the occupant to the zone and activity, which is mapped to the highest cost until the maximum possible stay duration at that particular zone and time.

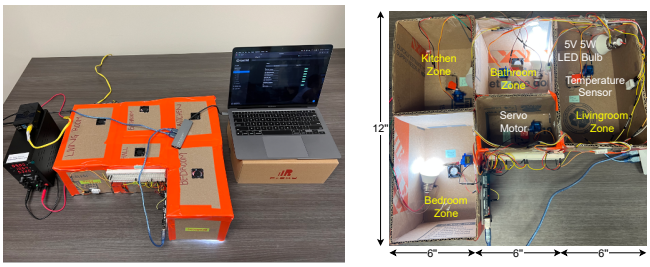
Algorithm 2: Greedy Schedule Generation.

```
Function GreedyScheduleGeneration(R):
    arrivalTime ← 0;
    while arrivalTime < length(T) do
        for o ∈ Range(O) do
            t ← arrivalTime;
            zone ← z | S̄_{t,o,z} ∧ G^S̄ t is maximized;
              duration ← maxStay(t, o, zone);
            for d ∈ Range(duration) do
                S̄t, o, z ← True;
            end
            arrivalTime ← arrivalTime + duration;
        end
    end
return
```

The ARAS zones- Bedroom (Z-1), Livingroom (Z-2), Kitchen (Z-3), and Bathroom (Z-4) incur 0.13¢, 0.135¢, 2.69¢, 0.79¢ respectively for HVAC control of single occupant presence doing the most intensive task in the corresponding zones, while the appliance triggering costs 0.197¢, 0.2096¢, 1.67¢, and 0.83¢ respectively. Hence, the control cost for Alice is 1.6¢, while there is no actual benign control cost since Bob was outside the home in all considered 10 slots. The total

TABLE III
CASE STUDY

Schedule	Occupant	Time	6:00 PM	6:01 PM	6:02 PM	6:03 PM	6:04 PM	6:05 PM	6:06 PM	6:07 PM	6:08 PM	6:09 PM
		Slot (t)	1080	1081	1082	1083	1084	1085	1086	1087	1088	1089
Actual	Alice	2		2	2	2	2	2	2	2	2	2
	Bob	0		0	0	0	0	0	0	0	0	0
Greedy	Alice	2		2	2	2	2	2	2	2	2	2
	Bob	0		0	0	0	0	0	0	0	0	0
SHATTER	Alice	2		2	2	2	2	2	3	3	4	4
	Bob	2		2	2	2	2	2	2	2	2	2
Range Threshold	Alice	[9 - 30]		[10 - 27]	[10 - 25]	[10 - 22]	[11 - 16]	[11 - 19]	[11 - 13]	[]	[75 - 75]	[66 - 75]
	Bob	[5-11]		[9-18]	[5-11]	[9-18]	[16-19]	[9-18]	[25-31]	[8-18]	[9-18]	[1-9]
Trigger Status	Alice	False		False	False	False	False	False	True	True	True	False
	Bob	True		True	True	True	True	False	False	False	False	False



(a) (b)

Fig. 8. (a) Demonstrates a testbed instance, when Alice is showering in the bathroom zone, and Bob is taking nap in the Bedroom zone, where (b) shows the benign control scenario, where bathroom and bedroom zone vents are open and is getting air supply to neutralize the added heat generated from the two occupants, corresponding zone lights and the smart bathtub appliance.

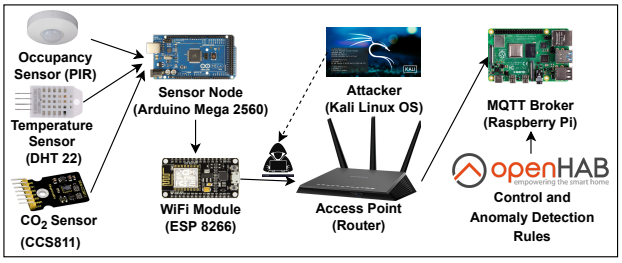


Fig. 9. Prototype testbed architecture.

