Available online at www.sciencedirect.com

ScienceDirect

00 (2018) 000–000

Procedia
Computer Science

www.elsevier.com/locate/procedia

The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks
(EUSPN 2019)
November 4-7, 2019, Coimbra, Portugal

Modeling and Graph Analysis for Enhancing Resilience in Smart Homes

Amir Modarresi*[a], *JohnSymons*[a]

[a]*The University of Kansas, Lawrence, KS 66045 USA*

Abstract

A number of network technologies applicable to home networking have emerged for various purposes in recent decades. Ethernet and IEEE 802.11 WLAN provide the home network backbone, along with a range of competing technologies for sensors and home automation such as IEEE 802.15.4/ZigBee, Z-Wave, and Bluetooth LE. Technologies in the home vary with respect to their importance. In this paper, we provide a model smart home network and analyze its graph-theoretic properties with an emphasis on the resilience of critical services and connections to the Global Internet. We consider both the network connectivity graph of nodes and links, and our novel *technology interdependence graph*. We explore the resilience of the network technologies in the smart home in light of complex technological interdependency. We analyze these graphs and discuss properties such as diameter, closeness, centrality, and k-connectedness. We explain why this analysis is a necessary pre-condition for understanding IoT-based smart-city resilience.

Keywords: Smart home; graph analysis; modeling; network resilience; future networks

1. Introduction

Diverse technologies currently support the varied 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 to ZigBee [17], Bluetooth [1], and Z-wave [14, 9] for low-energy consumption and low bit rate. Other very-low bit rate and long-range technologies such as LoRaWAN [5], Sigfox [7, 18], and NB-IoT [2] contribute to services requiring very low-energy consumption such

* Corresponding Author. A. Modarresi. Tel.: +1-733-492-1757.
E-mail address: amodarresi@ittc.ku.edu

as structure monitoring and leak management. The topologies of these network technologies range from star to mesh. Combining these technologies can result in a complex network even in a small network such as a home.

A typical smart home system is a combination of various sensors, actuators, controllers, control networks, and gateways [12]. The sensors generate data and send them to the controllers through control networks such as ZigBee or Z-Wave networks. The controllers manage the devices in the network containing actuators and sensors through the control networks while they are connected to the gateways to provide interconnection with other communication networks.Though this is the typical structure of a smart home system, what makes each of those systems different is the type of network technologies used. These determine the topology of the networks, the number of such network technologies, the overall network size, and the variation of the technologies leading to the complexity of the networks. On the other hand, 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. The heterogeneity of the technologies in one network can potentially improve resilience through diversity given suitable design principles. For example, since each network technology is self-contained, any disruption to the operation of the network technologies renders only that individual network inaccessible. However, when devices such as laptops and cell phones support various technologies, they can operate in many networks at the same time increasing the availability of the overall system and consequently network resilience.

In this paper, we present a home network model for smart home architectures and perform a graph-theoretic analysis on this model. The rest of this paper is organized as follows. In Section 2, we present our home network model and smart home abstract model. In Section 3, we perform a graph-theoretic analysis on the model. Finally, we conclude our paper in Section 4.

2. Smart home model

We have previously introduced a model for the interaction of technologies that will likely be typical in smart homes of the near future [8]. Our *connectivity graph* led us to our *technology interdependence graph* confirming that a high-bit-rate technology such as WLAN serves as the smart home backbone network. Other network technologies connect to this backbone. Given that result, we introduce our smart home abstract model in Part 2.1. Then, we present our home network graph representation model produced by Python NetworkX [10] for the smart home network in Part 2.2. The goal is to model a typical smart home network architecture in order to explore ways to improve network resilience.

2.1. Smart home abstract model

A first step toward creating a graph model that can be used for analytic and simulation-based analysis is to create an abstraction for the smart-home network. Our *smart home abstract model* is depicted in Figure 1. This shows the architecture and high-level structure as *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 technology. However, at the network layer it appears to be 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 topology, protocols, and addressing. Because of this difference, they generally only interconnect through gateways to the home backbone, resulting in a star topology of networks, of which two are shown in the figure.

