Journal of Ambient Intelligence and Humanized Computing (2020) 11:5825–5843
https://doi.org/10.1007/s12652-020-02095-8

ORIGINAL RESEARCH

Resilience and technological diversity in smart homes

A graph-theoretic approach to modeling IoT systems with integrated heterogeneous networks

Amir Modarresi[1] · **John Symons**[2]

Received: 30 December 2019 / Accepted: 15 April 2020 / Published online: 11 June 2020

Abstract
This article introduces our abstract modeling strategy to represent the general features and topology of the kinds of integrated and technologically diverse networks that feature in IoT systems. We begin with smart home networks. We generate instances of our model and analyze their graph-theoretic properties with an emphasis on the resilience of critical services and connections to the Global Internet. In addition to considering the network connectivity graph of nodes and links in the model, we explain our *technology interdependence graph* techniques. *Technology interdependence graphs* allow us to illuminate critical interactions in multi-technology systems such as smart homes. Using relatively simple examples we show how our approach permits the exploration of the resilience properties of various instances of smart systems involving complex technological interdependency. We describe a practical way of approaching the graphs of systems with a wide variety of integrated technologies and we discuss properties such as connectedness and other metrics. This approach can serve as the basis for tackling the challenge of designing resilient IoT-based smart-cities from the point of view of network topologies. We also study smart home resilience through path redundancy and heterogeneity of network technologies with graph centrality metrics.

Keywords Smart home · Science of security · Graph analysis · Modeling · Network resilience · Future networks · Internet of Things (IoT)

1 Introduction

The proliferation and variety of technologies in the so-called Internet of things (IoT) raises concerns with respect to security and resilience. Given the introduction of new attack surfaces and their associated vulnerabilities, IoT presents worrying new security threats to critical and often life-sustaining systems (Hassija et al. 2019). Because of the complexity of IoT systems, understanding the nature of these threats is not straightforward. For example, at the level of network analysis, the rapid growth of IoT has complicated matters in a variety of ways. IoT has changed edge networks by dramatically increasing the number of nodes and by introducing a variety of types of services and functions that are exposed to disruption. To date, this new context has proven difficult to tractably model. In this article, we examine the relatively simple context of smart home technologies in order to present strategies for thinking about improving the resilience of IoT systems more generally.

Diverse technologies, each with their own distinctive sets of vulnerabilities, support the functional requirements of so-called smart home and smart building systems. These include IEEE 802.11 and 802.3 for high-bit-rate and interactive applications, ZigBee (Alliance 2008), Bluetooth (Bluetooth 2015; Bluetooth Special Interest Group 2016) and Z-wave (Design Sigma 2018; Johansen 2017) for low-energy consumption and low bit rate. Other very-low bit rate and long-range technologies such as LoRaWAN (LoRa Alliance

This article is the extension of our previously published conference paper Modarresi and Symons (2019a) funded by NSA Science of Security initiative contract #H98230-18-D-0009.This work was also funded in part by NSF Grant 1856084.

✉ Amir Modarresi
amodarresi@ittc.ku.edu

[1] Information and Telecommunication Technology Center, University of Kansas, Lawrence, KS 66045, USA

[2] Department of Philosophy, University of Kansas, Lawrence, KS 66045, USA

2016), Sigfox (Moan 2017; Zuniga and Ponsard 2016), and NB-IoT (GSMA 2016) contribute to services requiring very low-energy consumption such as structure monitoring, leak management and the like. These technologies feature a variety of network topologies, ranging from star to mesh structures. Combining these technologies can result in the emergence of complex network properties even in a relatively small domain such as a smart home or building (Symons et al. 2007).

A typical smart home system is a combination of various sensors, actuators, controllers, control networks, and gateways (Paetz 2018). Sensors generate data and send them to the controllers through control networks such as ZigBee or Z-Wave. Devices in the network containing actuators and sensors are managed through the control networks while they are connected to the gateways that provide interconnection with other communication networks. Though this is the generic structure of a smart home system, in practice a range of distinct network technologies are used. The number of distinct network technologies with distinct topological features along with the overall network size contributes to the complexity of the system as a whole. Furthermore, each technology has unique physical and logical characteristics including the frequency bands, the network initiation process, the network components, the number of supported nodes, availability, and security features. With each of these features comes the potential for exploitable vulnerabilities.

While there is an understandable and justified concern that the heterogeneity of IoT technologies expands the available attack surface for adversaries and makes systems as a whole increasingly fragile, technological diversity need not be straightforwardly bad news for security and resilience. As we show in this paper, the heterogeneity of the technologies in a system can potentially improve resilience given suitable design principles. For example, since important aspects of each network technology are sometimes self-contained, any disruption to the operation of the network technologies renders only that individual network inaccessible. Furthermore, to take a simple example, when devices such as laptops and cellphones support more than one network technology, they can operate in many networks at the same time. Most obviously, this redundancy increases the probability that the overall system will be available and consequently the resilience of the system as a whole increases. These are simple examples, but they speak to a more general point: Understanding how diverse networks and technologies interact is critical to designing system-wide resilience.

A first step is to provide a general and abstract approach to tackling the problem that can be applied to a variety of contexts. Our goal is to provide general principles for helping to design resilience into complex and technologically diverse systems (Pipa and Symons 2019). To that end, in this paper, we present an abstract home network model for smart home architectures and perform a graph-theoretic analysis on various instances of this model. Our goal here is to demonstrate in simple terms, how to approach to designing resilient multi-technology systems. The paper is organized as follows. First, we review some of the available IoT models. In Sect. 3, we present our abstract smart home model to show the interaction of distinct network technologies. Then we generate instances of the model. In Sect. 4, we perform a graph-theoretic analysis on one instance of the smart home and compare it with two baseline models with star and mesh topologies. In Sect. 5, we analyze various instances of smart home models to explore the overall behavior of the system that results from the addition of devices and network technologies. So, for example, studying the addition of cellphones to the network allows us to consider the extent to which these additional devices provide additional redundancy and resilience. We conduct similar experiments involving the addition of network technologies in order to understand the changes that result in the behavior of the system as a whole. Finally, we offer some concluding comments and some plans for future work in Sect. 6.

2 Background and related work

IoT is already integral to a range of important endeavors, including industrial production and manufacturing, critical infrastructure, military applications, cities, and homes. Several models have been introduced to represent the IoT ecosystem (Modarresi and Sterbenz 2017; Streitz 2018; Plantevin et al. 2019; De Paola et al. 2019); however, most of these models lack important details about the relationship between the structure and function of the multi-technology networks in systems such as smart homes and cities. Existing work has provided useful maps and helpful distinctions, but it does not permit effective graph theoretic analysis for reasons we will explain, nor does it facilitate the kind of design that increases resilience in these systems.

The IEEE reference model (Minerva et al. 2015) shows IoT systems in three functional layers including sensing, network and data communications, and applications. The ITU Y.2060 model (ITU 2012) shows the integration of "things" to communication networks. The Internet Engineering Task Force (IETF) reference model concentrate on factors for enabling IoT communications. The National Institute of Standards and Technology (NIST) considers an IoT system as a cyber-physical system (CPS) technology to connect smart devices (Boutin 2014). Cisco defines the concept of fog computing and adds it to its seven-layer IoT model (Lake et al. 2012). Other specialized models as part of the IoT systems have been introduced for mobile (Fernando et al. 2013; Dinh et al. 2013), edge (Vaquero and Rodero-Merino

2014), and fog computing (OpenFog Consortium Architecture Working Group 2017).

In order to improve the resilience of these networks it will be helpful to develop models focusing on the distinctive structural properties of the networks involved in such systems. In previous work we have focused particularly on the topological features of networks. We have previously introduced a reference model for the interaction of technologies associated with the kinds of services that are likely be typical in smart homes in the near future (Modarresi et al. 2018). We obtain our *connectivity graph* by converting our reference model to a graph model. Our *connectivity graph* led us to our *technology interdependence graph* where we can represent the role of a high-bit-rate technology such as WLAN serving as the smart home backbone network. As explained below, other network technologies connect to this backbone in ways that we can model.

3 Smart home model

We introduce our abstract smart home model in Part 3.1. Then, we present our home network graph representation model produced by Python NetworkX (NetworkX developers 2018) for the smart home network in Part 3.2. At this stage, the goal is simply to model a typical smart home network architecture in order to provide a platform for exploring ways to improve its resilience.

3.1 Abstract smart home modeling

A first step toward creating a graph model that can be used for simulation-based analysis (Modarresi and Symons 2020) is to create an abstract representation of the smart-home network. The reason for abstracting from the details of particular networks is to achieve the kind of generalizations that apply to a wide range of distinct cases. At the same time, it is important to include some of the functionally relevant features of the smart home context, most importantly it is important to capture the ways in which diverse technologies interact. A scientifically useful model will be one that is abstract enough to provide general insights, but that also recognizes the implications of technological heterogeneity and interaction. Our *smart home abstract model* is depicted in Fig. 1. This shows the architecture and high-level structure consisting of the *home backbone* with other attached *home edge network* technologies introduced below. The home backbone is typically a mix of wired Ethernet and wireless 802.11 technologies. However, notice that at the network layer it appears as a single IP-addressable network. In addition to end systems such as laptops (not shown in this figure), the home backbone provides connectivity to various other home edge network technologies, with disparate

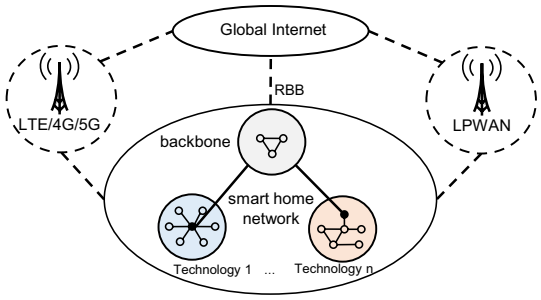


Fig. 1 Smart home abstract model

topology, protocols, and addressing. These edge technologies generally interconnect only through gateways to the home backbone, resulting in a star topology of networks, of which two are shown in Fig. 1.

