Towards a Model and Graph Representation for Smart Homes in the IoT

Amir Modarresi[*] and James P.G. Sterbenz[*†]
amodarresi@ittc.ku.edu, jpgs@{ittc.ku.edu|comp.lancs.ac.uk}

[*]Information and Telecommunication Technology Center
Electrical Engineering and Computer Science
The University of Kansas, Lawrence, KS 66045, USA
https://www.ittc.ku.edu/resilinets

[†]School of Comp. and Comm. (SCC) and InfoLab21
Lancaster University, LA1 4WA, UK

***Abstract*—A key aspect of the emerging Internet of Things is *resilience*, as life- and mission-critical services are incorporated. In contrast to the current emphasis on IoT network protocols and services, in this paper we take steps towards analyzing resilience by focusing on a smaller subset of the smart city: smart-home network-infrastructure resilience. We present a model smart home that we believe will be typical in the near future, and examine its network structure and vulnerable technologies, links, and nodes quantified as betweenness centrality. We then propose two novel graph representations to capture the importance and interdependence of particular technologies, such as the 802.11 core, 802.15.4/ZigBee IoT smart devices, and LTE/4G/5G access links: the *end-system technology graph* and *technology interdependence graph*. A preliminary analysis indicates the importance of a biconnected 802.11s mesh core and diverse Internet access paths so that mission-critical devices and services remain operational.**

***Index Terms*—Future Internet of Things (IoT) resilience, survivability model; wireless smart city, biconnected home network centrality; 802.11s, 802.15.4, Zigbee, LTE / 4G / 5G heterogeneous protocols, technology interdependence graph**

I. Introduction

The initial aim of the Internet of Things (IoT) [1], [2], [3], [4] is connecting “things” to the Internet, to control them from anywhere, for applications such as environmental control, security and safety, and entertainment. This has resulted in a significant market of things for business and household customers. Utilizing things such as sensors in a house to control resources, including water, electricity, and natural gas, promoting safety and security, and providing greater convenience for the residences is the idea of a smart home and a smart building. Hence, we observe rapid growth in the number of nodes [5] along with the diversity and heterogeneity of the protocols and networks at the edge of the Internet. This is due to the fact that various protocols should be used for different purposes to fulfill smart home requirements. The range of these protocols varies from IEEE 802.11 wireless LAN (WLAN) and 802.3 Ethernet for high bit rates and interactive applications to 802.15.4/ZigBee [6], [7], Bluetooth [8], and Z-wave [9], [10] for low bit rate and low energy consumption needs. Moreover, other very-low bit-rate and long-range protocols such as LoRaWAN [11], Sigfox [12], [13], and NB-IoT [14] add extra heterogeneity and thus more complexity to the edge networks.

While the current research and development focus is on enabling and implementing IoT service functionality, our lives are getting more dependent on the Internet and its related infrastructures. Consequently, other networking aspects such as resilience (including survivability, disruption tolerance, and security [15]) should be considered. Lack of network resilience and security may lead to life-threatening incidents in services such as healthcare and self-driving vehicles. Unfortunately, examples of such incidents are increasing in various domains such as the cracking of the Nest thermostats [16] to independent infrastructure failures [17], [18].

Many studies have been performed on the topology of the Internet for a better understanding of its behavior in response to various challenges. Presenting a detailed map for the Internet is impossible due to the size, lack of information from the Internet service providers (ISPs), and dynamic behavior. In contrast, the study of the network in a smart home is more tractable due to its small size. In this paper, we present a new model for smart home resilience against targeted attacks to facilitate later resilience analysis.

The rest of this paper is organized as follow. In Section II, we explain some of the related work. We present our model for a smart home in Section III. In Section IV, we provide our new graph theoretic technology representations. Finally, we conclude our paper in Section V.