Homes are typically connected to the Global Internet, traditionally for user access such as Web browsing and email. Additionally many *smart* home services use connectivity for remote access, e.g. controlling lights when away from home. 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 from 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 cut, and wired if the wireless channel is disrupted by heavy precipitation or jamming.

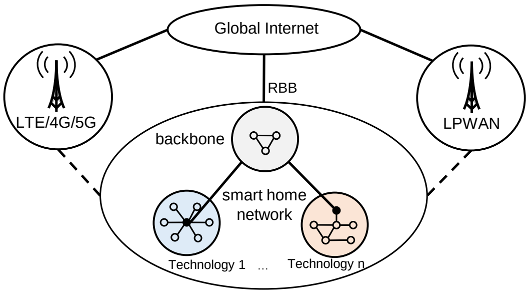
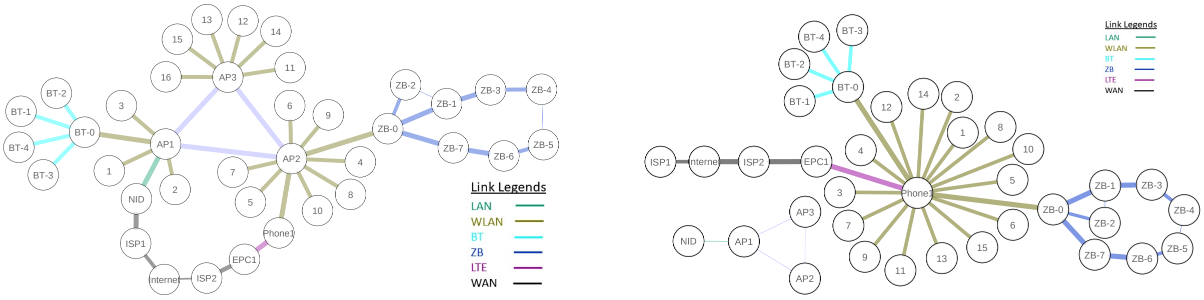


Fig. 1: Smart home abstract model



(a) Connectivity graph of the home network model

(b) Connectivity graph of a the backup topology

Fig. 2: Smart home connectivity graphs

2.2. Technologies in smart home model

As presented in Figure 2a, high-bit-rate LAN technologies including Ethernet, 802.11, and 802.11s are used as the home backbone. While wireless LANs are dominant to construct the home backbone, they may suffer interference in a dense urban environment and may 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 spanning tree overlay on top to avoid loop in the network. Considering network resilience, a mesh network with k-connectivity 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 construct 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 are the 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 typical technologies utilized in the network technologies of a smart home, including ZigBee and Z-Wave, can construct mesh topology. Other technologies including Bluetooth build star topology. Furthermore, Bluetooth can construct mesh topology by changing the role of a slave to a master node and vice versa.

While most of the low-bit-rate technologies such as ZigBee support a mesh topology, the ultimate topology of such networks depends on the density of the nodes in the network, the average distance among nodes, and the specialized nodes utilized in a particular technology such as coordinators and routers. The topology may be a star which is 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, and 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 has the capability of generating a particular number of cliques with a specific size. This structure can emulate a controlled mesh network. We process the produced graph from caveman 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 the networks with more nodes. Since these network technologies are low bit rates and self-contained, any structural changes or failure have no or minor effects on the home backbone LAN. Therefore, these networks can be studied separately.

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 cell phone can join the network through its 802.11 interface and act as a wireless station. However, during a WAN failure, a tethered cell phone 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 of this group, 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 out 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 does 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 Figure 2a assuming that the two ISPs are reachable with one hop to simplify the structural complexity of the Internet.

3. Graph-theoretic representation and analysis

In order to analyze our model, we present a formal graph representation. Then, we calculate various graph analysis metrics and compare with baseline home network architectures, including star and mesh, to study the characteristics of our model. We perform a similar analysis on our technology interdependence graph as the logical representation of the typical technologies employed in a smart home without any constraint to the physical details of a particular network and its associated components.