Traditionally, homes have been connected to the Global Internet for user access to Web browsing and email. More recently, many *smart* home services use connectivity for remote access, e.g. for access to security systems or for controlling lighting and heating when residents are away from home. While it is beyond the scope of the current paper to address in detail, it is worth noting that many IoT devices use cloud-based services, significantly increasing the available attack surface, while providing poor resilience for those systems given that they often cannot operate when disconnected from the Internet. While connecting to the Internet via an RBB (residential broadband) link such as DSL or HFC (hybrid fiber coaxial) has been the norm, increasingly LTE mobile networks (evolving to 4G LTE-advanced and 5G) are providing Internet access to homes. Additional connectivity to the Internet obviously enables the increased redundancy of a biconnected graph. It also provides diversity with respect to the communication medium such that wireless can be used if a cable is damaged, and wired if the wireless channel is disrupted by, for example, heavy precipitation or jamming.

3.2 Technologies in smart home model

As presented in Fig. 2, high-bit-rate LAN technologies including Ethernet, 802.11, and 802.11s are used as the home backbone. While wireless LANs are the dominant technology forming the home backbone, they may suffer interference in a dense urban environment and can be jammed to disrupt home services and operation. Each LAN technology usually supports a particular topology. IEEE 802.11 in the infrastructure mode uses a star topology while 802.11s uses a mesh topology. The range extension capability of 802.11s due to the mesh topology makes it preferable to basic 802.11 for the home backbone LAN. Furthermore, switched Ethernet can construct physical mesh with a logical

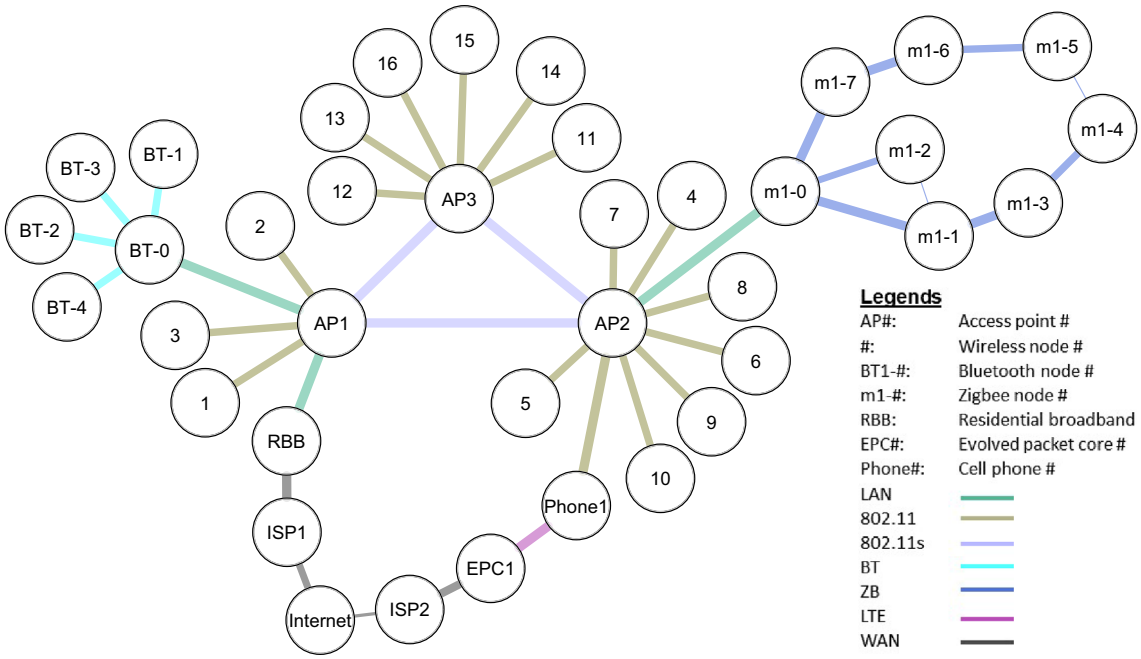


Fig. 2 Connectivity graph of the home network model

spanning tree overlay to avoid loops in the network. Considering network resilience, a mesh network with k-connectivity (a connected graph with k separate path between each node pair) of $k \geq 2$ should be constructed for the home backbone LAN. We consider k-connectivity of $k = 2$ for brevity of the model in the backbone structure while $k = 2$ offers minimum network resilience at the backbone.

The mesh nodes comprise a mesh basic service set (MBSS). MBSS can be connected to an infrastructure BSS through a distribution system by a mesh gateway. Therefore, the infrastructure BSS supports other typical and high-speed IP services constructing a star topology around each mesh station equipped with an access point. Although the access points in 802.11 represent a critical point of failure of this structure, mobile nodes can connect to other access points during failure of their native access point. On the other hand, implementing some of the mesh edges with Ethernet improves resilience more through the heterogeneity of the technologies and diversity of the protocol mechanisms.

Other network technologies are connected to the backbone through their gateways. Current technologies, including ZigBee and Z-Wave, can construct mesh topology. Other technologies including Bluetooth operate via a star topology. Notice also that Bluetooth can construct mesh topology by changing the role of a slave node to a master node and vice versa.

Most of the low-bit-rate technologies such as ZigBee support a mesh topology. However, the topology of such networks also depends on the density of the nodes in the network, the average distance among nodes, and the specialized nodes that are utilized by a particular technology such as coordinators and routers. The topology may be a star when all nodes are in the range of the coordinator or master node but far from each other, linear when the network coverage is extended, mesh when some nodes are in the range of the other nodes, or a combination of these options. In most low-bit-rate technologies including ZigBee and Z-Wave the battery-operated nodes do not participate in the routing or forwarding processes; therefore they are usually the endpoints of the network graph. We construct this part of the network graph by the *caveman* graph algorithm with Python networkX library, which permits us to generate a particular number of cliques with a specific size. This structure can emulate a controlled mesh network. We process the produced graph from caveman (Kang and Faloutsos 2011) algorithm for the number of connected components. We eliminate those nodes that are not part of the largest component in the graph to generate a graph with one connected component. Since both ZigBee and Z-Wave generate a mesh topology in an optimal condition, we consider one mesh network for brevity as a sample of these technologies in our model; although, many such networks with more complexity and number of nodes can exist simultaneously in a larger network. For instance, a simple network can have one particular network technology while a multi-story building may have various types of networks with more nodes. Since these network technologies are low bit rates and self-contained, any structural changes or failure will have minimal

or no effect on the home backbone LAN. Therefore, these networks can be studied separately. Notice that an effective network analysis involves taking account of the functional characteristics of the technology involved here.

Other high-bit-rate technologies, including 4G/LTE/5G, can be integrated to the network to increase the path diversity to the Internet. When the network is in the normal operation, a cellphone can join the network through its 802.11 interface and act as a wireless station. However, during a WAN failure, a tethered cellphone can operate as an access point to connect the internal network to the Internet through a different path.

LPWAN technologies including NB-IoT and LoRaWAN can also be utilized in a smart home network. However, we do not use them in our home network graph model; since, such technologies are part of larger networks which are mainly outside of the smart home network. Many technologies in this category, including NB-IoT, LoRaWAN, and Sigfox, have a star or star of star topologies similar to the topology in 4G/LTE/5G technologies. In all of these technologies, the center point of the star topology is usually outside of the home network. Such networks are connected to the home network at the ISP level or even an AS level. Hence, any failure in the lower levels of the network hierarchy will not affect both networks simultaneously; unless the failure happens at the same or higher levels of the hierarchy in which the two networks are connected. We represent the point of connection between the two networks with the *Internet* node in our home network graph model illustrated in Fig. 2 assuming that the two ISPs are reachable with one hop to simplify the structural complexity of the Internet.

4 Graph-theoretic representation and analysis

The analysis of our model uses a formal graph representation. We calculate various graph analysis metrics and compare with baseline home network architectures, including star and mesh, in order to study properties of our model. We perform a similar analysis on our technology interdependence graph. Here again, our goal is to study the logical representation of the typical technologies employed in a smart home with being unnecessarily any constrained by the details of a particular network and its associated components.

4.1 Home network model analysis

Given our home network model, we define an edge-colored graph $\mathbb{G}_{\text{conn}} = (V_c, E_c, C, \chi)$ as the connectivity graph illustrated in Fig. 2, such that $v_i \in V_c$ is a node with a transceiver t_{ik} of a particular technology and $e_n \in E_c$ is a communication link between two adjacent nodes v_i and v_j. Furthermore, C is a set of colors equivalent to the number of employed technologies in the graph and $\chi : E_c \rightarrow C$ is a function to assign a color to each edge. More precisely, we can define E_c as $E_c = \{((v_i, v_j) \in V_c \times V_c, c_i) | \chi(v_i, v_j) = c_i\}$.

We start this analysis by evaluating two baseline topologies: the star and mesh backbones. We consider a star wireless LAN implemented with IEEE 802.11 connected to the Internet by an Ethernet link through a DSL or HFC cable link, typical of many traditional home networks. We then enhance the star network to incorporate a full-mesh backbone as would occur by replacing a single 802.11 access point with three meshed 802.11s nodes (AP1, AP2, AP3). Next, we consider our home network graph (Fig. 2) and compare it with the other two baseline topologies. Finally, we calculate the graph metrics for our home network during a failure on the Internet access link ($NID \leftrightarrow ISP1$) that fails over to the backup access path through *Phone1*, illustrated in Fig. 3. The number of 802.11 wireless workstations are the same in both the baseline models and the home network model. However, the home network model has extra nodes representing the network technologies connected to the home backbone.

We then consider the following failover mechanism for our centrality analysis. If the Internet access link between *NID* and *ISP1* in our home network graph fails, the home backbone LAN and consequently the rest of the network is disconnected from the Internet. While the home network is still locally operational, the cloud services are inaccessible. Though *Phone1* can provide Internet access through the LTE network in the tethering mode, this process may partition the home network. This is due to the fact that a mesh node (an 802.11s mesh station) cannot connect to an 802.11 access point (a cellphone in the tethering mode) directly. Moreover, two access points cannot simply connect to each other without a distribution system. As a result, the mesh network would not have access to the Internet. Two possible options for resolving this Internet access disruption in the mesh nodes are either using Wi-Fi Direct (Wi-Fi Alliance 2018) on the mesh nodes and the cellphone or cellphones equiped with 802.11s. Wi-Fi Direct provides a one-hop connection between two nodes without a physical access point, while 802.11s support multi-hop connections. During the failure, other network technologies can connect to the second path if their gateways have 802.11 interfaces. We do not consider these two options in our measurement at this point.

