

Biologically Inspired Safety and Security for Smart Built Environments: Position Paper

Denis Gračanin*, Adam D’Amico*, Mark Manuel*, Walter Carson*, Mohamed Eltoweissy[†] and Liang Cheng[‡]

*Department of Computer Science

Virginia Tech

Blacksburg, VA 24060, USA

Email: gracanin@vt.edu, admico77@vt.edu, mmark95@vt.edu, walterc@vt.edu

[†]Department of Computer and Information Science

Virginia Military Institute

Lexington, VA 24450, USA

Email: eltoweissymy@vmi.edu

[‡]Department of Computer Science and Engineering

Lehigh University

Bethlehem, PA 18015, USA

Email: cheng@cse.lehigh.edu

Abstract—In the era of emerging Smart Built Environments (SBEs), a smart house, unlike regular houses with static “components”, consists of numerous interconnected and often actuated devices, capable of executing tasks independent of user supervision. Living in such a SBE, where for example, the furniture can rearrange itself, and the doors open and close of their own volition, may be difficult and unpredictable. Furthermore, cybersecurity attacks and intrusion could allow attackers to assume control of the SBE, damage its components and to potentially harm its inhabitants. Such novel characteristics of SBEs present developers with several unique challenges with regards to implementing the needed safety and security measures and protocols that go along with them. With such environments, therefore, there is a need for a system that is capable of monitoring user activities in real-time, identifying the safety and security hazards to users in their immediate local context, warning users of these hazards, and perhaps even taking preventative and mitigative action against the hazards that it identified. In this paper, we survey some of these challenges and explore the design and implementation of a system designed around the safety and security of SBE inhabitants. We propose an approach to modeling SBE safety that combines the three laws of robotics and the swarm behavior model. We also present a preliminary prototype and discuss a case study.

Index Terms—Internet of Things, Smart Built Environment, safety, security

I. INTRODUCTION

A Smart Built Environment (SBE), like a smart house, augments the traditional home by adapting new technology into the existing patterns of use to provide a rich computational and communication infrastructure that provides services to its inhabitants. This infrastructure includes smart things, devices and sensors that can not only observe the physical environment, but also interact with the environment and its inhabitants in novel ways. However, the physical and social structures within a home are subject to continuous change that creates the need for reconfigurable spaces within the SBE.

The concept of Internet of Things (IoT) describes the pervasive presence of things or objects which use a unique addressing scheme to interact with each other and cooperate

with their neighbors to reach common goals. These physical objects have a social existence that could be supported through the IoT. Designing and deploying IoT into the SBEs provides infrastructure capacities that can change how SBEs behave and how users interact with them. IoT-enhanced SBEs can improve the lives of individuals, groups, and the broader community by enabling mobile, actuated, flexible and collaborative spaces. For example, a reconfigurable space requires reconfigurable objects (furniture, walls, lights, etc.) to adjust to changing floor plans and room sizes. This is something that can be accommodated by an SBE. While this has been an ongoing trend for office spaces, it is now becoming more relevant for residential spaces as well, especially for smaller apartments and houses. Residential SBEs could include reconfigurable social spaces for dining, entertainment or other activities. A major challenge then, is incorporating this spatial and functional reconfigurability within SBEs while supporting security and safety.

When multiple devices in the same space become a part of a network of connected devices, several issues that could affect user safety begin to arise. Almost everything within the SBE could be a smart device, from faucets to stoves to doors and windows. Because of the sheer number of devices that can act independently, there exists the very real possibility of actuators activating in such a way that they put the SBE inhabitants in harm’s way. Clearly, there is a need to ensure the prevention of such situations in a proactive and predictive fashion. The SBE infrastructure should be designed in a way to restrict certain actions from occurring within the house under the right circumstances. The main problem then, is to determine how to effectively use IoT to detect safety hazards before they occur and enforce safety rules to preemptively mitigate any damage they might cause, thereby, creating a much safer environment for the occupants.