II. Background and Related Work

Though the IoT is evolving rapidly, to the best of our knowledge there is no standard model to explain every aspect of this complex ecosystem. IEEE has an active interest group P2413, toward introducing a standard model [1]. The previous IEEE model is only a simple abstract three-tiered model including sensing objects at the bottom, a communication network, and applications at the top level [19]. Other models including ITU Y.2060 [2] focus on connecting physical entities to logical counterparts without considering communication networks. IoT-A [20], presents data flows in the IoT system, while the Cisco model [5] concentrates on various entities that process data from the physical world to the cloud.

Other specialized models concerning a single aspect of the IoT system are available. Some of them that consider the placement of edge computing include the OpenFog model [21], [22] as a continuüm of computing from the cloud to things, mobile cloud computing (MCC) [23], [24], cloudlet [25], and mobile edge computing (MEC) [26]. We have introduced a multilevel model to present the complexity of the IoT network suitable to study network resilience for smart cities [27].

Other models and frameworks have been introduced to improve the privacy and security of smart homes. One of the frameworks presents risks associated with devices at home that focus on human assets, security goals, and device features [28]. In another overview, security features of the common protocols used in the smart home are reviewed [29].

EPIC [30] shifts the focus to prevent attackers from learning encrypted traffic patterns in smart homes and introduces another framework to preserve the privacy of traffic in smart communities.

Though security is one attribute to improve the network resilience in the sense of self-protection [15], in this paper, we concentrate on the network structure of smart homes to provide dependable and resilient service.

III. Smart Home Model

In this section, we present our model for a smart home that can be used to study network resilience. First, we define resilience as *the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to the normal operation* [15], [31]. Challenges are categorized into various groups including target and scope [32] such that they cover all challenges with the impact on nodes and links of network infrastructure.

Figure 1 illustrates our abstract model of a typical smart home. In this model, various protocols are employed to fulfill the requirement of different services from interactive applications with high bit rate and low delay such as video streaming, to low bit-rate sensors such as ambient light and thermal sensors. The conventional wireless protocols running in a smart home are IEEE 802.11, IEEE 802.15.4/ZigBee, Bluetooth, as well as new protocols such as Z-Wave and LoRaWAN. The topology of these protocols varies from a star as the dominant model to mesh. Though mesh topologies extend the network coverage and path diversity, they impose the additional complexity of the routing protocol and computational power in mobile networks, and consequently may drain more energy in battery operated nodes.

IEEE 802.11 in infrastructure mode presents a star topology while IEEE 802.11s [33], [34] utilizes a routing protocol at the link layer to provide a mesh topology. IEEE 802.15.5 provides mesh capabilities for IEEE 802.15.4. Alternatively, ZigBee builds a mesh over 802.15.4 running its own routing protocol. Bluetooth uses a piconet with a master/slave architecture in a star topology. In addition, Bluetooth Low Energy is able to construct a mesh topology. The nodes in the network are capable of changing their roles from master to slave and vice versa to extend the range. Z-wave also builds a mesh topology managed by a controller with source routing.

In addition to the various topologies, many of the protocols used at the edge network utilize their own native protocol stack including Bluetooth, ZigBee, and Z-wave. Therefore a gateway is required to interconnect with IP to be accessible through the Internet. Consequently, any failure of the gateway results in loss of accessibility of that specific network through IP. Nevertheless, the isolated network should still be operational. In our model, we show a gateway with the name of its native protocol on its icon such as “Z 15.4” for 802.15.4/ZigBee. While in the real world of smart homes, any manufacturer may build a separate hub to manage nodes of that particular native protocol and convert the native protocol to IP, hubs that support multiple protocols are available.

Given our abstract model illustrated in Figure 1, we define a graph $\mathbb{G} = (V, E)$ as the connectivity graph of the model, such that v_i is a device in the model with a transceiver of a particular protocol and e_n is a communication link between two adjacent nodes v_i and v_j. Figure 2 illustrates the connectivity graph $\mathbb{G}$ associated with our model. We use different colors for each type of link. In addition, the thickness of edges represents the value of betweenness centrality, which measures the importance of an edge quantified as the number of traversing shortest paths.

