

BIoTA: Control-Aware Attack Analytics for Building Internet of Things

Nur Imtiazul Haque*, Mohammad Ashiqur Rahman*, Dong Chen[†] and Hisham Kholidy[‡]

*Analytics for Cyber Defense (ACyD) Lab, Florida International University, USA

[†]Cyber-Physical Systems Laboratory (CPSLab), Florida International University, USA

[‡]Department of Network and Computer Security, State University of New York Polytechnic Institute, USA

*{nhaque004, marahman}@fiu.edu, [†]dochen@cis.fiu.edu, [‡]kholidh@sunypoly.edu

Abstract—Modern building control systems adopt demand control heating, ventilation, and cooling (HVAC) for increased energy efficiency. The integration of the Internet of Things (IoT) in the building control system can determine real-time demand, which has made the buildings smarter, reliable, and efficient. As occupants in a building are the main source of continuous heat and CO_2 generation, estimating the accurate number of people in real-time using building IoT (BIoT) system facilities is essential for optimal energy consumption and occupants' comfort. However, the incorporation of less secured IoT sensor nodes and open communication network in the building control system eventually increases the number of vulnerable points to be compromised. Exploiting these vulnerabilities, attackers can manipulate the controller with false sensor measurements and disrupt the system's consistency. The attackers with the knowledge of overall system topology and control logics can launch attacks without alarming the system. This paper proposes a building internet of things analyzer (BIoTA) framework¹ that assesses the smart building HVAC control system's security using formal attack modeling. We evaluate the proposed attack analyzer's effectiveness on the commercial occupancy dataset (COD) and the KTH live-in lab dataset. To the best of our knowledge, this is the first research attempt to formally model a BIoT-based HVAC control system and perform an attack analysis.

Index Terms—Internet of Things, Cyberattack, HVAC, Smart Buildings, Threat Analysis

I. INTRODUCTION

The heating, ventilation, and cooling (HVAC) control system accounts for almost 35% of energy consumption in residential and commercial building facilities [1]. With the advent of the building internet of things (BIoT), HVAC systems' energy consumption is reducing significantly [2]. Estimating the accurate number of occupancy through sensor nodes, BIoT can make optimal control decisions that benefit modern HVAC control systems to maintain precise mechanical ventilation and cooling [3]. In a BIoT-based HVAC control system, occupancy, temperature, and CO_2 monitoring sensor nodes send periodic measurements to the controller. The controller accumulates all the sensor status and generates control decisions accordingly to regulate actuators (e.g., air mixing vents and supply fans). The integration of IoT in the HVAC control system adds

several benefits concerning monitoring, analyzing, and tracking system status and generating automated control decisions. Additionally, if some inconsistent events occur, real-time alerts are sent to the system admin to take necessary actions.

Current building architecture implants distributed air handling units (AHUs) throughout the building for maximum energy efficiency [4]. Each AHU is responsible for maintaining the indoor air quality (IAQ) and the temperature of a specific zone using the outside fresh air, and the recirculating return air from the zone. Several factors contribute to energy consumption by an HVAC control system (e.g., weather condition, peak demand time, occupancy pattern, etc.). At the same time, occupants' comfort depends on IAQ and the desired set-point temperature. Allowing fresh outdoor air in the zones helps control the air quality, but the desired room temperature deviates significantly from the fresh air temperature. The HVAC control systems are prone to utilize recirculating the zone air for energy efficiency, which, in turn, raises the concentration of air pollutants as occupants of the zones always produce CO_2 . Therefore, for optimal control strategy, amalgamated fresh and return air is supplied through the zones to confirm comfort and cost-efficiency.

However, BIoT-enabled HVAC control systems are highly potential for cyberattacks. According to a report by Qualys, a cloud security service provider connecting almost 55,000 HVAC systems to the internet possess flaws that can easily be exploited by hackers [5]. Cybersecurity firm ForeScout Technologies reported in 2019 that 8,000 IoT devices related to HVAC systems are vulnerable to cyberattacks [6]. In Finland, an attack on the heating system left residents of two apartment buildings in the cold for nearly a week [7]. An adversary, depending on the attack capability, can achieve various attack goals exploiting these vulnerabilities. Therefore, it is essential to explore these wide-ranged potential attacks on a smart HVAC system considering various attack capabilities and thus understand the system's attack-resiliency in different scenarios. Such an analysis cannot be done empirically through experiments; instead, it requires non-invasive attack analytics.

This paper addresses the challenge mentioned above by proposing the BIoT analyzer (BIoTA), a formal framework to perform security analysis of smart building HVAC control systems. In particular, this formal analysis considers two distinct kinds of attack targets: (i) increasing energy con-

¹[https://github.com/imtiazulhaque/research-
implementations/tree/main/biota](https://github.com/imtiazulhaque/research-implementations/tree/main/biota)

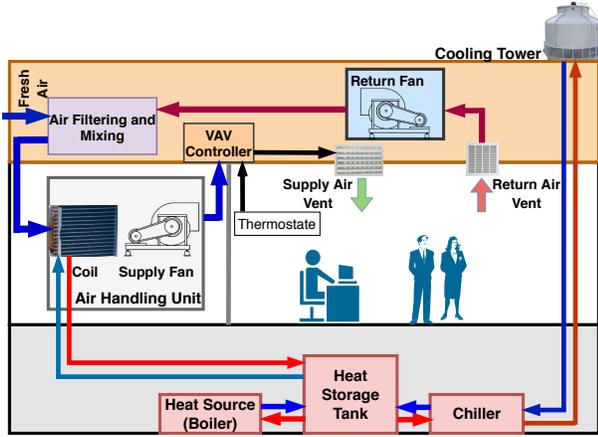


Fig. 1. HVAC Control Setup in Smart Building

sumption and (ii) disrupting occupants' comfort for maximum occupants. We think of a BIoT-enabled smart building, where the controller also looks for suspected behaviors (e.g., zone occupancy exceeding maximum capacity, inconsistency in sensor measurements, etc.) along with generating control decisions. Hence, an attacker cannot launch an attack manipulating sensor measurements arbitrarily. Our proposed framework synthesizes feasible attacks based on the attacker's knowledge, accessibility, and target/goal, which allows us to realize the system's attack-resiliency according to the attack model. In this work, we are formally modeling the HVAC control system leveraging mass balance equation-based ventilation control and energy balance equation-based temperature control, which can imitate the dynamics of air and heat balance of a HVAC control system [8]. Moreover, we analyze both commercial and residential buildings' security using two state-of-the-art building occupancy datasets naming commercial occupancy dataset (COD) [9] and KTH live-in lab dataset [10].