A potential solution to this problem is to use biologically-inspired computation techniques. These techniques use animal behavior, communication methods, family structure and

features for inspiration, as similar features are often needed or observed by computing and networking systems in the physical world [1]. An example of this is the use of swarm intelligence for biologically-inspired computation [2]. In the context of the SBE (or smart home) we can provide ambient assisted living (AAL) while applying bio-inspired computing to leverage available information and communication technologies, for example to help seniors benefit from independent living [3].

We can go beyond computing and communication to leverage smart materials [4] and ecosystem biomimicry for design of SBEs [5]. While there has been significant recent interest in biologically-inspired security [6], the related safety efforts are limited. In the following sections we discuss some of the challenges, related work as well as recent biologically inspired approaches towards security and safety.

II. RELATED WORK

A. Safety

One of the major challenges when supporting safety is the process of getting, processing, and returning data quickly and efficiently. Since SBEs incorporate multiple devices, a single second can mean the difference between the prevention or the occurrence of a devastating safety hazard. When trying to keep the user safe, these systems must be designed in such a way that the time between sending data, processing the data, and returning a mitigative action is minimal. This not only concerns the backend side of the system, but also the physical world where the data is coming from. The real-time constraints and requirements of deeply embedded devices with limited resources can be addressed by virtualization [7]

A malfunctioning sensor could cause a failure in data transmission, which could potentially result in harm to the users. Similarly, the accuracy of the collected data is very important. If data collected by sensors is frequently inaccurate, then the actuator devices within the SBE could activate at inappropriate times, or not at all. There is a much broader context of building safer built and urban environments [8] where IoT-based solutions must be integrated on a larger scale.

Designing the SBE infrastructure to support safety poses developers with a significant challenge. This is because doing so requires a considerable knowledge of the components present within SBE, as well as the knowledge of how to process the data received from these devices. To keep inhabitants safe in a largely-automated environment, there need to be clearly established rules that the smart home can abide by to determine whether it is safe for a certain action to be performed at any given time. This requires the collection of a significant amount of data, and an expansive set of rules, to evaluate whether a safety threshold is broken. The processing of all this data in a timely manner is paramount to keeping the user safe. We need simulation and modeling tools that can inform the design process and evaluate IoT-based systems [9].

Household members interactions are expressed through sequences of practical actions. Those sequences identify domestic routines and communication characteristics that form

a locally produced system of communication. Such communications must be considered for design and the deployment of new computing devices and applications in the home [10]. Usability of end-user composition interfaces for SBEs play an important role in safety consideration. Some of the factors include predictability of composition model, readability of composition representation, overview and means for planning compositions, and attractiveness and desirability [11]. When dealing with smart things like smart appliances, usefulness is the strongest predictor for the intention to use. However, the emotional response of the inhabitant user is also an important explanatory variable [12]. These indicators can be used to inform the safety features.

An example of a biologically-inspired approach is a dynamic stereo vision sensor can be integrated into an alarm, security, and monitoring system for the seamless analysis and tracking of elderly persons' behavior at home. This real-time information can be utilized towards incident detection (e.g., fall detection), and instantaneous alarming the concerned parties [13]. Another example includes telehealth services [14].

B. Security

The IoT-based infrastructure for SBEs has requirements that are not directly supported by the Internet. A huge number of devices and resources connected to the Internet form the Internet of Things (IoT). Those devices and resources can be grouped together to create new self-regulating IoT applications such as SBE [15]. Such grouping of devices and resources (things) is more general and complex due to specific challenges. Those challenges include “*heterogeneity of devices, diversity of protocols, variety or none established standards, self-manageability, self-organization, dynamic architectures, mobility, intermittent availability, distributed computing, security and privacy*” [16]. Future Internet of Things (FIoT) is emerging concept that indicates development and inclusion of new techniques into IoT. An overview of IoT and FIoT, the use of computational intelligence to FIoT and swarm optimization inspired intelligent data management framework [17].