greedy attack cost for Alice is 1.38¢, while the total SHATTER attack cost for her is 10.93¢(7.47¢for HVAC control and 3.16¢for appliance triggering). Hence, the SHATTER attack cost is 8 times than greedy cost for Alice. Similarly, for Bob total SHATTER attack cost is 1.5¢. The trigger status in Table III is calculated from Algorithm 1. The primary reason behind the greedy scheduling not performing similarly to the SHATTER attack is that at 5.32 PM, the greedy attack schedule chooses the most rewarding zone (i.e., Kitchen). Consequently, to be consistent with the anomaly detection model, the greedy attack schedule needs to choose the outside zone for Bob, which is the same as his current zone. Since the occupant stays at the exact location as the attack schedule as in Table III, Trudy cannot trigger any other devices in the zones to avoid suspicion of the occupants. On the other hand, SHATTER looks for long-term rewards in a specified time horizon. Accordingly, the SHATTER framework outperforms the greedy approach.

VI. TESTBED-BASED VALIDATION

We build a prototype testbed for validating our proposed framework. For testbed implementation, we consider that the attacker has full access to measurements and can access the devices. The occupants and appliances are modeled using 5V, 5W led light bulbs in the testbed. The testbed zones are considered from the ARAS testbed. We scaled down the testbed by the scale (=24) in all dimensions. The energy consumption of the occupants and the appliances are scaled accordingly. Our experimentation shows that the temperature and ventilation of the testbed DCHVAC control modeling are not linear. The primary reason behind this is that the zones in the testbed are not completely insulated. For learning the dynamics of the IAQ in the testbed, we trained a regression model for estimating the airflow and heat generation given the temperature. The temperature of the zones is measured using the DHT-22 sensor. We did not consider pollutant generation for the testbed. The emulation of the different activities is carried out by turning on the led lights for a different amount of time. Similarly, the DCHVAC is mimicked by turning on our 1.4 CFM supply fans for a different amount of time identified by the trained polynomial regression model (degree = 2). Such kind of modeling experienced less than 2% error compared to the testbed measurements. To discuss the studies easily, we denote the two occupants of our considered home system as Alice and Bob and the intruder/attacker as Trudy. Figure 8(b) shows the benign control situation while at the SHATTER-identified attack scenario. However, in the attacked scenario, the control system gets misinformed that Alice and Bob are cooking without getting alarmed (i.e., ADM is bypassed), so chill air is supplied in the kitchen zone. Eventually, the kitchen zone got more chilled compared to the setpoint letting temperature increment in the occupied zones and energy cost increment. We conducted experimentation by taking 1-hour measurements from the ARAS dataset (house-A). Figure 9 shows our prototype architecture. We used openHAB as our supervisory control and data acquisition (SCADA) system and attacked the raspberry pi-based MQTT broker to imitate the attack and measure the attack impact. Finally, we found a 78% increment in energy consumption after the experimentation. Our attack approach here aims at real-time modification of MQTT protocol network messages. To carry out the attack, we employ the Polymorph and the Scapy frameworks. The considered attack is feasible to be launched primarily with a $35 Raspberry Pi 2 device, which can play the role of a sniffer, MQTT broker, and also packet crafter [36], [26].

TABLE IV
COMPARISON OF ADMS BASED ON THE ATTACKER'S KNOWLEDGE.

ADM	Attacker's Knowledge	Dataset	Accuracy	Precision	Recall	F1-Score
DBSCAN	All Data	HAO1	0.75	0.83	0.63	0.71
		HAO2	0.83	0.75	1.0	0.85
		HAO1	0.73	0.71	0.76	0.73
		HAO2	0.67	0.62	0.89	0.73
	Partial Data	HAO1	0.67	0.64	0.78	0.70
		HAO2	0.63	0.57	1.0	0.73
		HBO1	0.61	0.56	0.70	0.38
		HBO2	0.56	0.54	0.89	0.67
K-Means Clustering	All Data	HAO1	0.71	0.77	0.6	0.67
		HAO2	0.93	0.87	1	0.93
		HBO1	0.76	0.8	0.69	0.74
		HBO2	0.88	0.82	0.96	0.88
	Partial Data	HAO1	0.64	0.6	0.87	0.70
		HAO2	0.71	0.62	1.0	0.77
		HBO1	0.60	0.56	0.88	0.68
		HBO2	0.67	0.62	0.89	0.73

VII. EVALUATION

This section presents the findings from the considered smart home control model and the feasibility of implementing our proposed framework. We present the SHATTER's evaluation results considering the following set of research questions.