3.1. Home network model analysis

Given our home network model, we define an edge-coloured graph $\mathbb{G}_{\text{conn}} = (V_c, E_c, C, \chi)$ as the connectivity graph illustrated in Figure 2a, 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 $\chi : E_c \to C$ is a function to assign a color to each edge. Precisely, we can define E_c as $E_c = \{((v_i, c_i), (v_j, c_i)) \in V_c \times V_c | \chi(v_i, v_j) = c_i\}$.

We start this analysis by evaluating two baseline topologies: star and mesh backbone. 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). At the next step, we consider our home network graph (Figure 2a) and compare 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* ↔ *ISP1*) failing over to the backup access path through *Phone1*, illustrated in Figure 2b. The number of 802.11 wireless workstations are the same in both 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 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 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 [15] on the mesh nodes and the cell phone or the cell phones are equipping 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 the above 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. The distance metric measurements are based on the shortest path and the number of hop count over the shortest path. The node-degree values are the main consideration for connectivity-based centrality metrics. Finally, eigenvalues and eigenvectors are the base 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 finding proper centrality metrics from these groups to describe our multi-technology model. One should note that the thickness of each edge in Figures 2a and 2b represent the value of edge-betweenness centrality (number of traversing shortest paths) computed by Cytoscape [13]. 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.

3.1.1. Distance-based centrality metrics

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

The network *diameter* represents the longest shortest path in the network. This is a metric that represents the minimum number of hops to connect the farthest pair node 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 the Internet access link failure, the backbone component is partitioned; therefore, the diameter value of the larger component decreases, causing changes in the value of metrics depending on the shortest path metrics. However, the shortened diameter, in this case, may not significantly change delay; because, one high-speed component of the network has failed, and all network technologies with low-speed connectivity are 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 perceive the reachability of vertex v_i. The higher value shows the proximity of node v_i to other nodes. Eccentricity decreases from star to our home network graph due to adding 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 considered in the smart home network design. We provide the eccentricity results in Table 1.

Closeness centrality calculates the average shortest path for any node v_i to other nodes in a network. Closeness centrality deals with 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 and it shows 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 nodes 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 as 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 Figures 2a and 2b 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. 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 observed during failure since the only high speed and long range available technology is LTE. Locating in a smart city with wireless access connectivity, it may provide another path to the Internet with a restriction; because all nodes should connect to the citywide wireless network as a station.

Although edge betweenness centrality may identify important edges that connects technology variants to the backbone network, it cannot recognize 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. One possible solution to alleviate the criticality of such nodes is installing redundant nodes in the same area by increasing system cost. Another solution is using a node supporting different technologies to participate in various network technologies by sacrificing energy consumption.

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 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 on edges can increase the accuracy of the measurement, weight normalization should also be considered in a multi-technology network. 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.

3.1.2. Connectivity-based centrality metrics

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

Degree centrality in the communication networks is a measure of the importance of a node with respect to how well-connected it is. A higher degree for a particular node 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 the 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 whole 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 [6, 3]. 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 $G' = (V, E \setminus X)$ 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 $v_i \in V$ [4, 16]. k-vertex connected graph is defined similarly.

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

3.1.3. Spectra centrality metrics

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

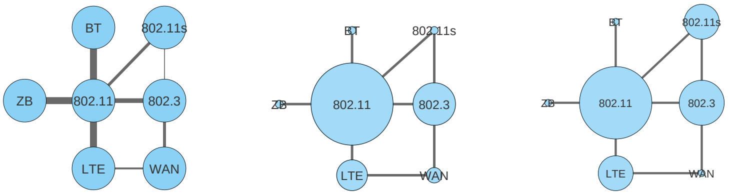
Eigenvector centrality is an extension of degree centrality that considers the importance of a node as its number of connections to the other important nodes [11]. Although this metric can identify an important node based on its number of connections in a homogeneous network, it cannot recognize such nodes in a multi-technology network especially with battery-operated nodes that they 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 [4, 11]. 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.