We examine various graph node and edge centrality metrics for this analysis, and report the minimum, maximum, and mean values in Table 1. Graph centrality metrics can be classified into three groups: distance, connectivity, and spectra classes (Hernández and Van Mieghem 2011). Distance metric measurements are based on the shortest path and the number of hop count over the shortest path. The node-degree

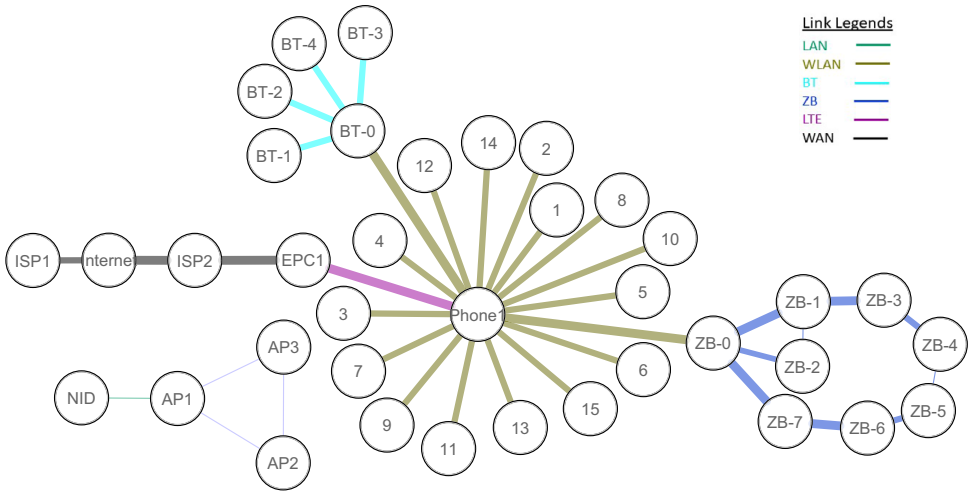


Fig. 3 Connectivity graph of the backup topology

values are the main consideration for connectivity-based centrality metrics. Finally, eigenvalues and eigenvectors are the foundational concepts for the spectra metric measurements. We emphasize that our list of centrality metrics is not comprehensive and we consider some of the relative metrics to our model from each category. The aim is to find appropriate centrality metrics from these groups to describe our multi-technology model. One should note that the thickness of each edge in Figs. 2 and 3 represent the value of edge-betweenness centrality (number of traversing shortest paths) computed by Cytoscape (Shannon et al. 2003). Each specific edge color shows a particular technology according to our graph model definition.

In the home network graph and consequently the backup graph, various network technologies interconnect, which differ in a number of aspects including topology, node responsibility, link data rate, and failover policy. Node and edge attributes may be employed to identify those characteristics, but not all can be simply represented as edge weights. Two possible options are introducing new role-based centrality metrics, or altering existing centrality metrics to consider a particular attribute in the calculation. For instance, if a critical node (such as Bluetooth or Zigbee/802.15.4 controller) is located at the edge of network technology, its node degree or betweenness can be significantly increased beyond the value computed from the graph structure to reflect its importance in network operation.

4.1.1 Distance-based centrality metrics

We examine *diameter*, *eccentricity*, *closeness*, *betweenness*, and *stress* from this group in our analysis.

The network *diameter* is a metric that represents the minimum number of hops to connect the farthest pair of nodes in a particular network. Regarding the graphs under study, the star topology has the shortest diameter among baseline models. The mesh network integrated with an access point on each mesh node has the next longest diameter. If the number of mesh nodes increases, a one-hop distance can be maintained as long as a complete graph is constructed among the mesh nodes.

During Internet access link failure, the backbone component is partitioned; therefore, the diameter value of the larger component decreases, affecting the value of metrics that depend on the shortest path metrics. However, the shortened diameter, in this case, may not significantly change the delay; because, one high-speed component of the network has failed, and network technologies with low-speed connectivity remain intact. Therefore, diameter alone is not an adequate measurement in a multi-technology network. It only provides an overall view of the network size.

Eccentricity centrality measures the longest of all shortest path from each vertex v_i to all other vertices to capture the reachability of vertex v_i. The higher value shows the proximity of node v_i to other nodes. Eccentricity decreases from the star topology to our home network graph due to the addition of network technologies and consequently the increase of the network diameter. However, the higher eccentricity with relatively close values of the backbone nodes shows that other technology networks are evenly installed around the backbone. Therefore, minimizing the maximum length from backbone nodes should be a consideration in the design of smart home and other IoT systems. We provide the eccentricity results in Table 1.

Closeness centrality is a measure of the average shortest path for any node v_i to other nodes in a network. Closeness centrality deals with the minimum-sum reachability problem. A network with a larger mean quantity of closeness centrality has the smaller average of the shortest path among all nodes showing that the nodes are more concentrated toward the center of the network.

The center node of the star topology has the maximum closeness centrality value. When a network is expanded, the node's closeness centrality values decrease due to longer paths as observed in our home network graph. In the backup topology, *Phone1* has the highest closeness value. In addition, the overall closeness values for all nodes increase. Since the network gets shorter because of losing the backbone nodes. A node with high closeness value and high degree centrality has an exceptional position to disseminate information. However, such nodes in communication networks are vulnerable in targeted attacks. Therefore, distributing closeness among all nodes are more favorable in communication networks, which makes our home network graph more resilient than other topologies.

Edge betweenness centrality is an edge centrality metric measuring the fraction of the number of the shortest path between every pair of nodes v_i and v_j that passes over a particular edge e_k. An edge with a high value of the edge betweenness connecting two low degree nodes at both ends indicates a bridge in which it connects two parts of a network. Failure of such edges may partition a network.

In our home network graph, all edges that connect a gateway to an access point have a high edge betweenness centrality values. Generally speaking, all edges connecting part of a network with a different technology to another have a high edge betweenness centrality value constructing a bridge between two parts of the network. Disruption of such edges partitions a network technology from the rest of the network. Therefore, such links should be considered critical links; although, they do not have the maximum edge betweenness centrality in the network. The same condition is observed between *Phone1* and *EPC* in the backup topology in which the home network is connected to the LTE network during the failure. The thickness of the edges in Figs. 2 and 3 illustrate such edges. Adding diverse paths in proper places either through the same or different technology decreases edge betweenness centrality on bridges improving the network resilience through increasing technology heterogeneity. This is particularly important as a general principle for IoT design.

For instance, given a particular gateway, two wired and wireless interfaces may decrease the edge betweenness value of the connected edge to the gateway. The limitation is easily observed during failure since the only high speed and long range available technology is LTE. In a smart city with wireless access connectivity, one might have another path to the Internet with a restriction; because all nodes should connect to the citywide wireless network at relatively short ranges.

Although edge betweenness centrality may identify important edges that connect technology variants to the backbone network, it is not an appropriate measure for recognizing critical edges connecting important edge nodes. All edges connecting edge nodes to other nodes receive a low value with this metric while such nodes including sensors may gather critical data (think, for example, of a smoke detector or similar life-critical sensor). Here we see an obvious mismatch between graph theoretic measures and other dimensions of importance. One possible solution to alleviate the criticality of such nodes would be to install redundant nodes in the same area, thereby increasing system cost. Another solution is to use a node supporting the capacity of different technologies to participate via a range of distinct network technologies. This would involve sacrifices in energy consumption. Our approach shows how one might weigh the various features of trade-offs like these. However, as noted throughout our discussion, graph theoretic measures alone cannot settle the question of the amount of resources to expend on maintaining the functionality of particular nodes in the network. Just how critical a particular node is judged to be is a matter determined by other means.

Node betweenness centrality, a node centrality metric, measures the fraction of the number of shortest paths between every two nodes v_i and v_j that lies on a particular node v_k. This value identifies the importance of a particular node in communication among other nodes. We provide the results of this metric for all models in Table 1.

Stress centrality measures the amount of communication that passes through an individual vertex v_i. It is measured based on the number of the shortest paths through a node v_i. This metric assumes that all the edges in the network have the same bandwidth and that all traffic goes through the shortest paths. Therefore, it does not provide an accurate result in a multi-technology network when each group of links has different bandwidth. For instance, *AP1* connected to *NID* handles both the Internet traffic and part of the local traffic while it has a lower value than *AP2* with more edges. Although assigning weights to edges can increase the accuracy of the measurement, weight normalization should also be considered in a multi-technology network. Here, it is important to note that a saturated link in a low-bit-rate technology has the same effect for that particular technology as the corresponding link in a high-bit-rate technology.

4.1.2 Connectivity-based centrality metrics

We analyze *degree centrality*, *neighborhood connectivity*, and *k-edge connected* metrics from this group.

Degree centrality in the network is a measure of the importance of a node with respect to how well-connected it is. A higher degree for a particular node in a communications network suggests that more nodes rely on it for their communication. A node with high degree centrality in a communication network is a potential vulnerability in targeted attacks.

The center point of a star topology has the maximum possible value for degree centrality ($n - 1$ where n is the number

of vertices), which makes it the most vulnerable node to any attack or failure. In a mesh topology, the WLAN backbone is divided among mesh nodes, decreasing degree centrality values and, consequently, distributing the effect of any failure or attack. We observe the same effect in the backbone network of our home graph since it has a similar architecture. Although a node failure with high degree centrality in the home backbone LAN can disrupt communication, failure of a gateway, even with lower degree centrality, in a star or mesh network technology can disconnect the entire associated network technology, which may support critical end nodes. Therefore, focusing on the degree centrality value alone cannot identify the crucial components of a multi-technology network.