The rest of the paper is organized as follows: We briefly discuss HVAC control systems in Section II. We present the BIoTA framework's architecture in Section III. In Section IV, we present the formal model of attack analysis. We provide two case studies in Section V. We present the evaluation results in Section VI. Finally, we conclude the paper in Section VII.

II. BACKGROUND

In this section, we briefly discuss the HVAC control system's working principle and the attack model.

A. HVAC Control System

A simplistic view of a building HVAC control system's overall control architecture is demonstrated in Fig. 1. The air handling unit (AHU) is the heart of HVAC control, which performs mixed air filtering, humidity control through humidifier and dehumidifier, as well as air temperature control using heating and cooling coils [11]. After proper air quality control, the AHU supplies air to the zones using the supply fan. The operation of the supply fan is scheduled by the control system, depending on the zone demand. The AHU brings air from a duct, where both fresh outside air and recirculated return air from the rooms are mixed and filtered. A zone's demand is

determined by a thermostat, which is used to set the preferred temperature, humidity, and CO_2 concentration of the zone occupants.

Each room of a zone has different air demand because of the difference in corresponding heating or cooling loads. The cooling and heating loads determine the amount of heat energy that needs to be removed or added in the building zone. A valve is placed in the vents to control the dampers' opening and maintain the required airflow. The temperature of the zone's supply air depends on the temperature of the mixed air and zone temperature setpoints. In the case of cooling, the temperature of supply air is typically set to 55°F, while for heating, supply air temperature is kept 40-70°F above the return air temperature [12], [13]. The air is chilled or heated through the refrigerants flowing through the coils. After heating or chilling air, the refrigerant temperature gets reduced, which is brought back to the coil setpoint temperature using the heat storage tank typically placed in the basement of the building. The heat storage tank's temperature is maintained using the connected chiller and the boiler based on the weather demand. The chillers are connected to the rooftop cooling tower, which brings air and water together into direct contact for reducing refrigerants' temperature.

B. Ventilation and Temperature Control

The ventilation control is required to maintain the indoor air quality (IAQ). The IAQ can be considered satisfactory, provided the CO_2 concentration of the occupied zone is less than 1000 parts per million (ppm) [14]. The CO_2 concentration of the fresh outside air stays near about 400 ppm. The steady-state ventilation control of smart building HVAC control system follows the dynamics of the mass balance equation to ensure derivative of CO_2 concentration over the time is equal to zero and thus maintains the IAQ to a specific setpoint [15]. On the other hand, temperature control obeys the energy balance equation for dealing with the cooling and heating loads of the room and keeps the room temperature steady to a comfortable temperature. The HVAC control system's main challenge for temperature and ventilation control arises from the sudden change of demand because of the varying occupancy rate, generating heat, and CO_2 . The ventilation control tries to utilize more fresh outside air for a faster reduction of the CO_2 concentration from the air. But using more fresh air increases control cost due to significant deviation between fresh air and supply air temperature. The return air temperature stays closer to the zone's setpoint temperature and supply air temperature. However, the return air is contaminated with zone pollutants, which makes CO_2 concentration in the return air to be high.

C. HVAC Cost Calculation

Hence, in order to satisfying the occupants' need for ventilation and temperature comfort, both fresh air from outside needs to be brought in and return air from the zones needs to be re-circulated. The effectiveness of the HVAC control system depends on optimally mixing fresh and return air to satisfy both energy consumption and occupants' comfort.

After proper mixing, the HVAC control system measures the temperature and CO_2 concentration of the mixed air. If the mixed air temperature is high, the cool refrigerant flowing through the coil chills down the hot air to the supply air temperature. As the air is coming in very warm and going out very cool, the air gets condensed in the form of water, and that water is removed from the system using a pipe. The mass flow rate of condensate water and mixed air are used with few other psychrometric parameters to calculate the energy used in the coil [16]. During this process of cooling, the refrigerant temperature gets high, which requires bringing back to normal temperature in the chiller. The mixed air processing and cooling refrigerants in the chiller are mainly responsible for the HVAC cooling control cost. The air heating follows a similar procedure.

D. *BiOT Architecture of HVAC Control System*

For efficient control, information of the zones must be shared, which creates the need for the internet of things-based models. In our work, we consider a BiOT system, where occupancy, temperature, and CO_2 sensor nodes send their measurements to a central controller for optimal control decisions. The controller generates control signals to actuate the supply fan, return fan, and the valves of the vents. Our HVAC modeling assumes the followings:

- 1) The cooling load and ventilation requirement of every room of a particular zone are similar.
- 2) The cooling load of summer season and heating load of the winter season are presumed to be equal and constant throughout the year.
- 3) The occupants of a particular zone radiates an equal amount of heat and exhales an equal amount of CO_2 in every time instance. The occupants generated heat and CO_2 amount in a particular zone depends on the level on average occupant's physical activity, age, and metabolism rate [17].
- 4) The sensors have no sensitivity issues and precision errors.

E. *BiOT HVAC Control Attack Model*

The BiOT architecture opens a massive cyberattack surface for the attackers. By compromising sensor nodes and the communication link between sensors and controller, an attacker can inject false sensor measurements and propel the controller to make wrong decisions. Most recent research has shown that HVAC sensors can be compromised. For instance, Tu et al. conducted a physical level attack on the temperature sensor of an infant incubator which also prevents triggering automatic temperature alarm [18]. In addition, leveraging a man-in-the-middle (MitM) attack in the open communication channel of a BiOT-based model, an attacker can sniff and tamper sensor measurements. Newaz et al. demonstrated that adversarial machine learning based attack generation technique can be adopted for compromising sensor measurements without alarming the system [19]. As the sensor measurements of the BiOT system can be altered due to adversarial intent or sensor faults, the controller undertakes several security measures. To model attacks, we consider that the incoming

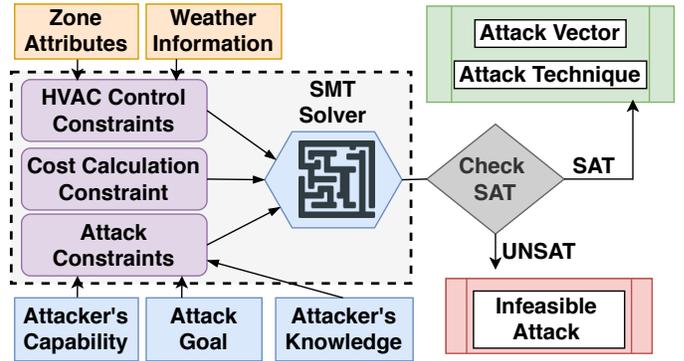


Fig. 2. BiOTA Framework

and outgoing events of the buildings are securely monitored through biometric sensors. Thus, malicious intent to increase the number of occupants in the targeted zones will notify the controller. Moreover, the maximum capacity for occupants in each zone is verified at every time slot by the controller.

