Multilevel IoT Model for Smart Cities Resilience

Amir Modarresi
Information and Telecommunication Technology Center
Electrical Engineering and Computer Science
The University of Kansas, Lawrence, KS 66045, USA
amodarresi@ittc.ku.edu

James P.G. Sterbenz
Information and Telecommunication Technology Center
Electrical Engineering and Computer Science
The University of Kansas, Lawrence, KS 66045, USA
School of Comp. and Comm. (SCC) and InfoLab21
Lancaster University, LA1 4WA, UK
Computing, The Hong Kong Polytechnic University
Hung Hom, Kowloon, Hong Kong
jpgs@{ittc.ku.edu|comp.{lancs.ac.uk|polyu.edu.hk}}

ABSTRACT

Currently, the Internet of Things (IoT) is in the center of attention as an emerging technology among researchers and stakeholders. It is assumed that it is a key enabler for other technologies such as smart cities, smart health, smart grids, and smart transportation. Although the concept of the IoT is generally understood among researchers, there is no standard model representing this technology, particularly with respect to network architecture, which will be necessary to apply existing and emerging resilience and survivability techniques. Additionally, security and privacy have not yet received the needed attention. In this paper we propose a new multilevel IoT network-centric model, and discuss its applicability to the application of resilience and survivability.

CCS CONCEPTS

• **Networks** → **Network structure**; **Cyber-physical networks**; *Network simulations*; • **Computer systems organization** → **Dependable and fault-tolerant systems and networks**;

KEYWORDS

Resilient, survivable, and dependable Future Internet; IoT, fog, cloud, and smart-city architecture and topology; multilevel modelling; ns-3 simulation

ACM Reference format:
Amir Modarresi and James P.G. Sterbenz. 2017. Multilevel IoT Model for Smart Cities Resilience. In *Proceedings of CFI'17, Fukuoka, Japan, June 14-16, 2017,* 7 pages.
https://doi.org/10.1145/3095786.3095793

1 INTRODUCTION

The basis for the Internet of Things (IoT) goes back many years when the Auto-ID Center at MIT introduced low cost radio frequency identification (RFID) to store serial numbers on a microchip embedded in merchandise tags. The idea was to decrease the price by using simple microchips at high frequencies instead of using complex chips with memory. This concept was developed to connect objects to the Internet through the tags with their information kept in databases [20]. Since then this idea has been enhanced with various terms applied, including the *Internet of Things* or *Internet of Everything*. Although this has become a hot area of research, to the best of our knowledge there is still no standard universally-accepted model for the IoT. For example, Cisco describes the IoT as a point in time when the number of connected devices to the Internet exceed the population of the earth [3]. Despite a number of proposed models for the IoT, they are generally conceptual with a high-level of architectural abstraction. IEEE describes the IoT as a network of elements embedded with sensors connecting to the Internet [21]. The International Telecommunication Union (ITU) defines the IoT as a global infrastructure that enables advanced services by interconnecting things with current communication technologies [12]. ITU has also updated the definition of the telecommunication system for the IoT by adding "anything" to it. *Anything* in this definition means any type of communication among humans, computers, and "things" (smart devices). The Internet Engineering Task Force (IETF) focuses on potential factors for enabling the IoT communication by considering RFID tags, sensors, and mobile phones as enablers of this technology. The National Institute of Standards and Technology (NIST) defines the IoT as a cyber-physical systems (CPS) technology to connect smart devices in various sectors such as transportation, health care, and energy [5]. Finally, Cisco in the commercial sector defines the IoT under the umbrella of "Internet of Everything" as a technology to connect people, processes, data, and things to change the information to valuable experiences, capabilities, and economic opportunity [13].

As is obvious from all of the above definitions, the current focus is enabling the IoT and explaining its capabilities and features, while other critical factors such as security, survivability, resilience, and privacy are yet to receive the attention they deserve. Recent events such as the cracking of the Nest thermostats [7] and automobiles [28], as well as the exposure of Samsung vulnerabilities [4], and the prospect of cracking[1] of interdependent infrastructures [19] highlight the importance of addressing these issues. In this paper, we propose a *multilevel* model [25] prepared to apply resilience and survivability concepts in the face of large-scale disasters or attacks. The rest of the paper is organised as follows: Section 2 presents some of the significant IoT models and summarises the

CFI'17, June 14-16, 2017, Fukuoka, Japan

ACM ISBN 978-1-4503-5332-8/17/06…$15.00
https://doi.org/10.1145/3095786.3095793

[1] We use the term "cracking" for *unethical* hacking.