Path redundancy and diversity are features that improve network resilience [35], [36]. On the other hand, heterogeneity provides diversity in mechanism. As observed in our model and its corresponding graph, the heterogeneity of protocols consists of various WAN paths providing redundancy of Internet access and diversity of networks. In our model, the smart home can access the Internet through one of the conventional end-user connection methods such as DSL or cable. In addition, cellular links can provide a second path to the Internet through LTE/4G/5G protocols. The low-power wide-area network (LPWAN) protocols such as LoRaWAN and Sigfox provide another path. If each of these WAN protocols establishes a connection to a different local ISP, then the diversity of the providers increases the network resilience. Consequently, any local targeted challenges such as a cable-cut or denial of service (DoS) attacks against the local ISP does not disrupt the other paths. This property is expanded if the local ISPs do not share the same upstream provider. However, one concern about the LTE/4G/5G tethered connections through cell phones is that the links are available only when the mobile user is at home. Therefore, we should consider these paths temporary unless a fixed LTE/4G/5G modem is installed. For the same reason, any mission-critical sensors such as smoke detectors and alarm systems should not rely on such temporary links. On the other hand, the LPWAN protocols do not have the LTE limitation as mentioned above, since they do not depend on a user being physically present. Hence, such protocols may be a better candidate for low bit-rate, mission-critical sensors.