F. *Related Work*

Research on smart building security recently has received special focus. Mace et al. introduced a multi-model methodology for assessing the security of smart-building systems, utilizing a suite of modeling, simulation, and analysis tools [20]. Meyer et al. presented an abstract model of a building automation system using attack trees in order to simplify the threat identification model [21]. In particular, the attack trees were used to analyze threats where an attacker could get sensor information and control actuators. Mustafa et al. analyzed the security of a smart building or building automation system using attack tree analysis tools based on a high-level requirement of safety and security [22]. Abdulmunem et al. also employed attack tree analysis and Markov models to analyze a building automation system's security and availability during the building's life cycle [23].

Model-driven security analysis-based researches of smart building control are also gaining popularity. Hachem et al. proposed a model-driven engineering method, systems-of-systems security (SoSSec), which comprises a modeling language (SoSSecML) to model system-of-systems (SoS) and multi-agent systems for security analysis of smart building's SoS architectures [24]. Moreover, Haque et al. has shown formal modeling based attack analytics in a machine learning-based smart healthcare system [25].

However, none of these works can perform automated attack analysis of a BiOT-based HVAC control system based on an attack model, a given set of adversarial capabilities, or an attack impact. Our proposed formal framework synthesizes formally proven attack vectors that can achieve an attack goal.

III. BIOTA FRAMEWORK

The architecture of the proposed framework is shown in Fig. 2. In this framework, the HVAC control constraints are generated using the building floor plan, properties of the zones, and the current states of sensor measurements. The attack constraints are dependent on the attacker's knowledge,

accessibility to sensor measurements, and attack goal. A set of constraints related to HVAC cost calculation are also needed to determine the cost of control before and after an attack to check whether the attack goal is satisfied or not. All these constraints are passed to the satisfiability modulo theory (SMT)-based solver as a constraint satisfaction problem (CSP). The solver solves the CSP utilizing various effective theories. If there is any possible solution, the SMT solver is guaranteed to find that which is indicated by SAT result. An UNSAT result, on the other hand, signifies that based on the current attacker's accessibility, the attack goal cannot be attained. When the solver approves the attack's feasibility, it also outputs the possible way of attack showing the attack vector. The attack vector discloses the complete attack technique showing which sensor measurements need to be altered along with the measurement values.

IV. FORMAL MODELING OF ATTACK ANALYSIS

In this section, we discuss the formal model of attack vector synthesis in detail.

A. Formal Modeling of HVAC Control System

For analyzing the smart building HVAC control system attacks, BIoTA formally models the control system using mathematical equations considering underlying system dynamics. Table I demonstrates the modeling notations for HVAC control. We consider the mass balance equation for ventilation control. Cali et al. approximated a numerical solution for the mass balance equation that can be utilized for taking ventilation control decisions [15]. The effectiveness of the controller depends on the accurate estimation of the number of people at a particular zone. We consider Passive Infra-red (PIR) sensors to measure the number of persons at a particular time instance. The ventilation requirement of a particular zone can be calculated using the following formula.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} \frac{S_{ij}^o C_i^P \Delta t}{V_i^Z} = C_{ij}^{set} - \left(1 - \frac{\dot{v}_i^m \Delta t}{V_i^Z}\right) S_{ij}^{ci} - \frac{\dot{v}_i^m \Delta t}{V_i^Z} S_{ij}^{cm} \quad (1)$$

Here, \dot{V}_{ij}^{mixed} is the mixed air volumetric flow which is the combination of both fresh and return air. Equation 3 is used to calculate the required amount of ventilation at each time instances. The temperature control decision is made based on the following equation.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} \dot{m}_{ij}^m Sh_{ij}^m (T_{ij}^{set} - S_{ij}^{ts}) = Q_j^L + S_{ij}^o Q_j^P \quad (2)$$

The controller also verifies the consistency of sensor measurements of the last control decision.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} \frac{S_{(i-1)j}^o C_i^P \Delta t}{V_i^Z} = S_{ij}^{ci} - \left(1 - \frac{\dot{v}_i^m \Delta t}{V_i^Z}\right) S_{(i-1)j}^{ci} - \frac{\dot{v}_i^m \Delta t}{V_i^Z} S_{ij}^{cm} \quad (3)$$

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} \dot{m}_{ij}^m Sh_{ij}^m (S_{(i-1)j}^{ti} - S_{ij}^{ts}) = Q_j^L + S_{(i-1)j}^o Q_j^P \quad (4)$$