Neighborhood connectivity measures the average number of neighbors of all v_i's neighbors (Maslov and Sneppen 2002; Jalili et al. 2015). The neighborhood connectivity of node v_i is small if v_i has neighbors with low-degree centrality. In contrast, nodes with low degree centrality connected to the neighbors with high-degree centrality have high value. It shows the capability of any particular node to communicate with other non-neighbor nodes. Therefore, all nodes at the center of a star topology have a low neighborhood connectivity value. Although this metric cannot consider a node criticality value and does not provide a direct connectivity measurement, it can identify a proper indication for the connectivity of the edge nodes. Since the edge nodes in a low-bit-rate and low-energy consumption technologies usually connect to other nodes with a single link, neighborhood connectivity can indicate the well-connectivity of an edge node if the first hop is intact.

k-edge connected, or k-connected, graph G is a connected graph with the maximum number of edges $\mid X \mid$ where $X \subseteq E$ and $\mid X \mid < k$ such that subgraph $G' = (V, E \backslash X)$ is still connected. k-edge connected implies that k separate paths exist between each node pair in G such that removing k edges partitions G. In k-edge connected graph G, it is required that $k \leq \delta(G)$ where $\delta(G)$ is the minimum degree of $v_i \in V$ (Koschützki et al. 2005; Wikipedia 2018). k-vertex connected graph is defined similarly.

Given the definition of k-edge connectness, neither of the models under study is k-connected; however, subgraph $G' = (V', E')$ where $V' = \{AP1, AP2, AP3\}$ is bi-connected (k-connected where $k = 2$) makes the mesh baseline model and consequently our home backbone network resilient to a single link failure.

4.1.3 Spectra centrality metrics

We examine *eigenvector centrality* and *Katz centrality* from this group.

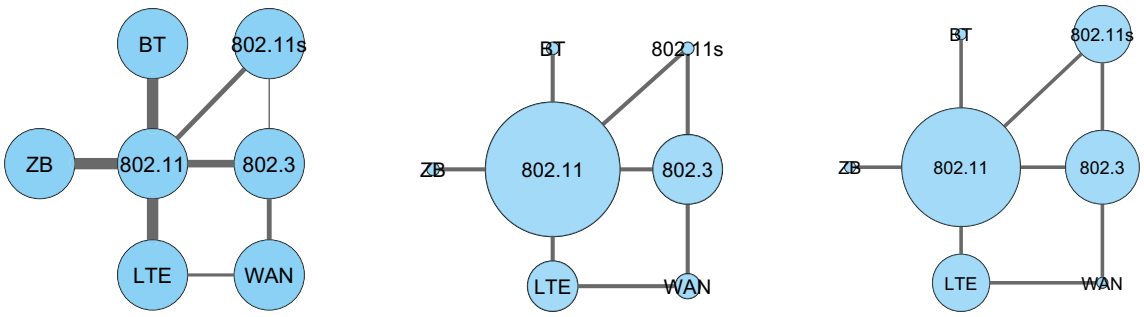
Eigenvector centrality is an extension of degree centrality that considers the importance of a node as its number of connections to the other important nodes (Newman 2010). Although this metric can identify an important node based on its number of connections in a homogeneous network, it cannot recognize such nodes in a multi-technology network. This is especially the case for nodes representing battery-operated devices which have limited capability to establish multiple connections.

Katz centrality is an extension of eigenvector centrality. Similar to eigenvector centrality, the importance of a node v_i depends on the number of direct neighbors, and neighbors of neighbors. However, the effect of neighbors of neighbors over the Katz centrality of v_i decreases when the distance from v_i increases. Katz centrality considers length of a walk between two vertices v_i and a neighbor v_j, and the effect of v_j over v_i (Koschützki et al. 2005; Newman 2010). Katz centrality can consider nodes with various importance in the measurement. Assigning a proper critical value to each node can provide a result considering the importance of nodes. We assign a high critical value to all access points and gateways in the models under study. A medium critical value is assigned to important nodes and sensors such as smoke detectors and routers in a particular network technology. We assign the lowest value to other nodes. In contrast to other metrics, Katz assigns proper centrality values to the edge nodes, if they are important. We show the overall centrality results in Table 1.

4.2 Technology interdependence model analysis

Our *technology interdependence graph* is the result of a one-mode projection over the incidence matrix of the bipartite node-technology smart home connectivity graph (Modarresi et al. 2018). The one-mode projection finds adjacency between nodes based-on their connectivity to another group of nodes. This graph illustrates the relationship among technologies in a typical smart home. However, the high-level representation of this graph hides the details of particular components in the network technologies and shows the relationship among technologies in the overall network structure. Due to the simplicity of this graph, the centrality metrics for the graph analysis provide especially intuitive results. We perform the same analysis as we provide in Subsection 4.1 and add the results to the last column of Table 1. We also interpret the results of some of the important metrics and refer the readers to Table 1 for brevity.

Figure 4a illustrates the result of the edge betweenness of our technology interdependence graph. The thickness of the edges represents the level of betweenness. Both short-range technologies used in the home network graph, ZigBee and Bluetooth, have equal edge betweenness values. It shows the contribution of each network technology to the overall connectivity of the network without considering how nodes in a network are connected or how many critical nodes there are.



(a) Edge betweenness **(b)** Node betweenness **(c)** Closeness

Fig. 4 Technology interdependence graph centrality metrics

Table 1 The graph metrics for the various topologies

Graph centrality metrics		Model				
		Star	Mesh	Home	Backup	Technology
Diameter	Value	4	5	8	8	3
Shortest path	Min	1.16	1.71	2.08	1.72	1.67
	Mean	2.16	2.66	3.48	3.09	1.72
	Max	3.67	4.33	5.19	5.22	2.00
Eccentricity	Min	0.25	0.20	0.13	0.13	0.33
	Mean	0.27	0.23	0.17	0.18	0.43
	Max	0.50	0.33	0.25	0.25	0.5
Closeness	Min	0.27	0.23	0.19	0.19	0.5
	Mean	0.48	0.39	0.30	0.34	0.6
	Max	0.86	0.58	0.48	0.58	0.86
Edge betweenness	Min	36	42	8	8	4
	Mean	41.11	55.91	126.73	96.18	9
	Max	96	114	496	400	12
Node betweenness	Min	0	0	0	0	0
	Mean	0.07	0.08	0.07	0.07	0.14
	Max	0.98	0.57	0.68	0.91	0.7
Stress	Min	0	0	0	0	0
	Mean	20.95	34.91	98.26	67.03	6
	Max	300	238	946	904	26
Degree	Min	1	1	1	1	1
	Mean	1.89	2	2.16	2.06	2.29
	Max	16	9	11	18	5
Neighborhood connectivity	Min	1.06	1.50	2	1.44	1.8
	Mean	13.35	6.60	5.76	10.16	3.54
	Max	16	9	11	18	5
Eigenvector centrality	Min	0.013	0.01	0.006	0.002	0.22
	Mean	0.19	0.17	0.12	0.13	0.36
	Max	0.71	0.53	0.56	0.69	0.59
Katz centrality	Min	0.08	0.08	0.08	0.08	0.33
	Mean	0.16	0.16	0.14	0.16	0.38
	Max	0.59	0.38	0.37	0.49	0.46

To take a simple example, if a cellphone with a Bluetooth interface joins the Bluetooth network (not shown in the figure) the k-connectivity of the Bluetooth network increases to 2 making it more resilient to the failure of technologies. If ZigBee technology can be integrated with more devices such as cellphones or laptops, we can expect the same resilient improvement for ZigBee.

In Fig. 4b the size of each node represents the value of node betweenness which can be interpreted as the importance of the technologies for the overall communication in the graph. As discussed, WLAN is the crucial technology in the smart home network connecting other technologies together. Furthermore, any disruption to the WLAN network partitions the home network into multiple components. Therefore, in order to improve the network resilience protecting WLAN in various ways such as increasing k-connectivity, enforcing higher security, and using dual-band connectivity would be essential tasks in the smart home improvement. One should note that losing any non-IP network technology does not have an effect on the operation of the home backbone. However, having a critical node in the disrupted network technology, such as a smoke detector, may increase the danger to the home residents. Therefore, as discussed above, any node judged to be critical could equipped with multiple technologies according to their level of importance.

Figure 4c illustrates the node closeness centrality value. The figure shows that 802.11 has the smallest average shortest path to other technologies. This result can confirm that 802.11 is at the center of the technology network.

5 Smart home topological analysis

As shown is Sect. 3, Smart home models are relatively small networks with complex interactions caused by the presence of diverse network technologies. If one fails to consider the functionality of nodes one generates misleading characterizations of network properties (Modarresi et al. 2019). This is critically important when we are attempting to determine the vulnerability of these networks. However, the kind of topological analysis of smart home networks that we conduct, provides valuable insight into the vulnerabilities of such networks. In this section, we analyze the topological structure of various smart home networks.

As mentioned, deploying different network technologies provides path redundancy and diversity to the Internet resulting in improving network resilience. In this section, we analyze how adding extra cellphones with 4G/LTE/5G and WiFi technologies can affect the topological structure of the smart home models. This analysis is performed over many randomly generated smart home models with a different number of nodes in their backbone, resulting in networks of various sizes.

In Sect. 5.1, we explain our framework to generate the variants of smart home networks to perform our study. In Sect. 5.2, we analyze the generated smart home instances with conventional centrality metrics. We inspect the effect of size, the number of technology networks connected to the backbone, and the number of cellphones to understand the overall topological structure of a smart home network. In other words, we would like to examine how several technologies incorporated into various nodes such as cellphones that improve path redundancy and technological diversity affect the smart home models and how conventional centrality metrics can capture such changes in the networks.

5.1 A framework for constructing smart home variants

In this section, we explain our method for constructing randomly generated smart home instances corresponding with the smart home abstract model proposed in Sect. 3.1. This approach can be applied generally, for example to situations where one needed to randomly generate instances of larger or more complex IoT contexts such as smart cities. We use the instances generated by this framework for further analysis of the topological structure of the smart home models. Each instance follows the same concepts, as explained in Sect. 3.1, with a backbone for each model. Then, the network technologies are connected to the backbone. The smart home network is connected to the Internet with RBB and 4G/LTE/5G technologies to provide diverse paths to the Internet. We construct smart home models with varying numbers of integrated access points for the backbones. We consider three to six integrated access points for the backbones. After constructing the backbones, we connect network technologies to the backbone for two groups of experiments. In the first group, we add one star- (representing Bluetooth networks) and one mesh- (representing Zigbee/Z-Wave networks) networks to the backbones. In the second group, we connect two star and two mesh network technologies to each backbone. Each generated instance is integrated with one to three cellphones to provide redundant network access to the Internet.