RQ1 What is ADM's contribution to reducing stealthy FDI attacks? Section VII-A)

RQ2 What is the Performance of the SHATTER-generated Attack Schedule? Section VII-B)

RQ3 What is the contribution of an activity monitoring system in the case of aggravating attack impact? (Section VII-C)

RQ4 What are the framework findings in assessing the proposed attack impact with variable attacker's capability? (Section VII-D)

RQ5 How feasible is implementing the proposed framework for a scalable smart home system/other CPS domain? (Section VII-E)

A. Evaluation of Anomaly Detection Model

As we discussed, stealthy FDI attacks can help knowledgeable adversaries to bypass the ADM and make the system vulnerable. Hence, assessing the system's ADM against stealthy FDI attacks is mandatory from a security perspective. Here, we compare the SHATTER-considered ADM to a state-of-the-art framework (i.e., BIoTA) that does not consider a robust ADM but rather considers some verification rules. The contribution of ADM is evaluated based on the reduction of stealthy FDI attack impact. In this attack impact evaluation process, we do not consider the triggering of the smart appliances. A comprehensive performance evaluation of the considered ADMs is provided in Table IV. The results indicate that other than the HAO1 dataset, K-Means clustering outperformed DBSCAN-based ADM. We generate the anomalous/attack data using the BIoTA framework for this evaluation process. We consider variable attackers' knowledge ADM assessment, i.e., the attacker has either access to all day's occupancy, activity, and sensor measurement data used for ADM training (all data) or 50% of them (partial data).

TABLE V
COMPARISON IN BETWEEN SHATTER ATTACK IMPACT WITH BIOTA FRAMEWORK AND GREEDY ATTACK SCHEDULING APPROACH.

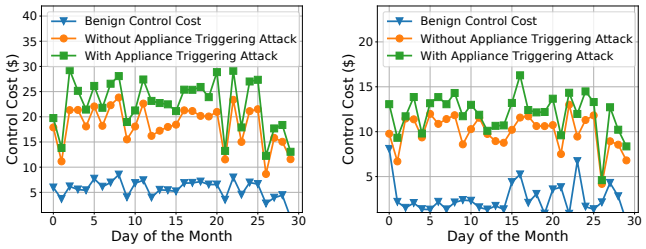
Framework/ Approach	**ADM**	**Attacker's Knowledge**	**House A Energy Cost ($)**	**House B Energy Cost ($)**
BIoTA	Rules-based	-	775.83	518.50
Greedy	DBSCAN	All Data	517.51	307.06
		Partial Data	447.02	148.39
	K-Means Clustering	All Data	513.92	220.37
		Partial Data	30.4.90	104.61
SHATTER	DBSCAN	All Data	549.58	299.69
		Partial Data	461.01	132.95
	K-Means Clustering	All Data	745.04	454.61
		Partial Data	361.15	434.09

Table V shows the cost comparison between the BIoTA, greedy attack scheduling, and our proposed SHATTER framework for both ARAS Houses A and B datasets. BIoTA-identified attack vectors' costs are at most 1.5 times higher than the SHATTER-identified attack vectors. However, our considered ADM identified (60-100)% attack vectors identified by the BIoTA framework as anomalies. Hence, we can conclude that the BIoTA-identified attack vectors are not stealthy for the considered ADMs. In our proposed framework, we consider a robust ADM to synthesize critical and hazardous attack vectors that can evade modern control systems and thus obtain a defense guide for secure control architecture.