TABLE I
MODELING NOTATIONS

Notation	Description	Unit	Data Type
P	Atmospheric pressure	Pa	Real
V_j^Z	Volume of j-th zone	ft^3	Real
C_j^P	CO_2 emission per person per minute at j-th zone	CFM	Real
Q_j^P	Heat radiation per person per second at j-th zone	kW	Real
Q_{ij}^L	Cooling or heating load of j-th zone at i-th time instance	kW	Real
C_{ij}^{set}	CO_2 setpoint of j-th zone at i-th time instance	PPM	Integer
T_{ij}^{set}	Temperature setpoint of j-th zone at i-th time instance	$^{\circ}F$	Integer
S_i^{to}	Temperature of fresh outdoor air at i-th time instance	$^{\circ}F$	Real
S_i^{co}	CO_2 concentration of fresh outdoor air at i-th time instance	PPM	Real
S_{ij}^{ti}	indoor temperature of j-th zone at i-th time instance	PPM	Real
S_{ij}^{ci}	indoor CO_2 concentration of j-th zone at i-th time instance	PPM	Real
S_{ij}^{tm}	Temperature of mixed air of j-th zone at i-th time instance	$^{\circ}F$	Real
S_{ij}^{cm}	CO_2 concentration of mixed air at j-th zone at i-th time instance	PPM	Real
S_{ij}^{hm}	Relative Humidity of mixed air of j-th zone at i-th time instance	(%)	Real
S_{ij}^{ts}	Temperature of supply air of j-th zone at i-th time instance	$^{\circ}F$	Real
S_{ij}^{hs}	Relative humidity of supply air of j-th zone at i-th time instance	(%)	Real
S_{ij}^o	Number of occupants j-th zone at i-th time instance	Person	Integer
\dot{v}_{ij}^m	Volumetric flow of mixed air of j-th zone at i-th time instance	CFM	Real
\dot{m}_{ij}^m	Mass flow of mixed air j-th zone at i-th time instance	$kg s^{-1}$	Real
Δt	Sampling time of the controller	minute	Integer
Pw_{ij}^m	Mixed air partial pressure of water vapor of j-th zone at i-th time instance	Pa	Real
Pw_{ij}^s	Supply air partial pressure of water vapor of j-th zone at i-th time instance	Pa	Real
Sh_{ij}^m	Specific heat of mixed air of j-th zone at i-th time instance	$J kg^{-1} K^{-1}$	Real
Sh_{ij}^s	Specific heat of supply air of j-th zone at i-th time instance	$J kg^{-1} K^{-1}$	Real
Sh^W	Specific heat of water	$J kg^{-1} K^{-1}$	Real
\dot{m}_j^{cl}	Mass flow of air in the coil in j-th zone	$kg s^{-1}$	Real
Eth_{ij}^m	Enthalpy of mixed air of j-th zone at i-th time instance	$J kg^{-1}$	Real
Eth_{ij}^s	Enthalpy of supply air of j-th zone at i-th time instance	$J kg^{-1}$	Real
T_{ij}^{cnd}	Temperature of condenser water of j-th zone at i-th time instance	$^{\circ}F$	Real
T_{ij}^{cl}	Temperature of coil water of j-th zone at i-th time instance	$^{\circ}F$	Real
Cl^{set}	Temperature setpoint of coil refrigerant	$^{\circ}F$	Real
\dot{m}_{ij}^{cnd}	Mass flow of condenser water of j-th zone at i-th time instance	$kg s^{-1}$	Real
$S_{ }$	Set of all Sensors of j-th zone	PPM, $^{\circ}F$, Person	Set
\mathcal{T}	Set of all timeslots	Unit	Set
\mathcal{Z}	Set of all Zones	Unit	Set
\mathcal{S}	Set of all Sensors	PPM, $^{\circ}F$, Person	Set

The temperature of supply air is kept 55 $^{\circ}F$ in summer season and 120 $^{\circ}F$ for winters. For effective control, the temperature of supply air is slightly increased at the time of cooling, while it is slightly reduced for heating.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} 55 \leq S_{ij}^{ts} \leq 120 \quad (5)$$

B. Formal Modeling of HVAC Cost Calculation

BloTA framework considers the cooling cost of a zone, which depends on the supply and the mixed air temperature. For chilling the mixed air to supply air, a significant amount of energy is needed in the cooling coil, which in terms increases the temperature of the refrigerants of the cooling coil. The refrigerants are sent to the chiller tower for cooling to the setpoint temperature, which also requires similar energy needed at the cooling coil.

For determining the psychrometric values, six co-efficient values are needed according to ASHRAE standard ($cf_0 = -5800.22$, $cf_1 = 1.39$, $cf_2 = -0.049$, $cf_3 = 4.17 \times 10^{-5}$, $cf_4 = -1.44 \times 10^{-8}$, $cf_5 = 6.54$). Calculating partial pressure of water is needed to determine specific heat, specific volume, and enthalpy of the supply and mixed air.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} Pw_{ij}^m = e^{\sum_{l=0}^4 (cf_l S_{ij}^{tl})^{l-1} + cf_5 \log_e(\mathcal{H}_{ij}^k)} \mathcal{S}_{ij}^{hm} \quad (6)$$

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} Pw_{ij}^s = e^{\sum_{l=0}^4 (cf_l S_{ij}^{ts})^{l-1} + cf_5 \log_e(\mathcal{H}_{ij}^k)} \mathcal{S}_{ij}^{hs} \quad (7)$$

The specific heat computation is needed to determine the mass airflow rate of condenser water, which in turn, is necessary for calculating the cost associated with coil cooling/heating.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}, k \in [m, s]} Sh_{ij}^k = \frac{0.621945 Pw_{ij}^k}{P - Pw_{ij}^k} \quad (8)$$

The enthalpy of the mixed and supply air is directly used to determine the HVAC cooling/heating coil cost.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} Eth_{ij}^m = 1.006 * \mathcal{S}_{ij}^{tm} + Sh_{ij}^m * (2501 + 1.86 * \mathcal{S}_{ij}^{tm}) \quad (9)$$

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} Eth_{ij}^s = 1.006 * \mathcal{S}_{ij}^{ts} + Sh_{ij}^s * (2501 + 1.86 * \mathcal{S}_{ij}^{ts}) \quad (10)$$

The specific volume of mixed air is used to calculate the volumetric flow of air simply by dividing mass flow rate by specific volume.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} Sv_{ij}^m = 287.042 \mathcal{S}_{ij}^m \frac{1 + 1.607858 Sh_{ij}^m}{P} \quad (11)$$

The mass flow of air in the condenser can be derived from the specific heat of mixed and supply air and mixed air flow rate.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} \dot{m}_{ij}^{cnd} = \dot{m}_{ij}^m (Sh_{ij}^m - Sh_{ij}^s) \quad (12)$$

The mass flow rate of condenser air can determine the heat energy required to chill the hot mixed air to supply air setpoint temperature.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} cost_{ij}^{cl} = \dot{m}_{ij}^m * (Eth_{ij}^s - Eth_{ij}^m) + \dot{m}_{ij}^{cnd} Eth_{ij}^{cnd} \quad (13)$$

But for chilling the mixed air, the temperature of coil refrigerant rises above the required temperature, which can be determined by following equation.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} T_{ij}^{cl} = Cl^{set} + (cost_{ij}^{cl} / (\dot{m}_i^{cl} * Sh^W)) \quad (14)$$

Hence, the refrigerants are passed to the chiller for cooling it back to the normal temperature which also adds cost to the system. The cost can be estimated by the following equation.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} cost_{ij}^{chil} = \dot{m}_i^{cl} * Sh^W * (T_{ij}^{cl} - Cl^{set}) \quad (15)$$

The overall cost of HVAC control cost is dependent on the coil cost and the chiller cost.

$$TC^{HVAC} = \sum_{i \in \mathcal{T}, j \in \mathcal{Z}} cost_{ij}^{cl} + cost_{ij}^{chil} \quad (16)$$

C. Formal Attack Model

Attack modeling is the process of potential threat recognition and security measures to protect a valuable system.

1) *Attacker's Knowledge*: The attacker's knowledge about the system determines the attack's stealthiness. This work considers a knowledgeable attacker aware of the surrounding weather pattern, building attributes, occupancy information, underlying control, and defense mechanisms of the smart building HVAC control system.