IoT security solutions must support different IoT platforms and large number device and resources, as well as the interactions that take place between devices and users. In doing so, protecting user privacy is essential since personal information, including preferences, actions, pattern of behaviors, will be used to customize user interactions with IoT-enabled systems. IoT implementations must include mechanisms that protect and monitor personal data, both locally (devices, services) and in the cloud. Some of the threats and concerns for security and privacy arising from IoT services, as well as approaches to solve these security and privacy issues in the industrial field, are described in [18].

Due to the distributed nature of IoT-based systems, security mechanisms are usually decentralized. However, with the proliferation of IoT systems there is an increased risk of security attacks that can have very serious consequences, for example, safety violations and physical injuries to inhabitants

in SBEs. Humans beings and animals have developed many natural forms of protection for survival. Those biological instincts and predispositions can be replicated and applied to cyber security systems to enhance a system's resilience in the face of an attack [19]. Therefore, there are similarities between the biological phenomenons and the operations of the IoT systems that can be used to develop biologically inspired models for security mechanisms for IoT-based systems. Various biologically-inspired approaches to security in IoT and significant findings, as well as a brief illustration of research gap for various robust and computationally efficient security techniques in IoT is provided in [20].

There are many routing algorithms for efficient communications within wireless networks and IoT. It is possible to investigate of biological systems, such as ant colonies, to improve the route selection mechanisms in such networks. An example of such approach is EICAntS (Efficient IoT Communications based on Ant System) [21]. Existing service discovery and selection approaches rely mostly on centralized architectures. However, such approaches do not work well for the IoT-based systems. Biologically-inspired computing paradigms have emerged due to their inherent capability to operate without any central control and thus work well when decentralization of decision-making is necessary. An example of such an approach is the biologically-inspired Response Threshold Model [22]. Many cybersecurity projects can benefit from implementing different nature-inspired solutions [6].

III. APPROACH

While there is an emerging emphasis on IoT security, the safety aspects are not yet addressed at the same level. Therefore, in the proposed approach we start with the safety requirements and then describe the corresponding security implications. Without proper security, the safety of an IoT-based SBE cannot be guaranteed.

A. Safety

Merriam-Webster dictionary defines safety as “*the condition of being safe from undergoing or causing hurt, injury, or loss*” as well as “*a device (as on a weapon or a machine) designed to prevent inadvertent or hazardous operation*”. The safety related factors can act on different time scales:

- Short-term: a movement of a automated door can result in almost instantaneous injury.
- Medium-term: a build of carbon monoxide could, over a period of time, result in a serious health issues or death.
- Long-term: an elevated presence of radon can over time result in lung cancer.

The safety requirements apply not only to the inhabitants but also to the SBE they live in. Due to mobility and reconfigurability of SBE components, it is possible to cause damage to the SBE.

Here we consider the three laws of robotics created by Isaac Asimov and their modifications [23]:

- 1) *A robot may not injure a human being or, through inaction, allow a human being to come to harm.*

SBE state/configuration space

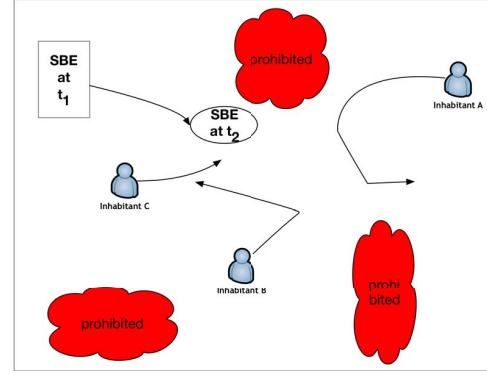


Fig. 1. An illustration of the swarm behavior model and three laws of SBE safety. The SBE navigates in the SBE state space avoiding inhabitants (the first law). A request from an inhabitant can change the SBE trajectory as long as all inhabitants are avoided (the second law). The SBE must avoid prohibited areas in the SBE state space unless to avoid inhabitants (the third law). The position and shape of the SBE in the SBE state space changes over time (e.g., from t_1 to t_2) reflecting the change in the SBE configuration.