There is an interesting insight from the results shown in Table V. It seems that the attack impact of DBSCAN-based ADM is lower than the K-Means clustering-based ADM although the latter mostly showed better performance (Table IV). The attack impact of the DBSCAN-based system can be as much as 35% lower than that of the K-means clustering-based ADM. The reason behind this is that the attacks obtained from BIoTA were very naive and maintained a large margin from the benign data distribution. Hence, the BIoTA-identified attacks are not a good choice for ADM model assessment. Since K-means clustering clusters all the training samples, unlike DBSCAN, which removes the noise points, the cluster areas were unnecessarily large. Accordingly, the k-means cluster-based ADM failed to capture the zero-day attacks found by SHATTER. From this evaluation, it can be inferred that the SHATTER-identified attack vectors are more appropriate to assess ADMs than the state-of-the-art. It needs to be noted that the purpose of this work is not to propose an optimal ADM. The developed ADM is used for the experimentation and evaluation of SHATTER. The framework is flexible enough to consider any ADM to assess its data-driven security and robustness against stealthy FDI/ integrity attacks in IoT-based control systems. In the rest of the evaluation, we will use DBSCAN-based ADM as it performs better.

B. Evaluation of SHATTER-generated Attack Schedule

The SHATTER framework generates an optimal attack schedule to misinform the controller with occupancy information at different zones. As discussed before, the considered scheduling is an NP-hard problem. To get a polynomial time solution, we consider window-based dynamic optimization. For the experimentation, we optimize each at every 10 slots



(a) (b)

Fig. 10. Control cost comparison with or without appliance triggering attacks for (a) ARAS House A (b) ARAS House B considering DBSCAN ADM.

(a slot corresponds to 1 minute sampling time) to get the final attack schedule. However, throughout the day, there can be 1440 possible slots (considering the sampling time to be 1 minute). Reducing sampling time will make the scheduling problem even more critical, in turn, a robust control system. Our experimentation suggests that a SHATTER-generated attack schedule can incur significantly higher costs than a greedy attack scheduling strategy. From Table V, we can see that the proposed attack scheduling is incurring up to $32.07 more cost (i.e., for DBSCAN-based ADM of House A) throughout a month compared to the greedy attack approach, where the benign control cost was $244.69. The higher attack cost for the greedy attack schedule compared to the SHATTER attack schedule supports the essence of dynamic attack scheduling. The SHATTER-identified attack vector would create more impact if the optimization window was larger.

C. Evaluation of Activity Monitoring System

In this evaluation, we show how the knowledge of activity information can help the adversaries to further increase the smart home HVAC energy cost. With the knowledge of activity information, a stealthy appliance-triggering attack is possible. Without the activity information, an attacker can maliciously activate an appliances that can create suspicion among the occupants even after evading the ADM. In the earlier evaluations, we did not consider any appliance-triggering attacks. The spikes in Figure 10 indicate a significant rise in control cost through appliance-triggering attacks. With full adversarial access, such an attack can increase the cost by $124.93 (+22.73%) and $60.03 (+20.03%), respectively, for ARAS Houses A and B.

D. Attack Impact Evaluation by Varying Attacker's Capability

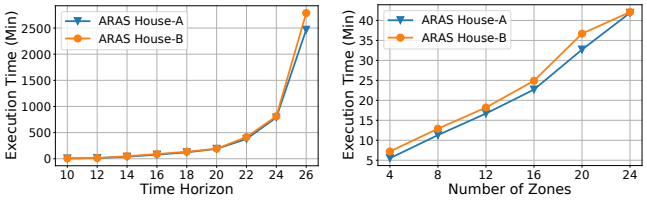
We evaluate the attack impact with different attackers' capabilities. In this evaluation, we analyze the appliance-triggering attack impact with variable measurement and appliance access. In Table VI, we show the attack impact considering that the adversary has accessibility to sensor measurements of different zones and can trigger all appliances. The evaluation shows that the attacker can create a significant attack impact by having access to 3 and 4 zones. However, access to 2 zones reduces the attack impact drastically (3.7 times in ARAS House A and 12.22 times in House B). Hence, SHATTER proposes a successful defense strategy. In Table VII, we show the attack impact considering that the adversary has