2) *Attack Goal*: The BloTA framework considers two different attack goals for launching attacks - increasing energy consumption and obstructing occupants' comfort. The energy consumption attack is straightforward in which the attacker attempts to change the sensor measurements to maximize the overall energy consumption in the building by forcing the control system to flow more fresh air in the supply airflow.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}, k \in [o, ti, ci]} \mathcal{S}_{ij}^k = (\mathcal{S}_{ij}^k + \delta_{ij}^k) \wedge TC^{HVAC} > \mathbb{H}\mathbb{C} \quad (17)$$

Here, $\mathbb{H}\mathbb{C}$ signifies the minimum threshold for cost increase due to attack. The occupants' discomfort attack attempts to deviate the CO_2 or temperature of the building zones far away from the setpoint.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}, k \in [o, ti, ci]} \mathcal{S}_{ij}^k = (\mathcal{S}_{ij}^k + \delta_{ij}^k) \wedge |S_{ci}^{ij} - C_{ij}^{set}| > \mathbb{O}\mathbb{C}\mathbb{C}_j \wedge |S_{ti}^{ij} - T_{ij}^{set}| > \mathbb{O}\mathbb{C}\mathbb{T}_j \quad (18)$$

Here, $\mathbb{O}\mathbb{C}\mathbb{C}_j$ signifies the minimum threshold for deviation from CO_2 concentration setpoint and $\mathbb{O}\mathbb{C}\mathbb{T}_j$ denotes the deviation of temperature setpoint due to attack.

3) *Accessibility to Sensor Measurements*: For compromising sensor measurement of a particular zone, the attacker needs to alter the sensor measurements of other sensors of that zone bypassing the controller's anomaly detector. The altered sensor measurements need to comply with controller verification.

4) *Attacker's Capability*: For successfully launching an attack, the attacker needs to compromise multiple sensor measurements. The altered occupancy sensor measurement of a zone must be less than the maximum capacity.

$$\forall_{i \in \mathcal{T}, j \in \mathcal{Z}} \mathcal{S}_{ij}^o + \delta_{ij} \leq \mathbb{M}\mathbb{O}_j \quad (19)$$

Here, $\mathbb{M}\mathbb{O}_j$ denotes the maximum occupancy at the j-th zone. The attackers are constrained to change the occupancy sensor measurements without making alternations in the total actual

TABLE II
ZONE PROPERTIES FOR COD AND KTH DATASETS

Datasets	Zones	Volume (ft^3)	CO2 Emission/Person (cfm)	Heat Radiation/Person (kW)	Cooling Load (kW)	Capacity (Person)
COD	Entrance	12570.36	0.0221	0.1082	0.725	50
	Clemente	11687.61	0.0213	0.1071	0.300	10
	Warhol	10910.79	0.0183	0.0924	0.450	25
	Laboratory	17937.48	0.0254	0.1193	0.825	40
KTH	Living Room	1119.2	0.0183	0.0924	0.05	5
	Kitchen	344.8	0.0221	0.1082	0.02	2
	Bathroom	252.2	0.0254	0.1193	0.02	1

occupant count of the current timeslots. Again, other sensor needs to be altered accordingly to avoid getting exposed.

$$\forall_{i \in \mathcal{T}} \sum_{j \in \mathcal{Z}} (\mathcal{S}_{ij}^o + \delta_{ij}) = \sum_{j \in \mathcal{Z}} (\mathcal{S}_{ij}^o) \quad (20)$$

V. EXAMPLE CASE STUDY

We perform two case studies on both commercial and residential datasets. Table II shows the properties of the zones of the datasets.

A. Case Study on the COD Dataset

To verify our BIoTA framework, we collect occupancy data from the COD dataset, which captures almost 90 thousand people entering and leaving five different spaces [9]. We analyze one year of data with ten-minute sampling by generating missing data from the data distribution. Table III shows actual sensor measurements and required average ventilation rate for the zones [26].

Energy Consumption Attack: Suppose an attacker is injecting false sensor measurements to launch a stealthy attack with the intent to increase the energy consumption of the building by 5%. Table III demonstrates a possible attack scenario, where the attacker achieves his attack goal by adding and subtracting occupancy sensor measurements by 17 to the entrance and the Warhol zones, respectively. At entrances, people produce 12% more CO_2 and radiates 17% more heat than the Warhol zones. Hence, due to the compromised measurements, the controller supplies 56% more air than required in the entrances, where the Warhol zone gets 13 times less airflow. Eventually, the entrance zone's temperature increases by 4%, whereas in Warhol zones, the temperature falls near the outdoor temperature. The actual energy requirement is 79.69 kWh for the presented scenario, but for compromised sensor measurements, the energy consumption goes higher to 82.23 kWh. The cost of electricity of Pennsylvania for wholesale electricity market is 7.02 \$ per kWh based on the recent rates [27]. So, is a 3¢ of overall cost increase in 10 minutes time interval because of the increased energy requirement. The attack analysis also reports that the same attack goal can be achieved by altering Warhol and laboratory measurements only, which in turn increases the energy consumption by 3.47 kWh and cost by 4.06¢.

Occupant Comfort Attack For performing occupants' comfort attack, let's assume, the attacker is modifying a set of sensor measurements to launch a stealthy attack with the intent to increase the CO_2 concentration of the laboratory zone by 25%. Table III demonstrates a possible attack scenario,

where the attacker achieves his attack goal by compromising occupancy sensors of the entrance and the laboratory zones by altering occupancy measurements by 20 people from Warhol to the entrance zone. In the laboratory zone, people produce 15% more CO_2 and radiates 10% more heat than the entrances. Hence, the controller supplies 66% more air than required in the entrances, where the laboratory zone will get four times less airflow. Eventually, the temperature of entrance zones increases by 5%, and in laboratory zones, the temperature falls near the outdoor temperature. For the presented scenario, the actual energy requirement is reduced by 1.69 kWh with the cost of significant discomfort to the occupants of the laboratory, which hampers the industry's productivity. The attack analysis shows that the same attack goal cannot be achieved by modifying any other two sensors.

B. Case Study on KTH Live-In Lab Dataset

We also verify our BIoTA framework using the KTH Live-In Lab dataset to assess the vulnerability of residential buildings. We analyze one-week data with ten-minute sampling by generating missing data from the available data distribution. We consider each room as a zone and the apartment to be a building for making HVAC control decisions. Table III shows actual sensor measurements and the required average airflow rate for the three zones.