ResiliNets resilience strategy and principles as background and related work. In Section 3, we introduce our model of the IoT in the context of smart cities. Section 4 describes how we apply our ResiliNets resilience methodology to our multilevel IoT network model. In Section 5, we present our preliminary experimental evaluation. Finally, we conclude our paper in section 6.

2 BACKGROUND AND RELATED WORK

This section provides a brief summary of current IoT models, and to the ResiliNets architecture as the basis for resilience, survivability, and dependability.

2.1 Current IoT Models

One of the simplest models for the IoT has been introduced by IEEE P2413 [10]. It is a three-tiered model including sensing objects, the communication network, and application layers. In this model, sensing objects ("things") are in the first level of the model. The entire communication network is located as the middle level of this model while applications are the top level. While this model explains the major parts of the IoT, it does not provide any detail for each level, needed for resilience analysis. IEEE P2413 is currently an active group that works standardising the IoT framework.

The ITU Y.2060 model illustrated in Figure 1 [11] focuses on integrating things to the communication networks, divided into two groups: objects in the physical world (*physical things*), and objects in the information world (*virtual things*) [12]. A device is the entity that maps every physical object into the information world, and must have communication capability. Devices can communicate with each other directly or through a gateway based on their communication capabilities and supported protocols. Other capabilities such as processing, sensing, or actuation are optional for such devices [11]. Although this model identifies a clear distinction between physical and logical worlds, it also does not provide any details about the communication network structure.

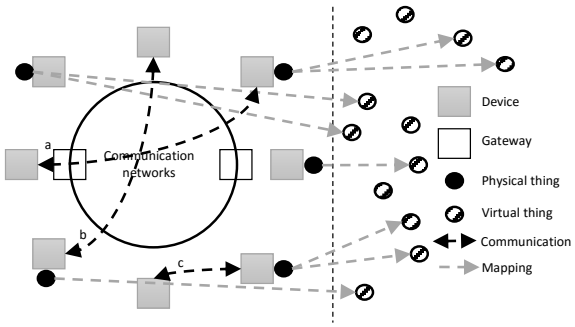


Figure 1: ITU overview of the IoT [11]

Cisco has introduced a seven-level IoT reference model, illustrated in Figure 2, considering physical devices, edge computing, people, and business processes [1]. In this model all physical end-devices including sensors and edge nodes are placed in the lowest *edge* level. Network devices and communication systems are defined in the second *connectivity* level. The third *edge computing* level is responsible for local packet-based processing [2] on behalf of simple devices with less processing power, data filtering, and transformation capabilities. The results may be stored for a short period of time in the *fog*, and are passed to the fourth *data accumulation* level for longer storage. After performing data integration and aggregation in the fifth *data abstraction* level, business analysis and reporting are conducted in the sixth *application* level. The top seventh *collaboration & processes* level is the place to impose policies to the whole system. While this is an interesting abstraction of the functional relationships of the IoT processing, it does *not* correspond to the physical and logical network layers needed for resilience, described in our model in Section 3.

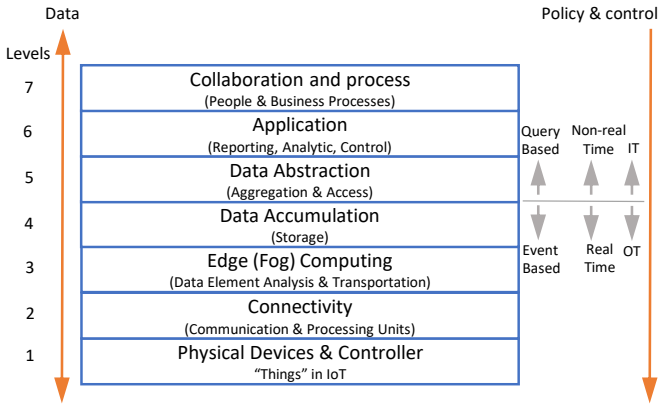


Figure 2: Cisco IoT reference model [1]

2.2 Resilience and Survivability Principles

We now briefly review our ResiliNets strategy and principles [24] that we have previously used to analyse a number of Internet and domain-specific networks (such as MANETs – mobile ad hoc networks). We define resilience as *the ability of the system to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation* [23, 26]. We also define survivability as *the ability of the system to tolerate correlated failures resulting from large-scale disaster and attacks* [23, 26]. Survivability is a required attribute for network resilience.