TABLE VI
APPLIANCE TRIGGERING ATTACK IMPACT WITH VARIOUS ZONE MEASUREMENT ACCESS CAPABILITY

Number of Accessible Zone	House A Energy Cost ($)	House B Energy Cost ($)
4 Zones	124.93	60.03
3 Zones	117.42	31.91
2 Zones	33.74	4.91

TABLE VII
APPLIANCE TRIGGERING ATTACK IMPACT WITH VARIOUS APPLIANCE TRIGGERING CAPABILITY

Number of Accessible Appliances	House A Energy Cost ($)	House B Energy Cost ($)
13 Appliances	124.93	60.03
8 Appliances	117.89	51.16
3 Appliances	93.05	50.82



(a) (b)

Fig. 11. Scalability analysis based on (a) time horizon, (b) horizontal scaling.

accessibility to appliances of different zones and can inject false measurements in all zone sensor measurements. The results show that even with access to 3 appliances (out of 13), a significant attack impact can be created in both houses. The analysis from Tables VI and VII suggests that the defense mechanism should focus on securing occupancy and IAQ measurements compared to appliances.

E. Scalability Analysis of SHATTER

Identification of an optimal stealthy attack vector through the proposed attack technique evading the complex ADM is an NP-hard problem. The optimal attack vector identification requires solving an optimization problem of 1440 (1 minute sampling time for all measurements) lookback time. We evaluate the scalability of the SHATTER framework by varying the time horizon (i.e., lookback time). The increase in the number of zones multiplies the number of constraints. Fig. 11(a) shows scalability analysis based on different lookback times, which affirms the exponential growth of execution time. However, horizontal scaling (i.e., increased number of zones) raises the number of constraints linearly. Hence, the execution time for an increased number of zone is growing linearly, as shown in Figure 11(b) (lookback = 10).

VIII. RELATED WORK

In this section, we compare our proposed attack analyzer with comparable literature. Although the work mainly focuses on attack analysis, we provide a comprehensive literature review of the control systems, ADM, and attack analytics.

A. Control Systems and Anomaly Detection

Traditionally, closed-loop control systems have relied on physics-based models of dynamic systems for optimal control decisions. These models are mathematically analyzed. However, in recent times, ML is increasingly used to develop

controllers. Since ML models are integrated into controllers as a classifier to identify control actions or as a validator to detect faulty/anomalous/attacked data [37], [38], [39]. Although ML-based methods are adaptable and robust against measurement errors and noises, they lack systematic mathematical analysis and are often viewed as black-box methods.

There has been extensive research into developing ADMs, in the context of smart homes and related domains. For instance, Pan et al. introduced an ADM that utilizes a context-aware BACnet data structure for building automation and control networks [40]. However, the ADM did not prove effective in reducing false-positive alarms. Another research developed a lightweight rule-based ADM for smart home/building control systems [41]. Analyzing BIoTA, we have discovered that rules-based ADMs leave backdoors to be exploited, which makes them vulnerable to zero-day attacks. In one of our previous works, we developed an ensembled unsupervised ML model for detecting attacks from the BIoTA framework [42]. The performance was extensively good although only getting trained with benign data, we have already experimented that most of the BIoTA-identified attacks are trivial. The definition of performance from different ADM-related research is questionable. The reason is that, in most cases, the performance of the models is evaluated based on some known attack or concrete decision boundary around the known benign samples. Hence, the vulnerability of those models can be easily exploited. Therefore, we focus on critical feature selection for model training.

B. Attack Analytics

Development of attack analytics has always been a concern for safety-critical CPSs. The existing research can be broadly classified into regulation, rules, and ML-based analytics.