Energy Consumption Attack: Suppose an attacker intends to increase the energy consumption of the considered residential building by more than 10%. Table III demonstrates a possible attack scenario, where the attacker achieves his attack goal compromising occupancy sensors of all three zones by adding one occupant to the bathroom and kitchen occupancy sensor measurements and balance it by removing 2 person from the living room occupancy sensor measurement. Therefore, the controller supplies 35% more air than required in the living room, where in the bathroom and the kitchen zones, the CO_2 concentration gets lower down to the outdoor air concentration. Eventually, the temperature of the living room zone falls by 13%, where in the kitchen and bathroom, the temperature rises by 6% and 10% respectively. For the presented scenario, the actual energy requirement is 16.41 kWh, but for compromised sensor measurements, the energy consumption increases to 18.37 kWh. The cost of electricity of Stockholm, Sweden for residential electricity market is 24.6 ¢ per kWh based on the 2019 rates [28]. There will be 3.48 cents of overall cost increase in 10 minutes of time because of the increased energy requirement. It can be seen that energy consumption attack is also affecting the occupant's comfort

TABLE III
EXAMPLE STEALTHY ATTACK SCENARIOS IN COD AND KTH DATASETS

Scenario	Measurement	COD Dataset				KTH Dataset		
		Entrance	Clemente	Warhol	Lab	Living Room	Kitchen	Bathroom
Actual	Zone Occupancy (Person)	30	3	18	26	4	1	0
	Zone Temperature (degree C)	75	75	75	75	69.8	68.9	69.5
	Zone CO ₂ (PPM)	1000	1000	1000	1000	927.1	923.5	854.7
	Zone Airflow (CFM)	1105.0	106.5	549.0	1100.66	138.87	42.21	1.3
Energy Consumption Attack	Zone Occupancy (Person)	47	3	1	26	2	2	1
	Zone CO ₂ (PPM)	704.26	1000	1282.13	1000	1254	400	400
	Zone Temperature (degree C)	78.67	75	62	75	60.9	73.1	76.6
	Zone Airflow (CFM)	1724	106.5	41.09	1100.66	69.43	84.43	55.86
Occupant Comfort Attack	Zone Occupancy (Person)	50	3	18	6	5	0	0
	Zone CO ₂ (PPM)	648.38	1000	1000	1283.2	763.59	156.45	854.7
	Zone Temperature (degree C)	79.08	75	62	62	71.5	39	69.5
	Zone Airflow (CFM)	1841.66	106.5	549.0	254.0	173.6	1.7	1.3

as well. BIoTA framework suggests that the attack goal of increasing energy consumption by 10% cannot be carried out attacking sensor measurements of two zones.

Occupant Comfort Attack To demonstrate the occupant comfort attack, let's assume that the attacker's goal is to increase the CO₂ concentration of the kitchen by more than 25%. Table III shows a possible attack scenario, where the attacker achieves his/her attack intent by compromising the occupancy sensor measurements of the kitchen and living room zone. Due to the attack, the controller supplies 25% more air than required in the living room. Due to the attack, the living room temperature increases by 2%, and in kitchen zones, the temperature falls near the outdoor temperature. Hence, the actual energy requirement is reduced by 2.2% with the cost of significant discomfort to the kitchen occupants. Compromising occupancy sensor measurements of the kitchen and the bathroom can not achieve the attack goal as suggested by our framework.

VI. EVALUATION

We implement our proposed BIoTA framework and evaluate it using two real datasets.

A. Implementation

The implementation source code for the BIoTA framework is available in GitHub [29]. We use the SMT solver to optimize a set of constraints [30]. We encode the conditions using integer and real terms. Based on the satisfiability, the model produces SAT or UNSAT results. The formal threat modeling has been implemented using Z3 library [31]. We have used python API of Z3 SMT solver for both solving and optimizing our modeling constraints. The psypy library is used to calculate and extract necessary psychrometric parameters from temperature and relative humidity [32]. The implementation of the library follows the ASHRAE standard.

TABLE IV
95% OF CONFIDENCE INTERVAL FOR ZONE-WISE OCCUPANCY

Dataset	Zone	95% Confidence Interval
COD	Entrances	7.88 - 12.36
	Clemente	0.21-0.55
	Warhol	0.31 -1.28
	Laboratory	6.14 - 9.67
KTH	Living Room	1.1-1.49
	Kitchen	0-0.27
	Bathroom	0-0.32

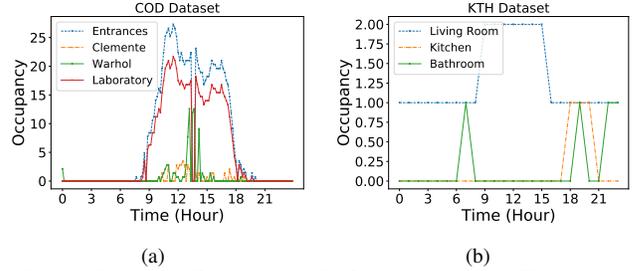


Fig. 3. Occupancy Pattern of (a) COD dataset and (b) KTH dataset.

B. Dataset Description

The occupancy pattern of both COD and KTH datasets are normally distributed. Figs 3(a) and 3(b) shows the average occupancy pattern throughout different hours of the day. The COD dataset captures data for almost a year. For KTH Live-In lab dataset, we only have one-week occupancy and temperature-related data. Table IV shows the zone-wise mean occupancy information with 95% confidence interval. In the COD dataset, the laboratory zone is the most occupied, and in the case of the KTH dataset, the living room zone is mostly occupied, probably by some visitors occasionally. The KTH outdoor temperature and relative humidity mean are within (39.3 - 41.2)^oF and (72.3 - 75.9)% for 95% confidence interval. In case of COD dataset, temperature mean lies in between (53.3 - 56.9)^oF, and relative humidity (63.39 - 65.96)% for 95% confidence interval. We present the source of additional data collection and processing in Section V.

C. Evaluation based on Energy Consumption Attack

To assess the maximum attack impact, we consider that an attacker is attacking every timeslot with optimal attack targets for maximizing the overall energy cost of the building. Fig. 4(a) shows the maximum and minimum attack impact

TABLE V
MAXIMUM INCREASE IN ENERGY OF COD DATASET BASED ON ACCESS TO SENSOR MEASUREMENTS OF ZONES

Access to Zones	Max Energy Increase (\$)
Entrances, Clemente , Warhol, Laboratory	303.95
Entrances, Clemente , Warhol	17.14
Entrances, Warhol, Laboratory	245.94
Entrances, Clemente, Laboratory	256.85
Clemente, Warhol, Laboratory	55.24
Entrances, Clemente	3.20
Entrances, Warhol	19.47
Entrances, Laboratory	192.42
Warhol, Laboratory	45.95
Clemente, Laboratory	8.95
Clemente , Warhol	3.75

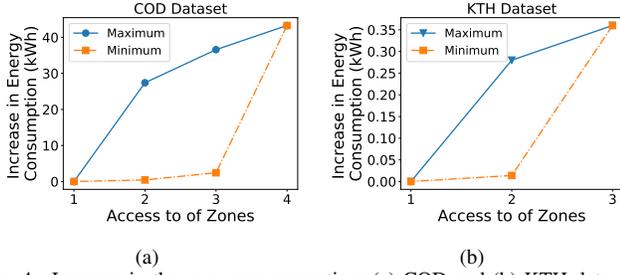


Fig. 4. Increase in the energy consumption: (a) COD and (b) KTH datasets.