- 2) *A robot must obey orders given it by human beings except where such orders would conflict with the First Law.*
- 3) *A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.*

In that context an SBE is a distributed robotics system and the three laws of SBE safety can be formulated as:

- 1) An SBE may not injure an inhabitant or, through inaction, allow an inhabitant to come to harm.
- 2) An SBE must obey viable service requests given it by inhabitants except where such orders would conflict with the First Law.
- 3) An SBE must protect its own existence as long as such protection does not conflict with the First or Second Law.

As with the laws of robotics, in a general case, an inhabitant can intentionally damage or destroy the SBE without harming inhabitants. Therefore, the SBE designers must include some protection mechanisms that define what is a viable service request given the SBE state.

Fundamentally, these laws can be viewed as obstacle avoidance requirements in the SBE state space (includes spatial, temporal, environmental and other attributes/dimensions). SBEs are distributed, “multi-robotics” systems with autonomous mobile components. Mobile robotics can be applied to create automated, self-moving furniture components that can be controlled, coordinated and configured based on the actions taking place in SBEs [24]. An example of a self-reconfiguring modular robotic system are Roombots that can move in their environment and that change shape and functionality during the day [25].

We can use swarm behavior as a biologically inspired model. Such behaviors are demonstrated by flocks of birds, schools of fish, and swarms of insects have been used for

distributed network of mobile sensor platforms [26] and can be used for SBEs. The combination of three laws of SBE safety with swarm behavior model provide a foundation for the SBE safety, as illustrated in Figure 1.

The first law of SBE safety essentially considers a human being as an obstacle that needs to be avoided in the real-time in the SBE state space. For that, the SBE needs to track all human beings within its reach when performing autonomous actions or maintenance. The tracking is based on human traits, particularly the static, intrinsic traits, that are the “ground truth” that can be used to determine occupancy and location [27]. A robot control framework can be based on biological data (spinal-cord stimulation in frogs) and human behavior to empirically describes how human beings avoid obstacles [28].

The second law of SBE safety means that the SBE must provide requested services to inhabitants as long as meeting the requests does not violate the first law for any inhabitant. That means that the SBE must avoid multiple obstacles in the SBE state space.

The third law of SBE safety means that the SBE must avoid damaging its infrastructure (e.g., a collision between two mobile components) as long as it does not conflict with the first or second law. The same swarm behavior model can be used [26] for requested SBE services while providing safe separation between SBE components.

The real-time obstacles (inhabitants, SBE damage) avoidance in the SBE state space is achieved by adjusting the trajectory using the swarm model that also results in the change of the SBE shape. The examples of shape change include physical attributes (re-arranging mobile components), environmental attributes (air quality), and others.

There are three basic controlling behaviors describing swarm particles movements [26] in the swarm model, separation, alignments, and cohesion. Separation describes avoiding collisions with nearby particles. Alignment describes matching velocity with nearby particles. Cohesion describes staying close to nearby particles. As a consequence, the swarm formation remains stable even in a dynamic environment.

B. Security

This model of SBE safety depends on the ability to continuously, reliably and accurately collect and process data and control its components. Any security breach can interfere with the SBE’s ability to follow the three laws. In Section I IoT was identified as the enabling technology for SBE infrastructure. IoT security is an emerging discipline that must take into account all components, including people, infrastructure, things, processes, and data. There are several layers of IoT security, including firewalls, intrusion detection systems, policies, the rules, regulations, and procedures (remote access, physical security, password policies, education, training, and awareness). We need to reexamine the whole idea of security and leverage the biologically-inspired approach, as described in Section II.