Regulation and Rules-based Analytics: Stellios et al. introduced a new approach to identify and evaluate attack paths against critical IoT systems based on assessing risks, utilizing existing tools (i.e., CVE, CVSS) [8]. Akatyev et al. evaluated potential threats for futuristic smart homes with multiple diverse components and advanced decision-making abilities [10]. Casola et al. proposed an automated method for threat modeling and risk assessment based on a threat catalog created during the FP7 SPECS project, which targeted the communication protocol and software elements of IoT systems [43]. The analysis of security threats and resiliency in rule-based IoT systems has been thoroughly researched and explored in previous studies. Mohsin et al. developed a formal security analysis framework for IoT-based systems by analyzing network topology and interdependencies between system components [11], [12]. This framework can identify potential attack vectors from integrity and availability types of attacks and assess the system's resiliency against attackers with varying accessibility and capabilities. However, these proposed frameworks are limited to analyzing the security of rules-based IoT systems. Analysis of such systems does not require investigating historical data or maintaining time-series patterns. SHATTER can find hazardous attack vectors that can evade sophisticated defense tools.

ML-based Analytics: Solving constraints in ML-based systems is much more complex than in rule-based systems, and as a result, formal analysis of deep neural network-based ML models has become a focus of contemporary research. Various effective tools, including Reluplex, Sherlock, and Marabou, have been developed for verifying ML models [14], [15], [16]. Researchers have attempted to identify issues and analyze the behavior of ML-based systems in uncertain environments using formal methods. Souri et al. formally verified a hybrid ML-based approach for fault prediction in IoT applications [13]. However, unlike these verification approaches, the proposed framework can synthesize attack vectors contemplating activity recognition, appliance triggering, and ML-based ADMs, producing useful attack vectors to assess and propose defense systems.

IX. Conclusion

In this work, we propose a novel framework that analyzes the threat space of a smart IoT-enabled home control system, efficiently extracting ADM rules. We evaluate the proposed attack analyzer's effectiveness on the ARAS dataset. Moreover, we also build a prototype testbed for validating the framework in real-life settings. Experimental analysis using the verification dataset and validation testbed exhibits the effectiveness of the proposed framework. SHATTER generates sub-optimal attack vectors by creating optimal attack schedules in constrained time horizons. The results show that SHATTER-generated attack vectors can increase a home's energy consumption by more than 20% by leveraging appliance-triggered attacks. Some modern homes generate (i.e., using generators or renewable energy sources) and store energy, using batteries to reduce peak hour energy expense. Based on the capacity of the energy storage, excess energy can be produced, which has not been modeled by our proposed framework. If there is excess energy production, the home can be viewed as a microgrid, which sells the excess energy to the grid. Even though SHATTER-identified attacks will unquestionably decrease earnings compared to a benign operating condition, the attack's impact in this scenario will be distinct and needs attention. In our future attack modeling, we will factor in renewable power sources.

X. Acknowledgment

This work is partially supported by the National Security Agency (NSA) under Award# H98230-21-1-0324, the Department of Energy (DOE) under Award# DE-CR0000024, and the Visiting Faculty Research Program (VFRP) with the Information Assurance Branch of the AFRL/RI, Rome, NY, and the Information Institute (II). Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the DOD/AFRL, NSA, or DOE.

REFERENCES

[1] Mojtaba Eskandari, Zaffar Haider Janjua, Massimo Vecchio, and Fabio Antonelli. Passban ids: An intelligent anomaly-based intrusion detection system for iot edge devices. *IEEE Internet of Things Journal*, 7(8):6882–6897, 2020.

[2] Ankit Anubhav. Iot thermostat bug allows hackers to turn up the heat. https://blog.newskysecurity.com/iot-thermostat-bug-allows-hackers-to-turn-up-the-heat-948e554e5e8b, 2017. Accessed: 2022-05-16.

[3] Nur Imtiazul Haque, Mohammad Ashiqur Rahman, Dong Chen, and Hisham Kholidy. Biota: Control-aware attack analytics for building internet of things. In *2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 1–9. IEEE, 2021.

[4] Predictive control. https://buildingiq.com/products/predictive-control/, 2023. Accessed: 2023-02-27.

[5] Hande Alemdar, Halil Ertan, Ozlem Durmaz Incel, and Cem Ersoy. Aras human activity datasets in multiple homes with multiple residents. In *2013 7th International Conference on Pervasive Computing Technologies for Healthcare and Workshops*, pages 232–235. IEEE, 2013.