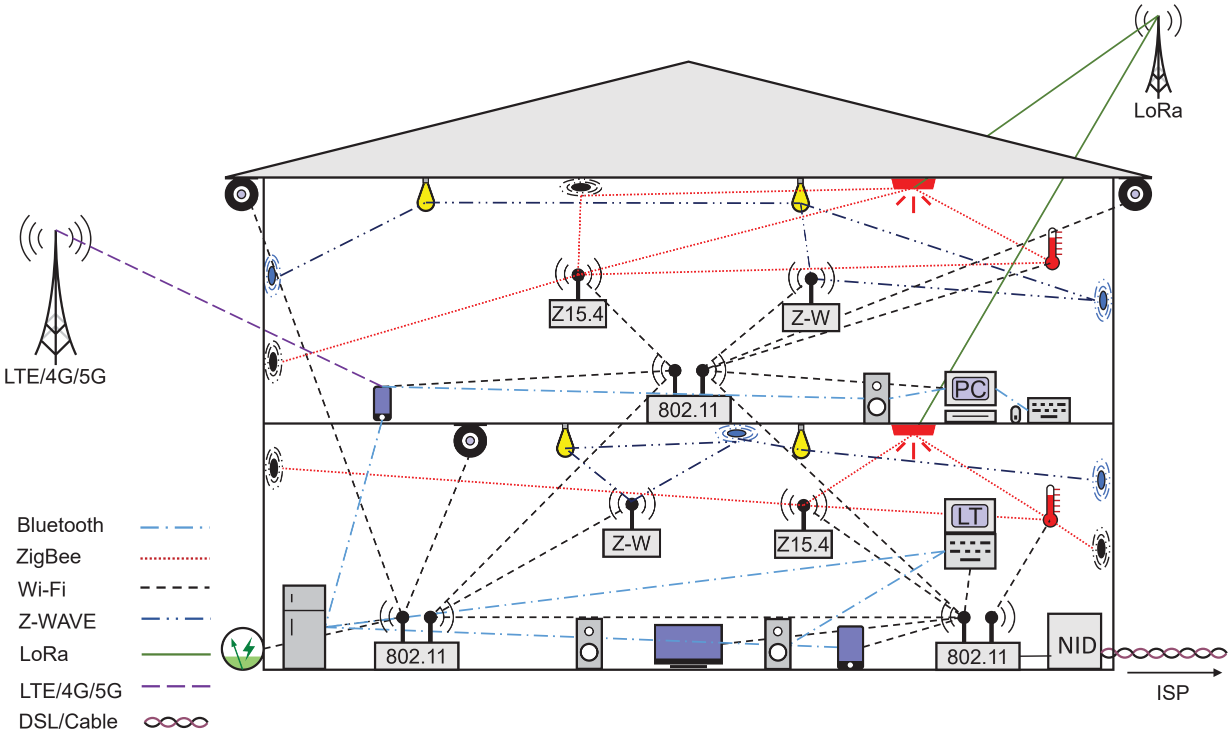

Fig. 1. Smart home model

As illustrated in Figure 1, the model uses several common Internet access technologies. Other protocols may be used to extend the smart home accessibility based on the availability of the services. For example, IEEE 802.11ah supports a lower bit rate but with wider coverage than other members of the 802.11 family, and it is suitable for battery-operated sensors and meters. Another option is conventional variants of IEEE 802.11 (e.g. 11n, 11ac) if the house is located in a smart city with city-wide wireless Internet coverage.

IV. Graph Theoretic Technology Representation

In this section, we present our new graph models of the smart home that represent the network infrastructure connectivity and protocol relationships. These models will enable our future work on graph theoretic resilience analysis as in [37], [38].

As illustrated in Figures 1 and 2, various network technologies and their corresponding protocols are represented in the model. Therefore, we construct another graph to show the relationship of nodes to a particular technology. In this graph, one group of nodes represents technologies in the model, and the other group represents end systems that use a specific type of technology protocol. Obviously, an end system with an interface of a particular technology has a direct connection to the corresponding protocol technology vertex. If an end system has more than one type of interface such as cell phones equipped with LTE, 802.11, and Bluetooth, they have more than one edge to the corresponding vertices. Therefore, given our abstract model, we define each element of the incidence matrix B with size $n \times t$ where n is the number of end systems in the model and t is the number of technologies as follows

$$b_{ij} = \begin{cases} 1 & \text{when node } i \text{ has interface type } j \\ 0 & \text{otherwise} \end{cases}$$

Figure 3 illustrates the *end-system technology graph* associated with the matrix B. This graph shows how various link technologies interconnect the devices including gateways that support more than one protocol stack. The thickness of the edges, drawn and calculated by Cytoscape [39], represents the value of edge betweenness centrality. As expected, gateways, the access point connected to the Internet, and the cell phone providing tethering are on the most critical paths. In other words, any failure of these nodes has more effect on the network connectivity.

We also calculate the *one-mode projection* [40] of matrix B, using the Python NetworkX library [41], to obtain the direct adjacencies between vertices of each technology, represented as the *technology interdependence graph* shown in Figure 4. There is a high degree centrality of 802.11 WLAN to other technologies, since it provides the backbone of this model smart home. Hence, if only one access point is used in the network, its failure partitions the network. If IEEE 802.11s is used as illustrated in Figures 1 and 2, multiple access points construct a mesh topology. In this case, a failure of one of the access points may cause the disconnection of