Securing IoT is different from traditional security due to additional challenges such as social engineering attack

or inferring information (also compromising privacy). Furthermore, manufacturers often release new devices, without proper testing so many have critical flaws. It is imperative to test for vulnerabilities and consider security risk before SBE implementation. Designing IoT security must include confidentiality, integrity and availability as first principles. Confidentiality means that the data should not be accessible to anyone without appropriate permissions. Integrity means that the code should be stable and not mutable to anyone without appropriate permissions. Availability means that the device should be available to anyone with appropriate permissions.

C. Performance

The SBE safety performance can be measured. Some of the swarm performance metrics proposed in literature [26] use connectivity and coverage efficiency. Connectivity describes swarm particle separation distance and coverage efficiency describes the ability of a swarm to efficiently cover a region.

One of the critical underlying factors determining the overall safety characteristics and performance are the characteristics of the SBE communication infrastructure. Network latency and its variability (jitter) introduce uncertainty in the timing of the collected data samples and the performed actions. In terms of the SBE state space, latency increases the effective volume of obstacles thus reducing the operating envelope of the SBE. If latency is large enough, the SBE will no longer provide safety. In terms of the swarm model, the swarm particles have reduced ability to maintain separation, alignments, and cohesion thus diminishing connectivity and coverage efficiency.

IV. PROTOTYPE SBE SAFETY TESTBED

Implementing an IoT-based SBE involves interconnecting a variety of devices, some of which with limited resources, through a communication network. Those devices rely on some communication protocol to exchange messages over the network. Different IoT applications tend to have different safety requirements, which in turn imply different QoS requirements that need to be met by the communicating devices. Several lightweight communication protocols are used in IoT-based systems, such as MQTT Protocol and the Constrained Application (CoAP) Protocol [29].

We describe a proof-of-the concept SBE safety testbed that can be used to design and model SBEs as well as to test the actual systems. We use the MQTT protocol as representative communication protocol for the IoT systems. However, other protocols can be used instead.

We created an example that models SBE safety in a simulated small physical environment, a kitchen (Figure 2 top). The example is based on an SBE prototype currently under development. Figure 3 shows the previous version of the kitchen module. The SBE system (swarm) contains several SBE components (swarm particles) that includes various sensors and actuators installed in individual components (represented as circles). The SBE components (sensors and actuators) are modeled using Node-RED [30] (Figure 2 bottom).

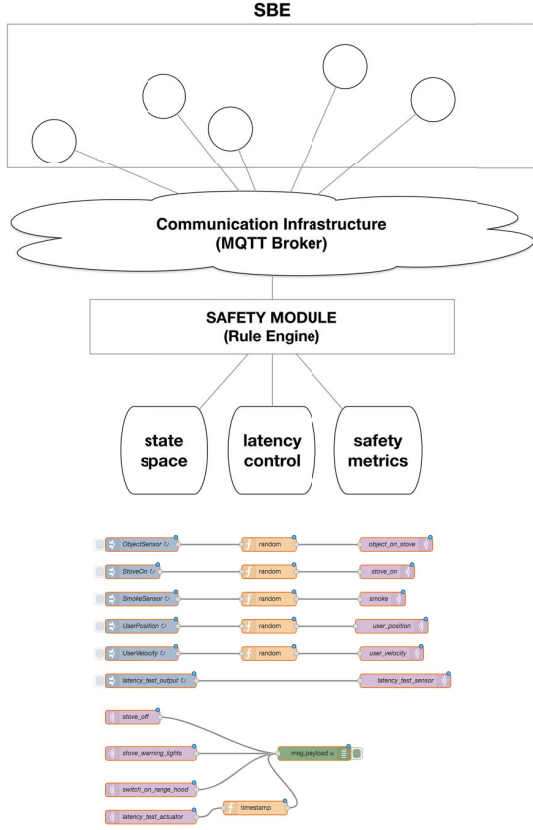


Fig. 2. **Top:** A proof-of-the concept implementation of the SBE safety testbed. The MQTT Broker provides support for security and Quality of Service requirements. The Safety Module monitors the messages and updates the state space information accordingly. The latency control allows the Safety Module to control network characteristics by introducing additional delay in the MQTT Broker. The safety metrics determine the corrective actions of the Safety Module. **Bottom:** An example of a Node-RED configuration for the kitchen module simulation.