[6] Testbed kth sample data, gdpr compliance. https://www.liveinlab.kth.se/en/projekt/2.90711/download-sample-datasheets-1.974705. Accessed: 2020-05-21.

[7] Diane J Cook, Aaron S Crandall, Brian L Thomas, and Narayanan C Krishnan. Casas: A smart home in a box. *Computer*, 46(7):62–69, 2012.

[8] Ioannis Stellios, Panayiotis Kotzanikolaou, and Christos Grigoriadis. Assessing iot enabled cyber-physical attack paths against critical systems. *Computers & Security*, 107:102316, 2021.

[9] Zeinab Bakhshi, Ali Balador, and Jawad Mustafa. Industrial iot security threats and concerns by considering cisco and microsoft iot reference models. In *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pages 173–178. IEEE, 2018.

[10] Nikolay Akatyev and Joshua I James. Evidence identification in iot networks based on threat assessment. *Future Generation Computer Systems*, 93:814–821, 2019.

[11] Mujahid Mohsin, Zahid Anwar, Ghaith Husari, Ehab Al-Shaer, and Mohammad Ashiqur Rahman. Iotsat: A formal framework for security analysis of the internet of things (iot). In *2016 IEEE conference on communications and network security (CNS)*, pages 180–188. IEEE, 2016.

[12] Mujahid Mohsin, Zahid Anwar, Farhat Zaman, and Ehab Al-Shaer. Iotchecker: A data-driven framework for security analytics of internet of things configurations. *Computers & Security*, 70:199–223, 2017.

[13] A. Souri, A. S. Mohammed, M. Y. Potrus, MH Malik, F. Safara, and M. Hosseinzadeh. Formal verification of a hybrid machine learning-based fault prediction model in internet of things applications. *IEEE Access*, 8:23863–23874, 2020.

[14] G. Katz, C. Barrett, D. Dill, K. Julian, and M. Kochenderfer. Reluplex: An efficient smt solver for verifying deep neural networks. In *International Conference on Computer Aided Verification*, pages 97–117. Springer, 2017.

[15] S. Dutta, S. Jha, S. Sanakaranarayanan, and A. Tiwari. Output range analysis for deep neural networks. *arXiv preprint arXiv:1709.09130*, 2017.

[16] G. Katz, D. Huang, D. Ibeling, K. Julian, C. Lazarus, R. Lim, P. Shah, S. Thakoor, H. Wu, A. Zeljić, et al. The marabou framework for verification and analysis of deep neural networks. In *International Conference on Computer Aided Verification*, pages 443–452. Springer, 2019.

[17] C Bradford Barber, David P Dobkin, and Hannu Huhdanpaa. The quickhull algorithm for convex hulls. *ACM Transactions on Mathematical Software (TOMS)*, 22(4):469–483, 1996.

[18] Nur Imtiazul Haque, Mohammad Ashiqur Rahman, Md Hasan Shahriar, Alvi Ataur Khalil, and Selcuk Uluagac. A novel framework for threat analysis of machine learning-based smart healthcare systems.

[19] Shatter repository. https://github.com/imtiazulhaque/research-implementations/tree/master/shatter, 2022.

[20] Andrew Persily and Lilian de Jonge. Carbon dioxide generation rates for building occupants. *Indoor air*, 27(5):868–879, 2017.

[21] Mete Çelik, Filiz Dadaşer-Çelik, and Ahmet Şakir Dokuz. Anomaly detection in temperature data using dbscan algorithm. In *2011 International Symposium on Innovations in Intelligent Systems and Applications*, pages 91–95. IEEE, 2011.

[22] John A Hartigan and Manchek A Wong. Algorithm as 136: A k-means clustering algorithm. *Journal of the royal statistical society. series c (applied statistics)*, 28(1):100–108, 1979.

[23] Lawrence Hubert and Phipps Arabie. Comparing partitions. *Journal of classification*, 2:193–218, 1985.

[24] Types of hvac communication protocols. https://blog.belimo.com/blog/types-of-hvac-communication-protocols, 2023. Accessed: 2023-02-27.