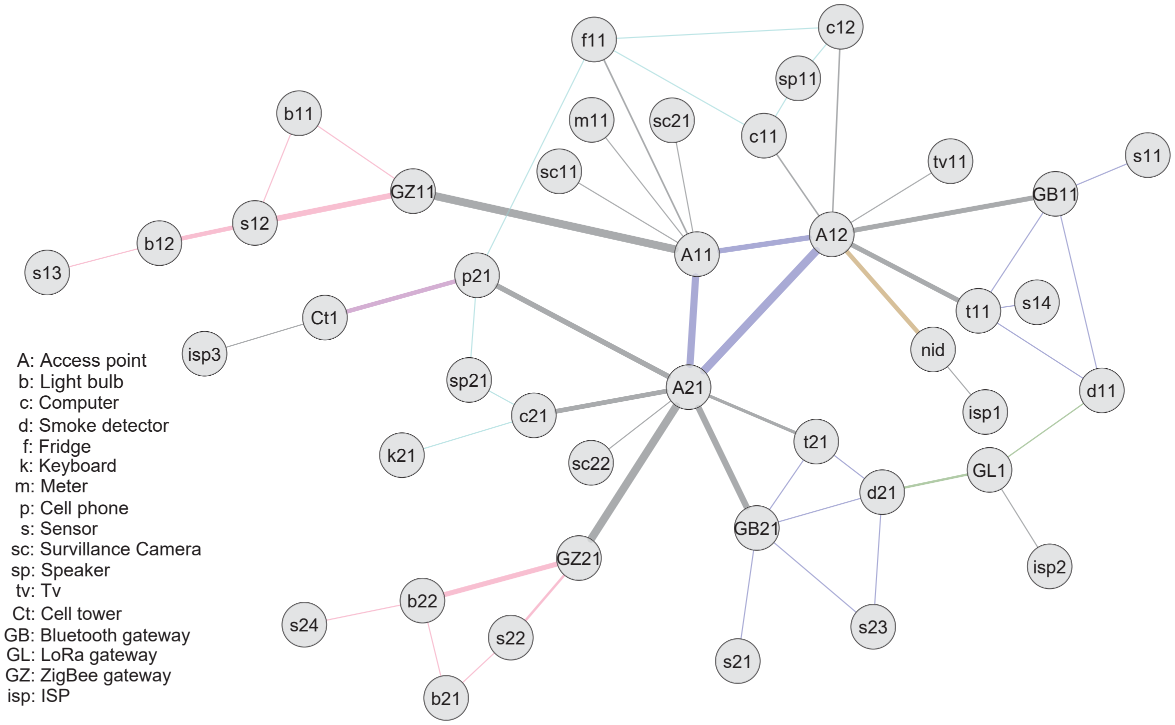

Fig. 2. Connectivity graph of the smart home model

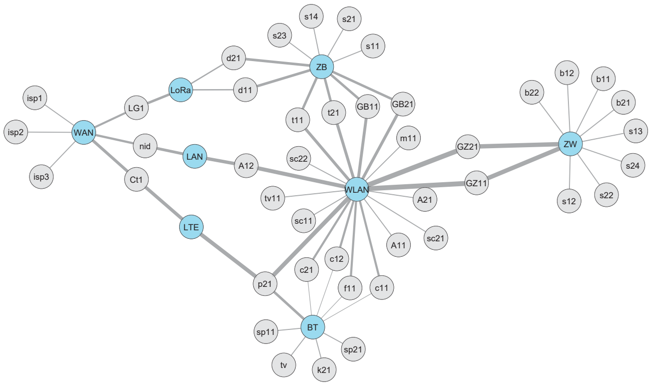

Fig. 3. End–system technology graph

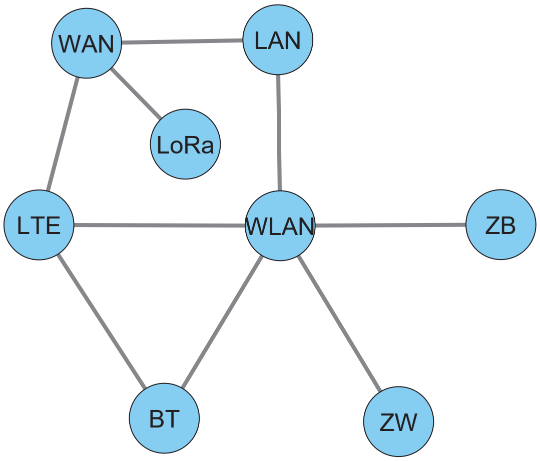

Fig. 4. Technology interdependence graph

some part of the network, but if the disconnected nodes are in the range of another access point or are mobile nodes, they may restore connectivity. Even if the 802.11 network is partitioned, the isolated subnetworks of other technologies should remain operational. However, if the isolated network includes critical nodes such as smoke detectors, the loss of interconnectivity may be life-threatening. Thus, resilience requires a k-connected graph where $k \geq 2$, which is not possible in a star topology. As a result, such technologies as Bluetooth are less resilient than technologies that support a mesh topology. 802.11s using additional nodes increases link redundancy and thus resilience; the trade-off between redundancy, cost, and delay should be considered.