Fig. 3. A previous version of the SBE's kitchen module. Cabinet doors in different configurations.

The sensors provide data to the MQTT Broker about the state of the environment and its users [31]. The actuators will respond to messages from the MQTT broker and affect the state of the environment to provide services to inhabitants or to react to safety hazards. In the case of an actual SBE, the SBE components communicate using MQTT protocol.

In Node-RED, multiple sensors were implemented, includ-

ing inhabitant position trackers and a sensor to detect the state of the SBE components. These sensors publish data about their state to the MQTT Broker just like physical sensors in the house would. A few actuators were also implemented in Node-RED. These included actuators to halt and alter the motion of moving SBE components, such as opening/closing of warmer drawer, cabinets and refrigerator doors.

The MQTT Broker receives messages that are published to it and passes the messages on to any devices that are subscribed to the topic of the message. It uses a publish/subscribe model that provides for authentication and security.

The Safety Module (a rule engine) contains all the logic of the safety rules that the SBE enforces. The logic for the Safety Module is based primarily around the three laws of SBE safety and can easily be expanded upon, i.e., new rules and hazard conditions can easily be added and safety measures updated.

The Safety Module subscribes to all the sensor data topics on the MQTT Broker. When it receives a message containing new sensor data, the Safety Module updates the state space information, which represents the state of the environment, and checks for any safety violations. If it detects such violation, the Safety Module will publish the corrective action (message) to the MQTT Broker. That message is intended to be consumed by an actuator that will fix the safety violation.

For example, if the Safety Module receives a message that a moving inhabitant has been detected, while SBE components are moving in the same space, it would identify this as a hazard condition and publish a warning message to the broker. The MQTT Broker will pass on this message to the actuators that subscribe to it, which cause the moving SBE components to cease their activity, until the space is clear of the human inhabitant.

With the MQTT Broker on the same computer or local network, the latency introduced by the MQTT infrastructure is small, 2-3 ms, thus having minimal effect on the safety performance. However, in real-world SBE system that are cloud based, the latency is much higher. We tested the latency using a cloud based implementation, which gave us insight into the kind of response time threshold that we would require for the system to be effective. We performed our latency testing by having sensors in Node-RED publish a timestamped start value to the broker. The Rule Engine then subscribed to this topic and published a message back to the broker under a different topic name.

These messages from the Safety Module were subscribed to a local actuator via Node-RED. This actuator client then obtained the difference between the original timestamp value from the publishing sensor and the current time, upon receipt of the message from the Safety Module, to get the overall latency of one message through the system. The average latency was around 400ms. However, we also noted a rather high variance (jitter) in these values; they ranged from under 200ms to 1000ms. This significantly reduced the safety margins. As a consequence, we added the latency control to the Safety Module used to introduce additional latency in the MQTT Broker thus changing the effective communications

performance. That allows for testing various network scenarios in terms of latency and jitter for individual SBE components and message types.

In this example the state space was limited to the spatial attributes (and time). That allows the direct use of the results from [26] to determine connectivity and coverage efficiency for different network scenarios and different scenarios of SBE use by the inhabitants.