[25] Wenbo Ding and Hongxin Hu. On the safety of iot device physical interaction control. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 832–846, 2018.

[26] Yanzi Zhu, Zhujun Xiao, Yuxin Chen, Zhijing Li, Max Liu, Ben Y Zhao, and Haitao Zheng. Et tu alexa? when commodity wifi devices turn into adversarial motion sensors. *arXiv preprint arXiv:1810.10109*, 2018.

[27] Liang Liu, Xiangyu Xu, Yulei Liu, Zuchao Ma, and Jianfei Peng. A detection framework against cpma attack based on trust evaluation and machine learning in iot network. *IEEE Internet of Things Journal*, 8(20):15249–15258, 2021.

[28] Wenbo Ding, Hongxin Hu, and Long Cheng. Iotsafe: Enforcing safety and security policy with real iot physical interaction discovery. In *the 28th Network and Distributed System Security Symposium (NDSS 2021)*, 2021.

[29] Nirupam Roy, Haitham Hassanieh, and Romit Roy Choudhury. Backdoor: Making microphones hear inaudible sounds. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, pages 2–14, 2017.

[30] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, pages 103–117, 2017.

[31] Nirupam Roy, Sheng Shen, Haitham Hassanieh, and Romit Roy Choudhury. Inaudible voice commands: The {Long-Range} attack and defense. In *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, pages 547–560, 2018.

[32] Qiben Yan, Kehai Liu, Qin Zhou, Hanqing Guo, and Ning Zhang. Surfingattack: Interactive hidden attack on voice assistants using ultrasonic guided waves. In *Network and Distributed Systems Security (NDSS) Symposium*, 2020.

[33] Leonardo De Moura and Nikolaj Bjørner. Z3: An efficient smt solver. In *International conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 337–340. Springer, 2008.

[34] Eugen. Do led lights produce heat? https://ledlightinginfo.com/do-led-lights-produce-heat, 2020. Accessed: 2023-02-27.

[35] Residential rate plan pricing. https://www.pge.com/pge_global/common/pdfs/rate-plans/how-rates-work/Residential-Rates-Plan-Pricing.pdf, 2023. Accessed: 2023-02-27.

[36] Kemal Akkaya, Ismail Guvenc, Ramazan Aygun, Nezih Pala, and Abdullah Kadri. Iot-based occupancy monitoring techniques for energy-efficient smart buildings. In *2015 IEEE Wireless communications and networking conference workshops (WCNCW)*, pages 58–63. IEEE, 2015.

[37] Mina Moghaddam, Tahsincan Köse, M Rasit Ozdemir, Zakiah Utami, and Seyda Ertekin. Energy-efficient smart buildings by occupancy prediction.

[38] Yuzhen Peng, Adam Rysanek, Zoltán Nagy, and Arno Schlüter. Using machine learning techniques for occupancy-prediction-based cooling control in office buildings. *Applied energy*, 211:1343–1358, 2018.

[39] Hamza Elkhoukhi, Y NaitMalek, A Berouine, Mohamed Bakhouya, D Elouadghiri, and Mohammed Essaaidi. Towards a real-time occupancy detection approach for smart buildings. *Procedia computer science*, 134:114–120, 2018.

[40] Zhiwen Pan, Salim Hariri, and Jesus Pacheco. Context aware intrusion detection for building automation systems. *Computers & Security*, 85:181–201, 2019.

[41] Hong Luo, Ruosi Wang, and Xinming Li. A rule verification and resolution framework in smart building system. In *2013 International Conference on Parallel and Distributed Systems*, pages 438–439. IEEE, 2013.

[42] Nur Imtiazul Haque, Mohammad Ashiqur Rahman, and Hossain Shahriar. Ensemble-based efficient anomaly detection for smart building control systems. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 504–513. IEEE, 2021.

[43] Valentina Casola, Alessandra De Benedictis, Massimiliano Rak, and Umberto Villano. Toward the automation of threat modeling and risk assessment in iot systems. *Internet of Things*, 7:100056, 2019.