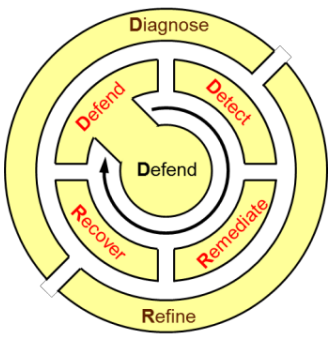


Figure 3: ResiliNets strategy

The ResiliNets strategy D^2R^2 + DR is shown in Figure 3, and consists of two control loops: An inner loop to *defend* against challenges (consisting of structural defences in the middle, and active defences as part of the control loop), *detection* of challenges (including attacks and large-scale disasters) that penetrate the defences, *remediation* to provide the best possible service during and immediately after a challenge, and *recovery* to normal operations. The outer *diagnosis* of faults and vulnerabilities and *refinement* of future design and operation are beyond the scope of this paper.

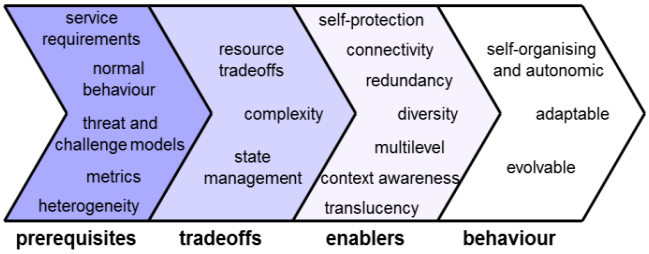


Figure 4: ResiliNets principles

In order to design resilient networks, ResiliNets has defined a set of principles; the ones most relevant to this paper are *redundancy* for fault-tolerance, *heterogeneity* and *diversity* for survivability, and *self-organising* and *adaptable* to remediate challenges. The application of this strategy and principles will be described in Section 3.

3 MULTILEVEL IOT MODEL

In this section, we introduce our multilevel model in Figure 5. As explained in the previous section, current IoT models provide levels of abstraction that are not aligned with the physical and logical network structure [25], nor do they capture the necessary details of diverse network architectures and protocols in use. For example, clouds, edge clouds (or fog), and things all have physical layer connectivity that must be represented at the lowest layer, as well as a higher logical (IP) network overlay level that can adapt to the changing lower level connectivity.

In our model, devices and physical links (wired and wireless) are at the lowest level. This includes backbone and access fibre to and in ISP networks, intra-cloud data centre and edge cloud links, layer-2 switches, as well as the interconnection to and among IoT devices and supporting physical network infrastructure such as Bluetooth masters, sensor network sinks, 802.11 base stations, and cellular access points.

Thus, this lowest layer consists of the physical topologies of a number of heterogeneous network technologies gatewayed to one-another directly, or to the Internet directly or through edge clouds. The edge clouds provide low-latency access to shared processing and storage for inexpensive low-capability things, and are thus located physically near IoT devices.

Above the physical infrastructure level is the logical network path and routing level. The basic idea of the IoT is connecting everything to one another, either directly via a base station within a PAN or LAN, or through the Global Internet with current and emerging networks technologies and protocols. Since the dominant networking protocol stack is TCP/UDP/IP with the *Internet hourglass waist* of IP, ideally all IoT devices in the edge networks should support IP. On the other hand, IPv4 can not easily scale to this massive increase in addressing, with IPv6 more capable; therefore, migration from IPv4 to IPv6 has been proposed to enable the IoT.

Furthermore, extremely inexpensive, simple, battery-powered devices including some sensors may have difficulty supporting the full TCP/UDP/IP protocol suite, and may be gatewayed to the Internet. These devices will require low power drain with limited transmission range, and have limited processing capability.

Emerging demand in the IoT market is encouraging sensor manufacturers to provide devices with standard communication protocols and supporting IPv6 to connect them directly to the Internet. These devices will be a mix of mains (wired into building power) and battery powered, and will be a mix of wired and wireless communication link technologies. In the case of battery-powered wireless things, low-energy technologies are important, including 802.15.4 sensors [9] with 6LowPAN [8, 17, 22] as an adaptation layer to carry IPv6, Bluetooth low energy (BLE) [6], LoRaWAN [14, 15], and Sigfox [16] devices.

Additionally, 802.11 and LTE-A 4G/5G will be important technologies in the IoT in smart cities context. While some sensors will be deployed as standalone things, the decreasing price of the sensors makes them more attractive as addons to more powerful devices such as mobile phones and smart watches. In this case, the problem of connectivity to the Internet is eased using the processing and communication power of the master device. For example, many mobile phones and tablets already support 802.11, Bluetooth, LTE, and near field communication (NFC).