V. Conclusion and Future Work

In this paper, we introduce a model for the smart home with the typical protocols to understand the complexity of the network due to the heterogeneity of the protocols and consequently the diversity of the network. We introduce two new graph representations to facilitate resilience analysis: *end-system technology* and *technology interdependence graphs*. In our typical example scenario, IEEE 802.11 is the dominant protocol for the smart home core network. However, using a single IEEE 802.11 access point in infrastructure mode results in a network vulnerable to a single point of failure. Therefore, if multiple access points are used with IEEE 802.11s, the resilience of the home network is improved. The network is then changed from a *star of meshes* topology to a *mesh of meshes*. Furthermore, critical nodes should have two diverse paths to access the Internet. In our future research, we plan to study the graph of the smart home in detail to use as the essential element of a robust smart city model. Such a study can reveal the weaknesses and strengths of smart city networks to improve their resilience.

References

[1] *P2413*. IEEE Standard Association, May 2015. https://standards.ieee.org/develop/project/2413.html.

[2] *Overview of the Internet of Things*. No. 2060 in Y, International Telecommunication Union, June 2012. https://www.itu.int/rec/T-REC-Y.2060-201206-I.

[3] *The Internet of Things Concept and Problem Statement*. IETF, 2010. http://tools.ietf.org/id/draft-lee-iot-problem-statement-00.txt.

[4] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the Internet of (important) Things," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 3, pp. 1389–1406, 2013.

[5] *The Internet of Things Reference Model*. Cisco Systems, 2014. http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.

[6] *IEEE Standard for Low-Rate Wireless Networks*. April 2016.

[7] *ZigBee Specification*. ZigBee Alliance, 2012. http://www.zigbee.org/wp-content/uploads/2014/11/docs-05-3474-20-0csg-zigbee-specification.pdf.

[8] *Bluetooth Core Specification v5.0*. Bluetooth Special Interest Group, 2016. https://www.bluetooth.com/specifications/bluetooth-core-specification.

[9] *Z-Wave Specifications*. Silicon Labs, 2018. http://zwavepublic.com/specifications.

[10] N. T. Johansen (editor), "Z-Wave Plus Device Type Specification." http://zwavepublic.com/specifications, 2017.

[11] N. Sorinin and A. Yegin, *LoRaWAN Specification v1.1*. LoRa Alliance, 2016. https://lora-alliance.org/resource-hub/lorawantm-specification-v11.

[12] "Sigfox." https://www.sigfox.com/en, 2017.

[13] J. Zuniga and B. Ponsard, "SigFox system description." https://tools.ietf.org/html/draft-zuniga-lpwan-sigfox-system-description-04 (Work in Progress), Dec. 2017.

[14] *3GPP Low Power Wide Area Technologies*. GSM Association, 2016. https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf.

[15] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Computer Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[16] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, "Smart Nest thermostat: A smart spy in your home," *Black Hat USA*, 2014.

[17] *Presidential Policy Directive – Critical Infrastructure Security and Resilience*. PPD-21, The White House, Office of the Press Secretary, Feb. 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[18] S. Pinnaka, R. Yarlagadda, and E. K. Çetinkaya, "Modelling robustness of critical infrastructure networks," in *2015 11th International Conference on the Design of Reliable Communication Networks (DRCN)*, pp. 95–98, March 2015.

[19] R. Minerva, A. Biru, and D. Rotondi, "Toward a definition of the Internet of Things (IoT)." https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf, May 2015.

[20] F. Carrez (editor), "Internet-of-Things Architecture IoT-A." EU FP7 2009-5 https://iotforum.org/wp-content/uploads/2014/10/D1.5.pdf, July 2013.

[21] "OpenFog." https://www.openfogconsortium.org/, 2017.

[22] *OpenFog Reference Architecture for Fog Computing*. OpenFog Consortium Architecture Working Group, 2017. https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf.