5.1.1 Backbone structures

Three integrated access points can construct only two different backbones, linear and complete graphs. However, when the number of integrated access points increases, the possible number of backbones increases accordingly. The maximum number of edges in a network obtains when a node v_i connects to $n-1$ other nodes where n is the total number of nodes in graph G resulting in a complete graph with graph

efficiency equal to 1. The efficiency between node v_i and v_j is the multiplicative inverse of the shortest path distance between v_i and v_j (Latora and Marchiori 2001).

In order to generate a controlled environment, we construct 25 different backbones manually in a way that we consider linear, partially completed, and bi-connected networks. For each backbone with n nodes, we use the backbone topologies with $n-1$ nodes and add one extra node. This extra node contributes to the overall backbone topologies in a way that we can generate different range topologies from linear to partially completed graph.

Figures 5 and 6 illustrate two samples of our smart home instances with three and six nodes in their backbones. Nodes *AP1* to *AP6* construct the backbone graphs in the corresponding figures.

5.1.2 Network technology structures

The network technologies connect to the backbones through their gateways. In a star topology, the center of the star network is considered the gateway. In a mesh topology, the first created node in the network is considered the gateway labeled with 0 in Figs. 5 and 6. We consider a fixed number of nodes in the star and mesh topologies in order to establish a controlled environment. During the generation of the network technologies, they connect to the backbone nodes randomly. This process is repeated ten times for each backbone to construct randomly generated topologies. It is possible that star and mesh networks connect to the same backbone node due to this random process.

The number of network technologies affects smart home networks in two ways. First, through the topology that each type of network technology uses to establish the network, and second, by the number of nodes used in each network. We generate the same network topology with the identical number of nodes for each particular network technology so as to generate a controlled environment. In order to study the effect of the number of technologies, we perform two groups of experiments. In the first group, we consider two mesh and two star topologies in each model and compare the results. In the second group, we add only one star and one mesh network to the models and compare the results with the corresponding models constructed in the first group. We use Python NetworkX library to construct both star and mesh topologies. The Caveman algorithm (Watts 1999) in NetworkX is used to build the mesh topology.

5.1.3 Cellphone integration

As discussed in Sect. 3, cellphones provide additional paths to the Internet, improving network resilience against Internet connection failures through redundant paths. In order to study the effect of redundant path with the number of cellphones on the topological structure of the networks, we

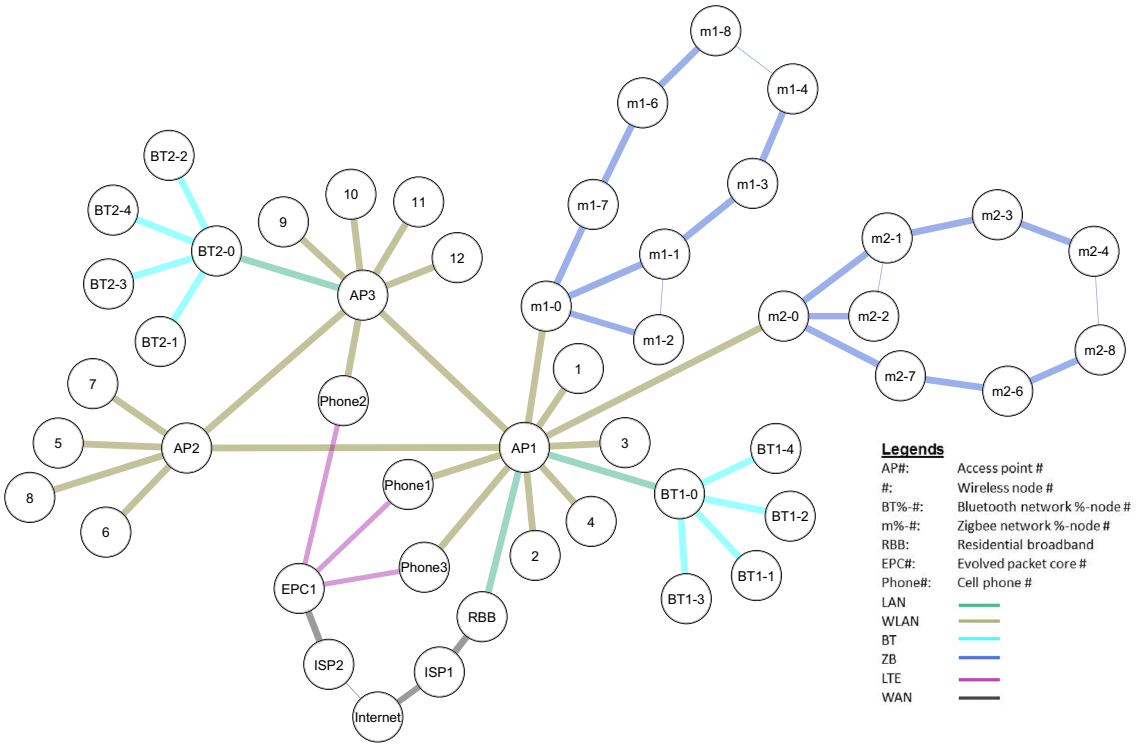


Fig. 5 An instance of a smart home with three access points

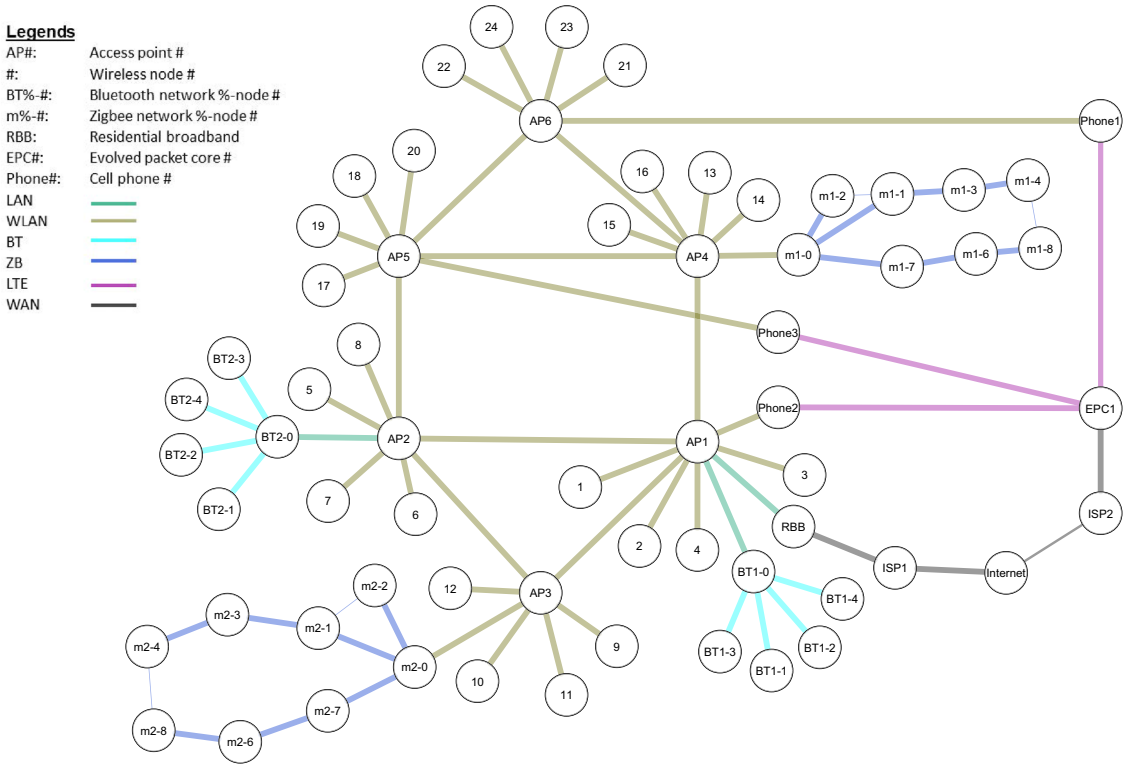


Fig. 6 An instance of a smart home with six access points

connect one to three cellphones to each constructed model after integrating the network technologies to the backbone. The cellphones are connected to the backbone nodes randomly. There is no restriction with respect to connecting multiple cellphones to any particular backbone node. We also consider all cellphones have the same provider; therefore, they connect to the same ISP through 4G/LTE/5G networks.

The generated instances connect to the Internet through *RBB* node to establish diverse path. Spatial diversity through connecting to different *ISP*, and technological diversity (wired vs wireless) are the results of the cellphones and *RBB* connections.

We generate 1500 smart home instances with two and four network technologies (750 instances for each group) with the aforementioned conditions.

5.2 Analysis of smart home instances

In this section, we analyze generated instances from our framework explained in Sect. 5.1 with graph centrality metrics. During the analysis, we categorize all instances with the same number of nodes in their backbones in one group and study the effect of adding cellphones to the models as nodes supporting multiple technologies and increasing path redundancy. In Tables 4, 5, 6, 7 and 8, we calculate centrality metrics for each group of instances per a particular number of cellphone. All instances have the same number of network technologies. For each group, the mean centrality value is calculated along with a 95% confidence interval.

Furthermore, we study the effect of the number of network technologies in Figs. 8, 9, 10, 11 and 12. In the figures, instances with four network technologies (two mesh and two star networks) are compared with the corresponding instances with two network technologies. The figures also show the mean values with a 95% confidence interval for each corresponding metric.

We start our analysis by measuring general properties of the models. Tables 2 and 3 show values for the network diameter, average connectivity, algebraic connectivity, and efficiency of each group of instances without categorizing the calculated values for a particular cellphone number. Table 2 shows the results for instances with two network technologies while Table 3 shows the corresponding results for instances with four network technologies.