TABLE VI

MAXIMUM INCREASE IN ENERGY BASED ON ACCESS TO SENSOR MEASUREMENTS OF ZONES

Access to Zones	Maximum Energy Increase (\$)
Living Room, Kitchen, Bathroom	8.95
Living Room, Bathroom	7.01
Living Room, Kitchen	2.77
Kitchen, Bathroom	0.35

based on energy consumption for a varying number of zone sensor measurements access in the COD dataset when the attacker is attacking optimally on all the timeslots. Table V shows the maximum increase in cost for all combination of zone sensor measurement access. It can be depicted that an attacker cannot do much harm if he/she has no access to sensor measurements of the laboratory zone. As people in the laboratory tend to work harder than the other zones, the controller needs to flow more air per occupant for this zone. Hence, the optimal attack goal will try to alter measurements showing occupants' movement from other zones to laboratory zones. As in Fig. 4(a), there is no increase in energy cost for only one zone sensor measurement access as changing the occupancy of a single zone will eventually fail the verification of the total number of people at a particular control instance. Table VI shows the maximum increase in cost for all combinations of zone sensor measurement access.

Fig. 4(b) shows the attack impact based on energy consumption for a varying number of zone sensor measurement access, and Table VI shows the maximum increase in cost for all combination of zone sensor measurement access for the KTH Live-In lab dataset. If an attacker can access two zone's sensor measurements, maximum attack impact can be attained if he/has access to all sensor measurements of the living room and bathroom. This is because the living room zone has most people to be swapped in the two other rooms.

D. Evaluation based on Occupants' Comfort Attack

Our proposed framework performs a two-step evaluation of attacks on occupants' comfort. At first, the attack impact is analyzed, considering the attack goal is to disrupt the occupants' ventilation need. Depending on the zones' sensor accessibility, we assume that the attacker is conducting optimal attacks in every timestep to ensure maximum discomfort in the maximum zones. Fig. 5(a) and 5(b) demonstrates the percentage of time CO_2 concentration of various zones of our dataset in consideration were failed to maintain IAQ due to stealthy FDI attack. It can be seen that if an attacker has access to all sensor measurements of the zones, attack analysis of the

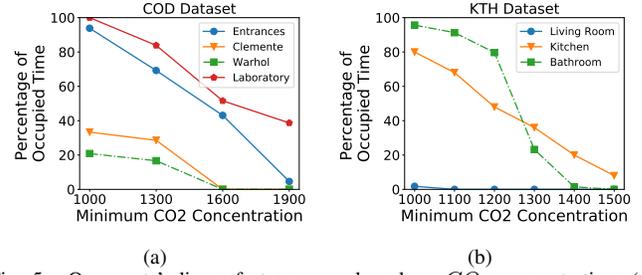


Fig. 5. Occupants' discomfort measure based on CO_2 concentration: (a) COD dataset and (b) KTH dataset.

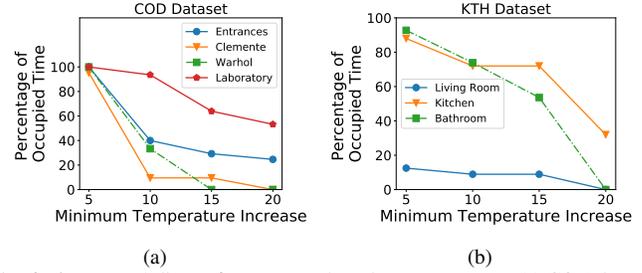


Fig. 6. Occupants' discomfort measure based on temperature: (a) COD dataset and (b) KTH dataset.

COD dataset says that almost 4% of the occupied time, CO_2 concentration in entrance zone exceeds 1900 ppm throughout the year while for laboratory zone it is almost 38%. Analysis of the KTH dataset indicates that 8% of the occupied time, the kitchen's CO_2 concentration exceeds 1500ppm.

Attack analysis on occupants' comfort attack shows that if an attacker has access to all sensor measurements of the zones, the temperature of the zones in entrance zone exceeds more than 20 °F almost 24.6% of the occupied time throughout the year while for laboratory zone it is almost 53.22%. Analysis of the KTH dataset indicates that during 32% of the occupied time, kitchen zone temperature exceeds more than 20 °F throughout the week. For the bathroom, it is almost 53.62% of the occupied time.

E. Scalability

We evaluate the scalability of BioTa framework by varying the sizes of the zones of the available dataset. The increase in the number of zones multiplies the number of constraints. The occupancy of the new zones follows the distribution of the available zones. The SMT solver takes significantly less time for SAT cases, as seen from Fig. 7. For the COD dataset, the SAT cases take 1.59, 3.14, 23.42, and 62.3 seconds respectively for 4, 8, 12, and 16 zones respectively, where for the UNSAT case it took 61.8, 285.1, 819.2, and 2389.2 seconds. For the KTH dataset, SAT cases take 1.02, 2.5, 10.82, and 25.6 seconds respectively for 3, 6, 9, and 12 zones respectively, where for the UNSAT case it took 34.8, 123.1, 345.7, and 1289.2 seconds. The addition of zones affects the solver's solving time almost exponentially, which proves that the solver is not scalable.

The scalability depends on the number of clauses. We analyze the complexity of our solver based on the number of clauses. Table VII shows the number of clauses for a

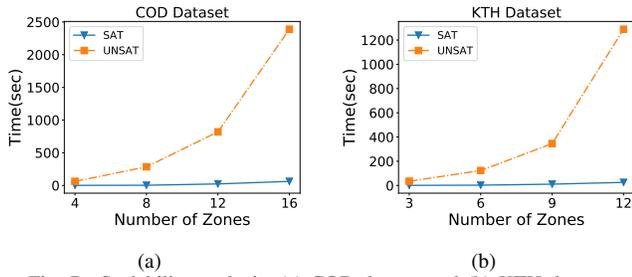


Fig. 7. Scalability analysis: (a) COD dataset and (b) KTH dataset.