[23] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, no. 1, pp. 84 – 106, 2013. Including Special section: AIRCC-NetCoM 2009 and Special section: Clouds and Service-Oriented Architectures.

[24] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, vol. 13, no. 18, pp. 1587–1611, 2013.

[25] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Computing*, vol. 8, pp. 14–23, Oct 2009.

[26] M. T. Beck, M. Werner, S. Feld, and S. Schimper, "Mobile edge computing: A taxonomy," in *Proc. of the Sixth International Conference on Advances in Future Internet*, pp. 48–54, IARIA, 2014.

[27] A. Modarresi and J. P. G. Sterbenz, "Multilevel IoT model for smart cities resilience," in *Proceedings of the 12th International Conference on Future Internet Technologies*, CFI'17, (New York, NY, USA), pp. 7:1–7:7, ACM, 2017.

[28] T. Denning, T. Kohno, and H. M. Levy, "Computer security and the modern home," *Commun. ACM*, vol. 56, pp. 94–103, Jan. 2013.

[29] S. Marksteiner, V. J. E. Jimenez, H. Valiant, and H. Zeiner, "An overview of wireless IoT protocol security in the smart home domain," in *Internet of Things Business Models, Users, and Networks, 2017*, pp. 1–8, IEEE, 2017.

[30] J. Liu, C. Zhang, and Y. Fang, "EPIC: A differential privacy framework to defend smart homes against Internet traffic analysis," *IEEE Internet of Things Journal*, vol. 5, pp. 1206–1217, April 2018.

[31] J. P. G. Sterbenz and D. Hutchison, "ResiliNets: Multilevel resilient and survivable networking initiative." http://wiki.ittc.ku.edu/resilinets, 2005.

[32] E. K. Çetinkaya and J. P. G. Sterbenz, "A Taxonomy of Network Challenges," in *Proceedings of the 9th IEEE/IFIP International Conference on the Design of Reliable Communication Networks (DRCN)*, (Budapest), pp. 322–330, March 2013.

[33] *IEEE Draft Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks - Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE, Nov 2011.

[34] G. R. Hiertz, S. Max, R. Zhao, D. Denteneer, and L. Berlemann, "Principles of IEEE 802.11s," in *2007 16th International Conference on Computer Communications and Networks*, pp. 1002–1007, Aug 2007.

[35] J. P. Rohrer, A. Jabbar, and J. P. G. Sterbenz, "Path Diversification: A Multipath Resilience Mechanism," in *Proceedings of the IEEE 7th International Workshop on the Design of Reliable Communication Networks (DRCN)*, (Washington, DC), pp. 343–351, October 2009.

[36] Y. Cheng, M. T. Gardner, J. Li, R. May, D. Medhi, and J. P. Sterbenz, "Optimised Heuristics for a Geodiverse Routing Protocol," in *Proceedings of the IEEE 10th International Workshop on the Design of Reliable Communication Networks (DRCN)*, (Ghent, Belgium), pp. 1–9, April 2014.

[37] M. J. Alenazi and J. P. G. Sterbenz, "Comprehensive comparison and accuracy of graph metrics in predicting network resilience," in *2015 / 11th International Conference on Design of Reliable Communication Networks (DRCN 2015)*, (Kansas City, USA), 2015.

[38] E. K. Çetinkaya, M. J. F. Alenazi, J. P. Rohrer, and J. P. G. Sterbenz, "Topology Connectivity Analysis of Internet Infrastructure Using Graph Spectra," in *Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, (St. Petersburg), pp. 752–758, October 2012.

[39] P. Shannon, A. Markiel, O. Ozier, N. S. Baliga, J. T. Wang, D. Ramage, N. Amin, B. Schwikowski, and T. Ideker, "Cytoscape: a software environment for integrated models of biomolecular interaction networks," *Genome research*, vol. 13, no. 11, pp. 2498–2504, 2003.

[40] M. Newman, *Networks: An introduction*. Oxford university press, 2010.

[41] "NetworkX: Software for complex networks." https://networkx.github.io/, May 2018.