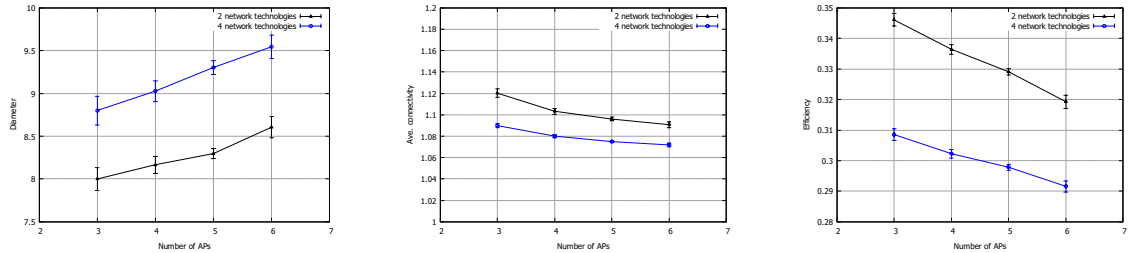
Figure 7a illustrates that the network diameters increase slowly when the number of nodes in the backbones increases; however, the increment is less than a unit. As expected, the instances with two network technologies have shorter diameter compared with instances with four network technologies; however, it shows that adding two network technologies with different topologies increases the network

Table 2 Graph measurement for models with two network technologies

No. APs	Measurement							
	Diameter	±Δ	Connect.	±Δ	Algebra.	±Δ	Efficiency	±Δ
3 APs	8	0.13335	1.12019	0.00388	0.07716	0.00285	0.34604	0.00208
4 APs	8.16667	0.09931	1.10333	0.00276	0.0736	0.00219	0.33642	0.00156
5 APs	8.29722	0.05964	1.096	0.0017	0.07364	0.0013	0.32907	0.00105
6 APs	8.60556	0.12547	1.0908	0.00259	0.06956	0.00228	0.31928	0.00218

Table 3 Graph measurement for models with four network technologies

No. APs	Measurement							
	Diameter	±Δ	Connect.	±Δ	Algebra.	±Δ	Efficiency	±Δ
3 APs	8.8	0.16868	1.08989	0.00206	0.06341	0.00324	0.30853	0.00188
4 APs	9.02667	0.12209	1.08008	0.00144	0.06027	0.00208	0.30229	0.00141
5 APs	9.30278	0.08285	1.07492	0.00101	0.05953	0.0013	0.29785	0.00094
6 APs	9.54444	0.13544	1.07186	0.00155	0.05862	0.00203	0.2916	0.00183



(a) Network diameter vs access points

(b) Average connectivity vs access points

(c) Efficiency vs access points

Fig. 7 Smart home graph measurement

Table 4 Betweenness centrality metrics for models

No. Phones	Betweenness					
	1 Phone		2 Phones		3 Phones	
No. APs	Mean	±Δ	Mean	±Δ	Mean	±Δ
3 APs	0.06812	0.007	0.06574	0.00786	0.06348	0.00655
4 APs	0.06285	0.00382	0.06045	0.00323	0.05868	0.00246
5 APs	0.05776	0.0019	0.05583	0.00187	0.05435	0.00178
6 APs	0.05433	0.00431	0.05276	0.00466	0.05123	0.0039

diameters nearly one unit. Diameter shows the longest shortest path in a network and can be utilized as an indicator to calculate delay. In small networks with the same size as the smart homes delay is negligent; however, when low-speed technologies are involved, each extra hop can add significant delay. Simulation is an adequate tool in such analysis compared to graph analysis when links have different properties (Modarresi and Symons 2020).

Figure 7b shows the results of the average connectivity (Beineke et al. 2002). In the figure, the values of the average connectivity decrease when the number of nodes increases. This figure also shows that instances with more network technologies have smaller connectivity compared with instances with fewer network technologies. The trend of decreasing network connectivity is slower when more access points are added to the network. The plots in Fig. 7b always stay above one since the models are connected. Adding more network technologies especially with star topology to an instance with a particular number of node decreases the current average connectivity. In addition, the results

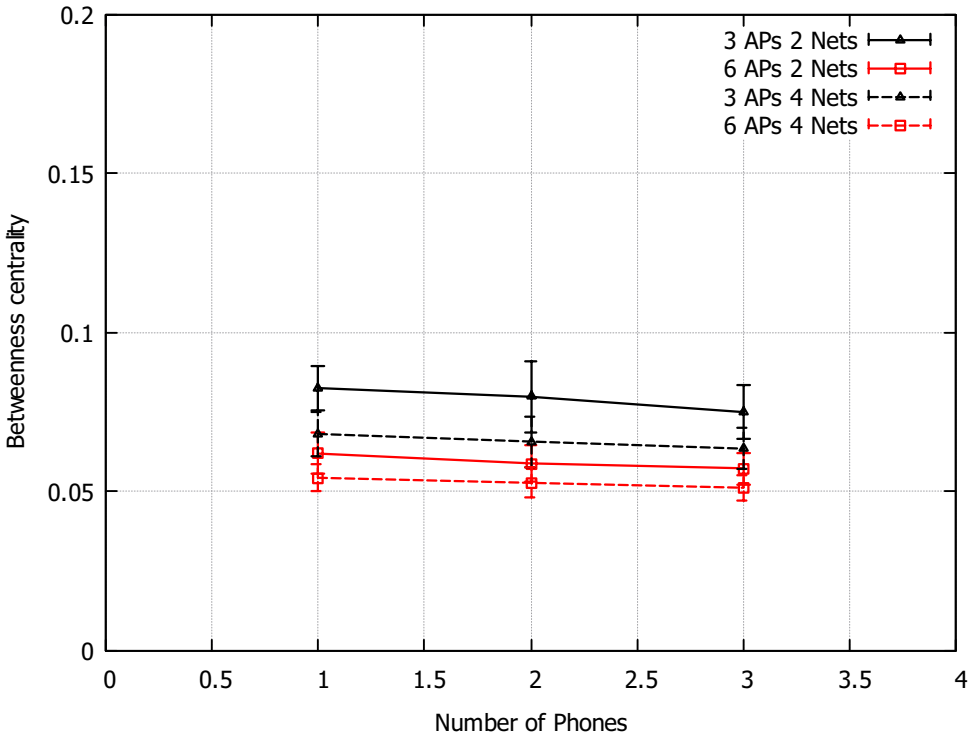


Fig. 8 Betweenness results for models with two and four network technologies

Table 5 Closeness centrality metrics for models

	Closeness					
No. Phones	1 Phone		2 Phones		3 Phones	
No. APs	Mean	$\pm\Delta$	Mean	$\pm\Delta$	Mean	$\pm\Delta$
3 APs	0.25623	0.0209	0.25892	0.0243	0.26138	0.02164
4 APs	0.25176	0.0117	0.25531	0.01049	0.25706	0.00838
5 APs	0.24969	0.00604	0.25256	0.00623	0.25431	0.0061
6 APs	0.24477	0.01418	0.24729	0.01547	0.24947	0.01383

show that the instances are partitioned approximately with one failure even if the backbones are bi-connected in most instances. Another conclusion, specifically in our study, is that star networks are dominant in the models since most of the nodes in star networks have degree one and keep the average connectivity low.

Algebraic connectivity in Tables 2 and 3 shows a decreasing trend meaning that the connectivity in the instances is getting weaker and the diameter is getting longer. This is because the number of nodes with a small degree, mostly degree one (edge nodes), is increasing.

Figure 7c illustrates that the values of efficiency has a decreasing trend in both groups of instances containing two and four network technologies. This is due to the fact that all nodes in any network technology connect to other nodes through their gateways. Therefore, there is no direct way for such nodes to communicate with other nodes outside their network.

Table 4 shows the mean values of the betweenness centrality for each group of models per number of cellphones. We observe that betweenness values decrease when both the number of nodes in the backbones and the number of cellphones in the models increase. However, in both cases, betweenness values decrease slowly.

Figure 8 illustrates the betweenness results for three-node-backbone instances with two and four network technologies, and six-node-backbone instances with two and four network technologies. We do not show the results for four and five-node-backbone instances in order to prevent overwhelming the figure. The results indicate that the value of betweenness decreases for all models when the number of cellphones increases. Moreover, though the overall betweenness values for all instances are small, we observe a distinct difference between three-node-backbone instances with two network technologies, compared with the rest of the instances. We can also observe that the slope in the

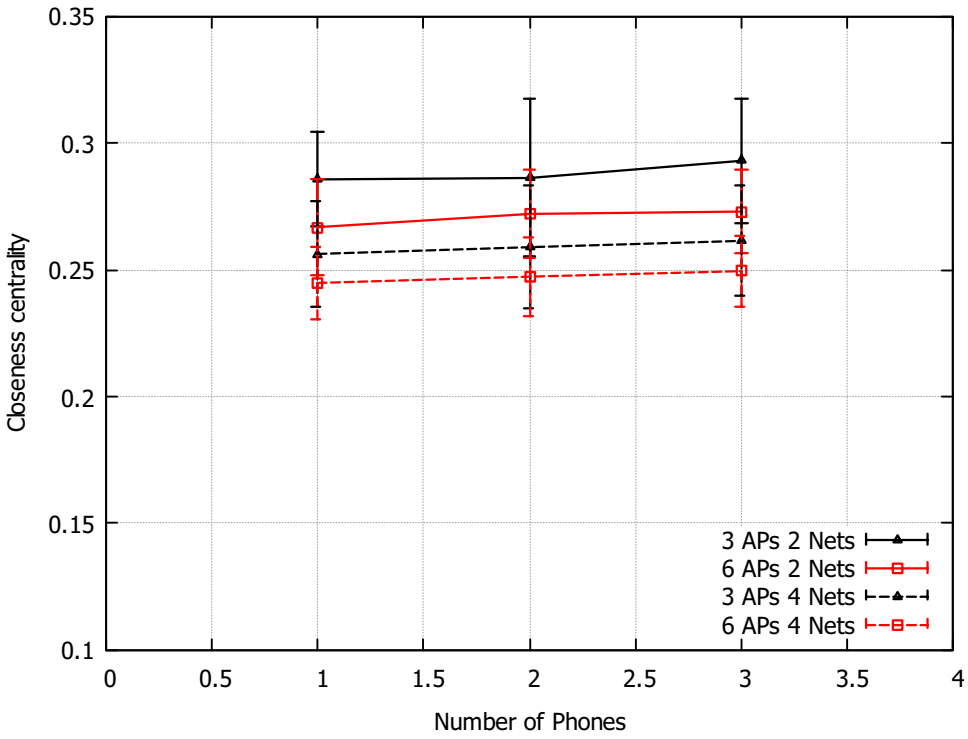


Fig. 9 closeness results for models with two and four network technologies

Table 6 Degree centrality metrics for models

No. Phones	Degree centrality					
	1 Phone		2 Phones		3 Phones	
No. APs	Mean	$\pm\Delta$	Mean	$\pm\Delta$	Mean	$\pm\Delta$
3 APs	0.04764	0.0014	0.04743	0.00134	0.0472	0.0013
4 APs	0.04314	0.00065	0.04296	0.00063	0.04277	0.0006
5 APs	0.03958	0.00039	0.03942	0.00037	0.03926	0.00037
6 APs	0.0364	0.00083	0.03627	0.0008	0.03613	0.00078