V. CONCLUSION

We presented challenges faced by IoT-based SBEs related to the design and implementation of a system designed around the safety and security of SBE inhabitants. While there is an emerging emphasis on IoT security, the safety aspects are not yet addressed at the same level. We proposed an approach to modeling SBE safety that combines the three laws of robotics and the swarm behavior model. Safety is maintained by the real-time obstacle (inhabitants, SBE damage) avoidance in the SBE state space by adjusting the trajectory and the shape of the SBE in the state space. A preliminary, proof-of-the-concept implementation is described. The future work will focus on formalizing the proposed model to support more general SBE state space for a SBE safety and security testbed that can inform the design of an SBE with fully functional safety and security features. The ongoing SBE development will provide ground truth and allow for iterative improvements of the SBE testbed based on real-world testing.

REFERENCES

- [1] Y. Xiao, Ed., *Bio-Inspired Computing and Networking*. Boca Raton, FL: CRC Press, 2016.
- [2] X.-S. Yang, Z. Cui, R. Xiao, A. H. Gandomi, and M. Karamanoglu, *Swarm Intelligence and Bio-Inspired Computation*. Elsevier, 2013.
- [3] M. R. Miller, *My Smart Home for Seniors*. Que, 2017.
- [4] E. K. Petrovic, B. Vale, and M. P. Zari, *Materials for a Healthy, Ecological and Sustainable Built Environment*. Woodhead Publishing, 2017.
- [5] M. P. Zari, "Mimicking ecosystems for bio-inspired intelligent urban built environments," *Intelligent Buildings International*, vol. 8, no. 2, pp. 57–77, 2016.
- [6] M. Choraś, R. Kozik, and I. Maciejewska, "Emerging cyber security: Bio-inspired techniques and MITM detection in IoT," in *Combating Cybercrime and Cyberterrorism*, ser. Advanced Sciences and Technologies for Security Applications, B. Akhgar and B. Brewster, Eds. Cham: Springer, 2016, pp. 193–207.
- [7] F. Bruns, D. Kuschnerus, and A. Bilgic, "Virtualization for safety-critical, deeply-embedded devices," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*. New York: ACM, 2013, pp. 1485–1492.
- [8] M. Stevenson, "Building safer environments: injury, safety, and our surroundings," *Injury Prevention*, vol. 12, no. 1, pp. 1–2, Feb. 2006.
- [9] G. Brambilla, M. Picone, S. Cirani, M. Amoretti, and F. Zanichelli, "A simulation platform for large-scale Internet of Things scenarios in urban environments," in *Proceedings of the First International Conference on IoT in Urban Space*. Brussels: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2014, pp. 50–55.
- [10] A. Crabtree, "Design in the absence of practice: Breaching experiments," in *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*. New York: ACM, 2004, pp. 59–68.
- [11] Y. Dahl and R.-M. Svendsen, "End-user composition interfaces for smart environments: A preliminary study of usability factors," in *Design, User Experience, and Usability. Theory, Methods, Tools and Practice*, A. Marcus, Ed. Berlin, Heidelberg: Springer, 2011, pp. 118–127.
- [12] M. Rothensee, "User acceptance of the intelligent fridge: Empirical results from a simulation," in *The Internet of Things*, C. Floerkemeier, M. Langheinrich, E. Fleisch, F. Mattern, and S. E. Sarma, Eds. Berlin, Heidelberg: Springer, 2008, pp. 123–139.
- [13] A. N. Belbachir, T. Lunden, P. Hanák, F. Markus, M. Böttcher, and T. Mannesola, "Biologically-inspired stereo vision for elderly safety at home," *e & i Elektrotechnik und Informationstechnik*, vol. 127, no. 7–8, pp. 216–222, Aug. 2010.
- [14] Z. Mahmood, H. Ning, A. Ullah, and X. Yao, "Secure authentication and prescription safety protocol for telecare health services using ubiquitous IoT," *Applied Sciences*, vol. 7, no. 10, pp. 1–22, 2017.