3.2. Technology interdependence model analysis

Our *technology interdependence graph* is the result of a one-mode projection over the incidence matrix of the smart home connectivity graph [8]. This graph illustrates the relationship among employed 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 provides more intuitive results. We perform the same analysis as we provide in Subsection 3.1 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 3a illustrates the result of the edge betweenness of our technology interdependence graph. The thickness of the edges represents the betweenness quantity. Both short-range technologies utilized 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.If a cell phone with a Bluetooth interface joins the Bluetooth network (not shown in the figure), 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 cell phones or laptops, we can expect the same resilient improvement for ZigBee.



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

Fig. 3: Technology interdependence graph centrality metrics

Table 1: The graph metrics for the various topologies

		Model				
Graph centrality metrics		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

In Figure 3b the size of each node represents the value of the 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, we suggest that any critical node equips with multiple technologies according to their level of criticality.

Figure 3c 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.

4. Conclusion and future work

In this paper, we introduce our network model for smart homes. We consider commonly used technologies and their network topologies with the goal of simplifying the representational complexity of networks composed of heterogeneous technologies. We compare our model in the normal state and during the main Internet connection failure with other baseline topologies such as star and mesh through various graph centrality metrics. Our model represents a multi-technology network whose nodes have a variety of functionality 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 the case of the communication 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 highly complex and diverse networks.

Acknowledgements

This work is funded by NSA Science of Security initiative contract #H98230-18-D-0009. We are greatly indebted to James P.G. Sterbenz whose work has been fundamental for this analysis.

References

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

[2] GSMA, . 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.

[3] Jalili, M., Salehzadeh-Yazdi, A., Asgari, Y., Arab, S.S., Yaghmaie, M., Ghavamzadeh, A., Alimoghaddam, K., 2015. CentiServer: a comprehensive resource, web-based application and R package for centrality analysis. PloS one 10, e0143111.

[4] Koschützki, D., Lehmann, K.A., Peeters, L., Richter, S., Tenfelde-Podehl, D., Zlotowski, O., 2005. Centrality Indices. Springer Berlin Heidelberg, Berlin, Heidelberg. pp. 16–61. doi:10.1007/978-3-540-31955-9_3.

[5] LoRa Alliance, 2016. LoRaWAN specification. https://www.lora-alliance.org/For-Developers/LoRaWANDevelopers.

[6] Maslov, S., Sneppen, K., 2002. Specificity and stability in topology of protein networks. Science 296, 910–913.

[7] Moan, L.L., . Sigfox Website. https://www.sigfox.com/en.

[8] Modarresi, A., Sterbenz, J.P.G., 2018. Towards a model and graph representation for smart homes in the IoT, in: 2018 IEEE International Smart Cities Conference (ISC2) (ISC2 2018), Kansas City, USA.

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

[10] NetworkX developers, . NetworkX: Software for complex networks. https://networkx.github.io/.

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

[12] Paetz, C., 2018. Z-Wave Essentials. Christian Paetz. URL: https://books.google.com/books?id=t80nDwAAQBAJ.

[13] Shannon, P., Markiel, A., Ozier, O., Baliga, N.S., Wang, J.T., Ramage, D., Amin, N., Schwikowski, B., Ideker, T., 2003. Cytoscape: a software environment for integrated models of biomolecular interaction networks. Genome research 13, 2498–2504.

[14] Sigma Design, . Z-wave. http://z-wave.sigmadesigns.com/.

[15] Wi-Fi Alliance, 2018. Wi-Fi Direct. https://www.wi-fi.org/discover-wi-fi/wi-fi-direct.

[16] Wikipedia, . k-edge-connected graph. https://en.wikipedia.org/wiki/K-edge-connected_graph.

[17] ZigBee Alliance, 2008. Zigbee document 053474r17. ZigBee Specification, ZigBee Alliance .

[18] Zuniga, J., Ponsard, B., . SigFox system description. https://tools.ietf.org/html/draft-zuniga-lpwan-sigfox-system-description-01.