betweenness plot for the three-node-backbone models with two network technologies is steeper compared with other models in Fig. 8. We should emphasize that the values in Table 4 and Fig. 8 indicate the mean betweenness for all nodes. The growth of the number of nodes in the backbones increases the probability of establishing new shortest paths between each node pair resulting in decreasing the mean betweenness value. However, for a fixed number of cellphones, the large values belong to the three-node-backbone models due to the fewer number of nodes in the models compared with the rest of the models. In other words, increasing the number of network technologies decreases the betweenness values due to integrating more nodes. Regardless of the number of network technologies, increasing the number of cellphones has a negligible effect on the betweenness values.

Table 5 shows the closeness values for all instances per number of cellphones. Closeness shows the average shortest path values from any node v_i to other nodes. The larger value indicates that the nodes are closer to each other. The values in Table 5 indicate that neither adding a new node to the backbone nor integrating a new cellphone has a negligible effect on the closeness values. However, reducing the number of network technologies illustrated in Fig. 9 changes closeness values noticeably.

Table 6 shows the degree centrality values for all models per number of cellphones. Degree centrality values are relatively small for all models. The results in Table 6 indicates that the three-node-backbone models have the highest and six-node-backbone models have the lowest values. Integrated cellphones change the degree centrality values very slightly since cellphones have degree 2 in the models. The reason for very low mean centrality values is the number of edge nodes with degree 1. All nodes in a star topology except the central node have degree 1. Several star topologies have been integrated with each model resulting in low mean degree values. Adding more

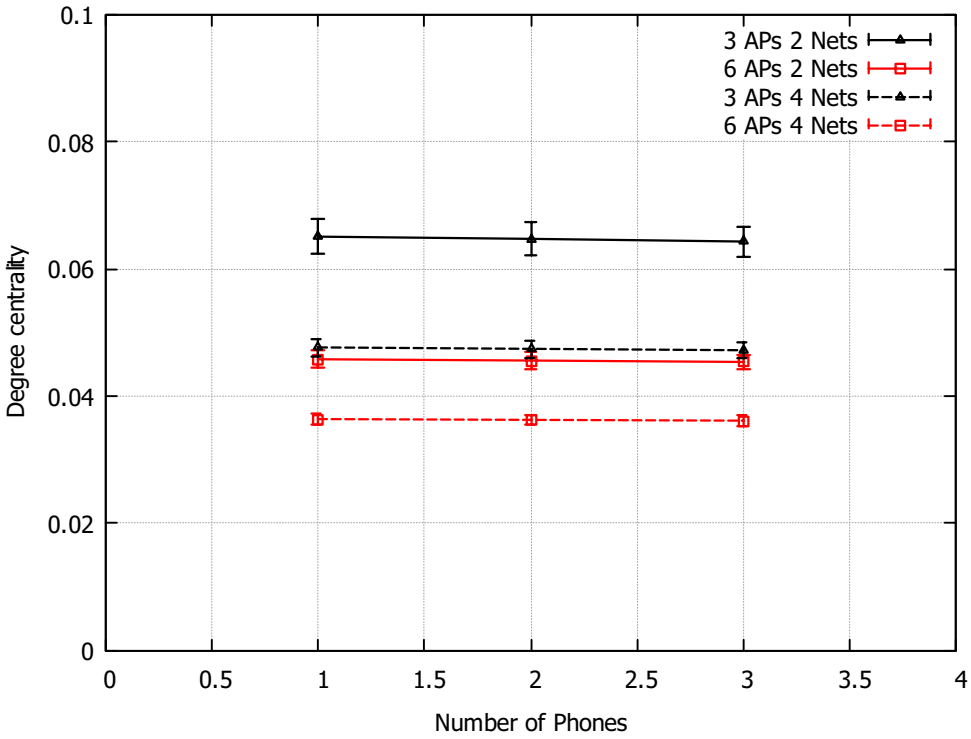


Fig. 10 Degree results for models with two and four network technologies

Table 7 Eigenvector centrality metrics for models

No. Phones	Eigenvector centrality					
	1 Phone		2 Phones		3 Phones	
No. APs	Mean	$\pm\Delta$	Mean	$\pm\Delta$	Mean	$\pm\Delta$
3 APs	0.10284	0.0083	0.10208	0.00744	0.10146	0.00731
4 APs	0.09448	0.0035	0.09411	0.00376	0.09357	0.00266
5 APs	0.08758	0.0017	0.08721	0.0015	0.08714	0.00142
6 APs	0.0852	0.00258	0.08536	0.00302	0.08515	0.00293

network technologies with a star topology reduces degree centrality more.

In contrast, removing technologies with a star topology increases mean degree centrality. Figure 10 shows changes in the mean centrality values. Furthermore, the number of wireless stations connected to the backbone nodes of the three-node models is fewer than other models resulting in increasing the mean degree centrality values. Figure 10 also shows that adding one extra cellphone changes the mean centrality values slightly while adding a network such as a star with low degree centrality values changes the mean centrality values noticeably.

We present the results of the mean eigenvector centrality values for all models per number of cellphones in Table 7. Since eigenvector centrality is an extension of the degree centrality, we observe that the number of cellphones does not change the mean eigenvector values sharply. When the number of nodes on the backbones increases, the amount of centrality values change even slower. In addition, the distance between the values of each plot decreases from three-node-backbone to six-node-backbone models. The distances between plots are much recognizable when the number of network technologies changes, as in Fig. 11, showing the results between two and four network technologies.

Katz centrality is an extension of the eigenvector centrality. However, in Katz centrality, the effect of the farther nodes in a walk decreases in the calculation of the centrality values. In addition, Katz centrality accepts weight for nodes to change their effect on the centrality values. Table 8 presents the value of the mean Katz centrality values. A noticeable change between the eigenvector and Katz centrality is that the Katz values are larger than eigenvector values. Regardless of this change, the trends of the values in both Tables 7 and 8 are identical.

The above results show that adding new cellphones does not change the centrality metrics values significantly,

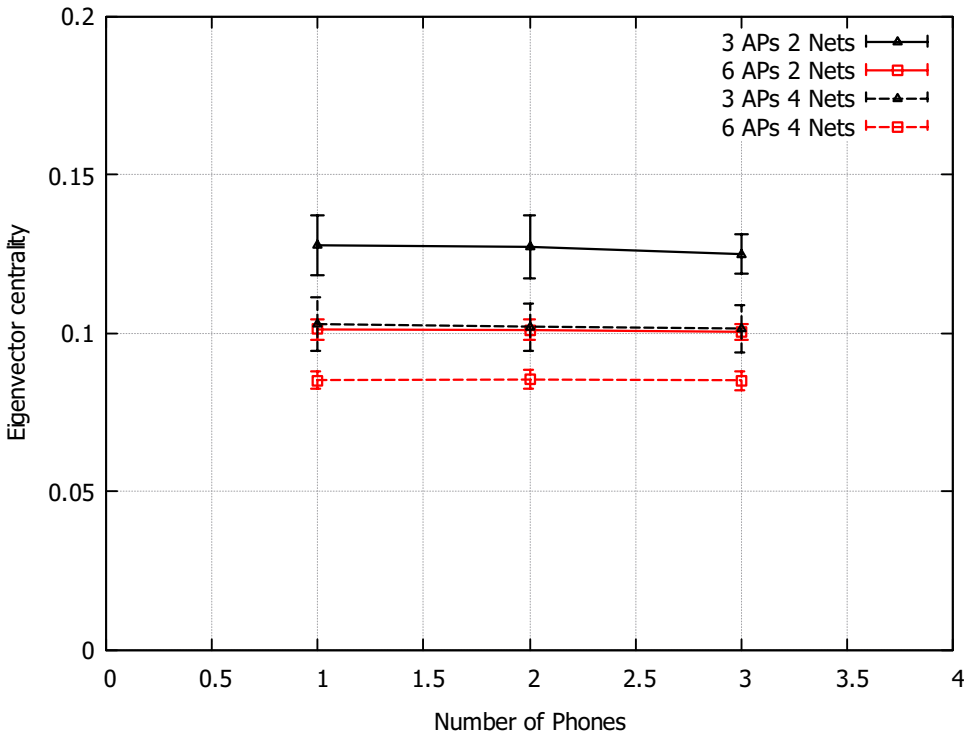


Fig. 11 Eigenvector results for models with two and four network technologies

Table 8 Katz centrality metric for models

No. Phones	Katz					
	1 Phone		2 Phones		3 Phones	
No. APs	Mean	$\pm\Delta$	Mean	$\pm\Delta$	Mean	$\pm\Delta$
3 APs	0.14327	0.00101	0.1416	0.00112	0.13998	0.0011
4 APs	0.13574	0.00054	0.13431	0.00054	0.13293	0.0005
5 APs	0.12915	0.00034	0.12793	0.00035	0.12671	0.00035
6 APs	0.12367	0.00074	0.12258	0.00076	0.1215	0.00075

although providing duplicate and diverse paths in a model improve the network resilience. As we have shown in previous work, a multilayer model can illustrate duplicate and diverse paths better than a single layer model (Modarresi et al. 2019).