- [15] N. M. do Nascimento and C. J. P. de Lucena, "FioT: An agent-based framework for self-adaptive and self-organizing applications based on the Internet of Things," *Information Sciences*, vol. 378, pp. 161–176, 2017.
- [16] A. Zakriti and Z. Guennoun, "Service entities model for the internet of things: A bio-inspired collaborative approach," in *Proceedings of the 2011 International Conference on Multimedia Computing and Systems*, Apr. 2011, pp. 1–5.
- [17] C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, "Future Internet of Things: Open issues and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2201–2217, Nov. 2014.
- [18] Y. H. Hwang, "IoT security & privacy: Threats and challenges," in *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security*. New York: ACM, 2015, pp. 1–1.
- [19] A. Guthikonda, E. Al-Shaer, A. Farooq, and M. Y. A. Raja, "Bio-inspired innovations in cyber security," in *Proceedings of the 14th International Conference on Smart Cities: Improving Quality of Life Using ICT IoT (HONET-ICT)*, 9–11 Oct. 2017, pp. 105–109.
- [20] R. Banu, G. F. A. Ahammed, and N. Fathima, "A review on biologically inspired approaches to security for internet of things (IoT)," in *Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 3–5 Mar. 2016, pp. 1062–1066.
- [21] S. Hamrioui and P. Lorenz, "Bio inspired routing algorithm and efficient communications within IoT," *IEEE Network*, vol. 31, no. 5, pp. 74–79, 2017.
- [22] E. Rapti, C. Houstis, E. Houstis, and A. Karageorgos, "A bio-inspired service discovery and selection approach for IoT applications," in *Proceedings of the 2016 IEEE International Conference on Services Computing (SCC)*, Jun. 2016, pp. 868–871.
- [23] R. R. Murphy and D. D. Woods, "Beyond Asimov: The three laws of responsible robotics," *IEEE Intelligent Systems*, vol. 24, no. 4, pp. 14–20, Jul. 2009.
- [24] A. Yuliana, O. Felipe, S. Byron, L. Liliana, and V. Andres, "Configuration of work environments with smart furniture," in *Proceedings of the III International Congress of Engineering Mechatronics and Automation (CIIMA)*, Oct. 2014, pp. 1–5.
- [25] A. Spröwitz, R. Moeckel, M. Vespignani, S. Bonardi, and A. J. Ijspeert, "Roombots: A hardware perspective on 3D self-reconfiguration and locomotion with a homogeneous modular robot," *Robotics and Autonomous Systems*, vol. 62, no. 7, pp. 1016–1033, 2014.
- [26] B. A. Kadrovach and G. B. Lamont, "A particle swarm model for swarm-based networked sensor systems," in *Proceedings of the 2002 ACM symposium on Applied computing*. ACM Press, 2002, pp. 918–924.
- [27] Y. Benezeth, H. Laurent, B. Emile, and C. Rosenberger, "Towards a sensor for detecting human presence and characterizing activity," *Energy and Buildings*, vol. 43, no. 2–3, pp. 305–314, 2011.
- [28] H. Hoffmann, P. Pastor, D.-H. Park, and S. Schaal, "Biologically-inspired dynamical systems for movement generation: Automatic real-time goal adaptation and obstacle avoidance," in *Proceedings of the 2009 IEEE International Conference on Robotics and Automation*, 2009, pp. 2587–2592.
- [29] D. Thangavel, X. Ma, A. Valera, H.-X. Tan, and C. K.-Y. Tan, "Performance evaluation of MQTT and CoAP via a common middleware," in *Proceedings of the 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*. IEEE, 21–24 Apr. 2014, pp. 1–6.
- [30] JS Foundation, "Node-RED: Flow-based programming for the Internet of Things," <https://nodered.org/>, JS Foundation, last accessed 29 Jan. 2018.
- [31] M. Arlitt, M. Marwah, G. Bellala, A. Shah, J. Healey, and B. Vandiver, "MQTT version 3.1.1 plus errata 01," OASIS, Standard, 10 Dec. 2015.