TABLE VII
COMPLEXITY ANALYSIS OF BIOTA

Dataset	Number of Clauses		
	Control	Cost Calculation	Attack
COD	52	28	16
KTH	39	21	12

single zone. The addition of new zones adds an almost similar number of new clauses to the solver, which enlarges the solution domain significantly.

VII. CONCLUSION

The BIOT-based HVAC control system is gaining popularity because of its reliability, efficacy, and cost-efficiency. But our attack analysis on the smart building HVAC control system using the BIOTA framework suggests that exploitation of vulnerable sensor measurements of smart building HVAC control system can result in a significant increase in cost and raises health concerns of the occupants. Our proposed attack model is verified using two state-of-the-art building occupancy datasets. The COD dataset's evaluation results show that using an energy consumption attack, the HVAC control system can encounter an additional cost of \$300. We plan to study cyber attacks that exploit multiple smart building control systems, running independently, to create a deeper, cascaded impact.

REFERENCES

- [1] Encycle delivers instant energy savings with swarm logic®, our patented iot-enabled technology. <https://www.encycle.com/swarm-logic/>, 2020. Accessed: 2020-10-21.
- [2] Marcin Bajer. Iot for smart buildings-long awaited revolution or lean evolution. In *IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 149–154, 2018.
- [3] K. Akkaya, I. Guvenc, R. Aygun, N. Pala, and A. Kadri. Iot-based occupancy monitoring techniques for energy-efficient smart buildings. In *IEEE Wireless Communications and Networking Conference Workshops*, pages 58–63, 2015.
- [4] Yuebin Yu. Integrating air handling units in office buildings for high performance. 2010.
- [5] Target attack shows danger of remotely accessible hvac systems. <https://www.computerworld.com/article/2487452/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html>, 2014. Accessed: 2020-10-13.
- [6] Smart hvac systems vulnerable to being controlled by hackers through cyber attacks. <https://www.asmag.com/showpost/30716.aspx>, 2019. Accessed: 2020-10-13.
- [7] International Business Times India Ashok. Hackers leave finnish residents cold after ddos attack knocks out heating systems. <http://www.ibtimes.co.uk/hackers-leave-finnish-residents-cold-after-ddos-attack-knocks-out-heating-systems-1590639>, November 2016. Accessed: 2020-07-20.
- [8] Tao Lu, Xiaoshu Lü, and Martti Viljanen. A novel and dynamic demand-controlled ventilation strategy for co2 control and energy saving in buildings. *Energy and buildings*, 43(9):2499–2508, 2011.

- [9] K. Liu, E. Pinto, S. Munir, J. Francis, C. Shelton, M. Berges, and S. Lin. Cod: a dataset of commercial building occupancy traces. In *ACM International Conference on Systems for Energy-Efficient Built Environments*, pages 1–2, 2017.
- [10] Testbed kth sample data, gdpr compliance. <https://www.liveinlab.kth.se/en/projekt/2.90711/download-sample-datasheets-1.974705>. Accessed: 2020-05-21.
- [11] Cheng Yew Leong. Fault detection and diagnosis of air handling unit: A review. In *MATEC Web of Conferences*, volume 255, page 06001. EDP Sciences, 2019.
- [12] Gang Wang and Li Song. Air handling unit supply air temperature optimal control during economizer cycles. *Energy and Buildings*, 49:310–316, 2012.
- [13] Warm air heat temperatures & supply air temperature improvement. https://inspectapedia.com/heat/Warm_Air_Supply.php/. Accessed: 2020-06-21.
- [14] An assessment of energy technologies and research opportunities. <https://ohsonline.com/Articles/2016/04/01/Carbon-Dioxide-Detection-and-Indoor-Air-Quality-Control.aspx?Page=2>, 2015. Accessed: 2020-10-13.
- [15] D. Cali, P. Matthes, K. Huchtemann, R. Streblov, and D. Müller. Co2 based occupancy detection algorithm: Experimental analysis and validation for office and residential buildings. *Building and Environment*, 86:39–49, 2015.
- [16] Joseph Dyro. *Clinical engineering handbook*. Elsevier, 2004.
- [17] Andrew Persily and Lilian de Jonge. Carbon dioxide generation rates for building occupants. *Indoor air*, 27(5):868–879, 2017.
- [18] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. Hei. Trick or heat? manipulating critical temperature-based control systems using rectification attacks. In *ACM SIGSAC Conference on Computer and Communications Security*, pages 2301–2315, 2019.
- [19] AKM Newaz, Nur Intiazul Haque, Amit Kumar Sikder, Mohammad Ashiqur Rahman, and A Selcuk Uluagac. Adversarial attacks to machine learning-based smart healthcare systems. *arXiv preprint arXiv:2010.03671*, 2020.
- [20] JC Mace, C Morisset, K Pierce, C Gamble, C Maple, and J Fitzgerald. A multi-modelling based approach to assessing the security of smart buildings. 2018.
- [21] D. Meyer, J. Haase, M. Eckert, and B. Klauer. A threat-model for building and home automation. In *2016 IEEE 14th international conference on industrial informatics (INDIN)*, pages 860–866, 2016.
- [22] Q. Mustafa, A. Waleed, and V.S. Kharchenko. Ata-based security assessment of smart building automation systems. *Radioelectronic and computer systems*, (3):30–40, 2016.
- [23] A. Abdulmunem and V. Kharchenko. Availability and security assessment of smart building automation systems combining of attack tree analysis and markov models. In *Intl. Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, pages 302–307, 2016.
- [24] J. Hachem, V. Chiprianov, M. Babar, T. Khalil, and P. Aniorte. Modeling, analyzing and predicting security cascading attacks in smart buildings systems-of-systems. *Journal of Systems and Software*, 162, 2020.
- [25] Nur Intiazul 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. *arXiv preprint arXiv:2103.03472*, 2021.
- [26] The pennsylvania state climatologist. http://www.climate.psu.edu/data/city_information/index.php. Accessed: 2020-06-21.
- [27] Pennsylvania commercial electric rates. <https://www.electricrate.com/commercial-rates/pennsylvania/>. Accessed: 2020-06-21.
- [28] Electricity prices for households in sweden 2010-2019, semi-annually. <https://www.statista.com/statistics/418124/electricity-prices-for-households-in-sweden/>. Accessed: 2020-06-21.
- [29] Biota. <https://github.com/mtiazulhaque/research-implementations/tree/main/biota>, 2020.
- [30] Clark Barrett and Cesare Tinelli. Satisfiability modulo theories. In *Handbook of Model Checking*, pages 305–343. Springer, 2018.
- [31] 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.
- [32] Psypy project description. <https://pypi.org/project/psypy/>. Accessed: 2020-03-19.