The results also show that most centrality metrics have higher values for models with a small number of nodes in the backbone compared with larger networks with more nodes in the backbones. The intermediate results also reveal that for the most centrality metrics models with larger backbones and fewer network technologies have higher centrality values compared with the models with smaller backbones and more network technologies. For instance, models with five access points and two network technologies have higher Katz centrality values than models with three access points and four network technologies. We should emphasize that this relationship is only true for models that are one or two access points (nodes in the backbone) apart from each others.

6 Conclusion and future work

In this paper, we introduce and demonstrate the role of an abstract model for understanding the network properties of a complex IoT system. We focus on the relatively simple context of smart homes. We consider commonly used technologies and their corresponding network topologies with the goal of simplifying the representational complexity of networks composed of heterogeneous technologies. Our goal is to demonstrate how designers and engineers can take network topologies into account so as to develop more resilient IoT systems. In our analysis we show how to compare an instance of our model in the normal state and during the main Internet connection failure with other baseline topologies such as star and mesh using various graph centrality metrics. Our model represents a multi-technology network whose nodes have a variety of functionality

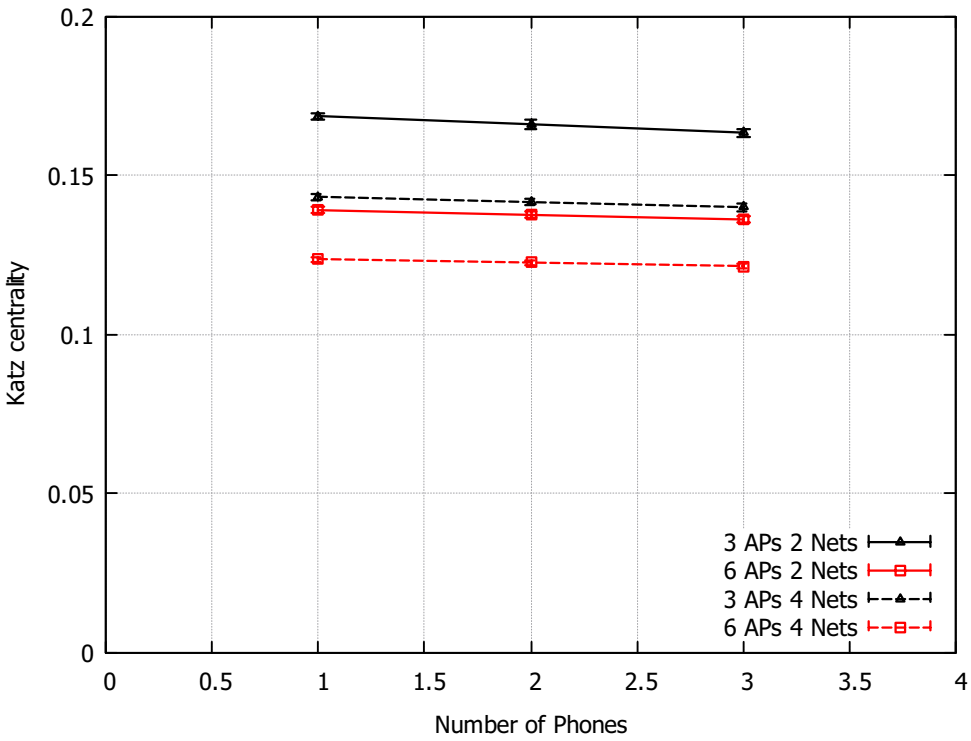


Fig. 12 Katz results for models with two and four network technologies

and different bit-rate links. In these contexts, centrality metrics typically fail to explain the correct behavior of the associated graph of the network. We identify which metrics are more applicable in light of the functions and importance of the nodes of the network. We perform the same analysis on our technology interdependence graph. This analysis provides valuable results without requiring researchers to consider all the details of intractably complex networks.

We show how to build controlled experimental studies of instances of these models and as an example, we analyze hundreds of instances of our smart home instances to study resilience of such networks through path redundancy and diversity when nodes such as cellphones with supporting multiple technologies are added. The results show that although the engineered home backbones can resist multiple node failures, the networks on average are one-connected and one failure can partition them. In addition, redundant paths do not change the mean values of the centrality metrics noticeably.

Our plan for the future research is to design centrality metrics sensitive to various link interactions. Such centrality metrics consider link diversity in the calculation providing more salient results compared to typical centrality metrics in which only path redundancy is considered.

Acknowledgements We are very grateful to the reviewers of this paper for their helpful suggestions and critical comments.

References

Beineke LW, Oellermann OR, Pippert RE (2002) The average connectivity of a graph. Discr Math 252(1–3):31–45

Bluetooth SIG (2015) Bluetooth. http://www.bluetooth.com/

Bluetooth Special Interest Group (2016) Bluetooth Core Specification v5.0. https://www.bluetooth.com/specifications/bluetooth-core-specification

Boutin C (2014) The internet's next big idea: connecting people, information, and things

De Paola A, Ferraro P, Re GL, Morana M, Ortolani M (2019) A fog-based hybrid intelligent system for energy saving in smart buildings. J Ambient Intell Hum Comput 1–15

Dinh HT, Lee C, Niyato D, Wang P (2013) A survey of mobile cloud computing: architecture, applications, and approaches. Wirel Commun Mob Comput 13(18):1587–1611

Fernando N, Loke SW, Rahayu W (2013) Mobile cloud computing: a survey. Fut Gen Comput Syst 29(1):84–106 Including Special section: AIRCC-NetCoM 2009 and Special section: Clouds and Service-Oriented Architectures

GSMA (2016) 3GPP low power wide area technologies. https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf

Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B (2019) A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7:82721–82743

Hernández JM, Van Mieghem P (2011) Classification of graph metrics. Delft University of Technology, Mekelweg, pp 1–20

ITU (2012) Terms and definitions for the internet of things. https://www.itu.int/rec/T-REC-Y.2069-201207-I/en

Jalili M, Salehzadeh-Yazdi A, Asgari Y, Arab SS, Yaghmaie M, Ghavamzadeh A, Alimoghaddam K (2015) CentiServer: a

comprehensive resource, web-based application and R package for centrality analysis. PloS One 10(11):e0143111
Kang U, Faloutsos C (2011) Beyond 'caveman communities': Hubs and spokes for graph compression and mining. In: 2011 IEEE 11th international conference on data mining, pp 300–309
Koschützki D, Lehmann KA, Peeters L, Richter S, Tenfelde-Podehl D, Zlotowski O (2005) Centrality indices, pp 16–61. Springer Berlin
Lake D, Rayes A, Morrow M (2012) The internet of things. Int Protocol J
Latora V, Marchiori M (2001) Efficient behavior of small-world networks. Phys Rev Lett 87(19):198701
LoRa Alliance (2016) LoRaWAN specification. https://www.lora-alliance.org/For-Developers/LoRaWANDevelopers
Maslov S, Sneppen K (2002) Specificity and stability in topology of protein networks. Science 296(5569):910–913
Minerva R, Biru A, Rotondi D (2015) 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
Moan LL (2017) SigFox website. https://www.sigfox.com/en
Modarresi A, Sterbenz JPG (2017) Multilevel IoT model for smart cities resilience. In: Proceedings of the 12th international conference on future internet technologies, CFI'17, pp 7:1–7:7, New York
Modarresi A, Sterbenz JPG (2018) Towards a model and graph representation for smart homes in the IoT. In: IEEE International Smart Cities Conference (ISC2) (ISC2 2018). Kansas City, USA
Modarresi A, Symons J (2019a) Modeling and graph analysis for enhancing resilience in smart homes. Proc Comput Sci 160:197–205
Modarresi A, Symons J, (2019b) Modeling technological interdependency in IoT - A multidimensional and multilayer network model for smart environments. In: 11th International Workshop on Resilient Networks Design and Modeling (RNDM) (RNDM 2019). Nicosia, Cyprus
Modarresi A, Symons J (2020) Technological heterogeneity and path diversity in smart home resilience: A simulation approach. In: Proceedings of the 11th international conference on ambient systems, networks and technologies (ANT), Warsaw, Poland. Elsevier
Johansen NT (editor) (2017). Z-wave plus device type specification. http://zwavepublic.com/specifications
NetworkX developers (2018) NetworkX: Software for complex networks. https://networkx.github.io/
Newman M (2010) Networks: an introduction. Oxford University Press, Oxford
OpenFog Consortium Architecture Working Group (2017). OpenFog reference architecture for fog computing. https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf
Paetz C (2018) Z-Wave Essentials. Christian Paetz, Jena
Pipa F, Symons J (2019) Towards an understanding of resilience with complex networks. In: Proceedings of the 6th annual symposium on hot topics in the science of security, page 26. ACM
Plantevin V, Bouzouane A, Bouchard B, Gaboury S (2019) Towards a more reliable and scalable architecture for smart home environments. J Ambient Intell Hum Comput 10(7):2645–2656
Shannon P, Markiel A, Ozier O, Baliga NS, Wang JT, Ramage D, Amin N, Schwikowski B, Ideker T (2003) Cytoscape: a software environment for integrated models of biomolecular interaction networks. Genom Res 13(11):2498–2504
Design Sigma (2018) Z-wave. Online
Streitz N (2018) Beyond 'smart-only' cities: redefining the 'smart-everything' paradigm. J Ambient Intell Hum Comput 10:791–812
Symons J, Louçã J, Morais A, Rodrigues DM (2007) Detecting emergence in the interplay of networks. Emergent Agents and Socialities, In AAAI Fall Symposium, pp 86–93
Vaquero LM, Rodero-Merino L (2014) Finding your way in the fog: towards a comprehensive definition of fog computing. SIGCOMM Comput Commun Rev 44(5):27–32
Watts DJ (1999) Networks, dynamics, and the small-world phenomenon. Am J Sociol 105(2):493–527
Wi-Fi Alliance (2018) Wi-Fi Direct. https://www.wi-fi.org/discover-wi-fi/wi-fi-direct
Wikipedia (2018) k-edge-connected graph. https://en.wikipedia.org/wiki/K-edge-connected_graph
Alliance ZigBee (2008) Zigbee document 053474r17. ZigBee Specification, ZigBee Alliance
Zuniga J, Ponsard B (2016) SigFox system description. https://tools.ietf.org/html/draft-zuniga-lpwan-sigfox-system-description-01