Finally, above the network layer (not shown in the figure) are the end-to-end flows that things, users, and applications use to communicate on the paths created by the network layer below.

4 IOT RESILIENCE AND SURVIVABILITY

In this section, we discuss the application of our multilevel IoT network model to resilience analysis, with emphasis on a smart city scenario that is subject to attacks and large scale disasters, and with respect to interdependent critical infrastructures including the power grid and transportation.

An important property of the IoT is its high degree of heterogeneity. While this complicates system design, it is a property that can be *exploited* for resilience and survivability, particularly when some devices have multiple physical interfaces (e.g. LTE/LTE-A/5G, 802.11, Bluetooth, and NFC on mobile phones).

A key aspect of *defence* in the D^2R^2 + DR strategy is the *diversity* principle, manifest in communication medium and paths between communicating devices [25]. Multiple geodiverse paths defend against the area-correlated failures from a disaster, and multiple link technologies defend against attacks such as jamming and fibre cuts with an alternative available. The provision of geographically distributed edge clouds [27] with essential Internet services such as DNS and PKI ensures that parts of the network that are partitioned in *islands of resilience* can continue to operate as much as possible in *normal operations* meeting user and application *service specifications*. This assumes that power is available; thus the topologies and isolatability of interdependent infrastructures

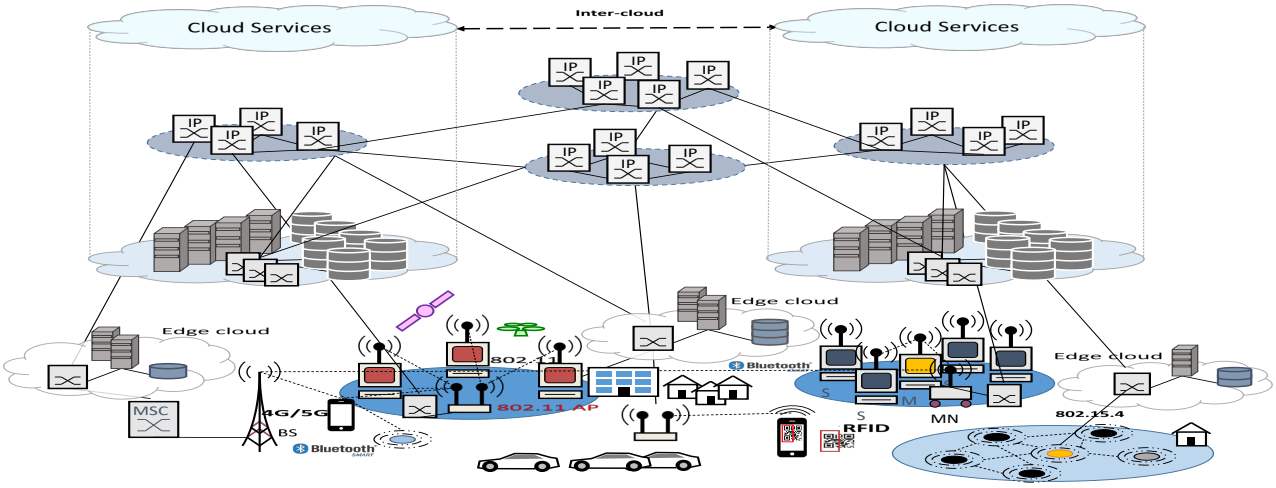


Figure 5: Multilevel IoT model

such as the power grid and attached microgrids match, so that the network can use the grid for power and the smart grid can use the network for SCADA (supervisory control and data acquisition).

The *detection* aspect of the D^2R^2 + DR strategy is enhanced beyond normal network monitoring procedures given the additional information and situational awareness capabilities of IoT sensors. For example, these sensors can help with disaster assessment by not only reporting connectivity, but with building, vehicle, and city sensors able to report on the type of disaster or attack (e.g. fire, earthquake, flood, storm, or biochemical) as well as determine the extent by using edge detection algorithms.

The *remediation* aspect of the D^2R^2 + DR consists of using *self-organisation and autonomic* behavior to *adapt* to the attack or disaster. In this case, *heterogeneity* is exploited to use communication media not affected: wired, fixed terrestrial wireless, mobile wireless through vehicles, airborne through drones, and satellites. The increasing ubiquity of mobile things such as smart cars and drones greatly enhances the ability to rapidly deploy temporary network infrastructure for remediation.

5 EXPERIMENTAL EVALUATION

As illustrated in Figure 5, an IoT network is complex due to the involvement of various standards and protocols. In order to evaluate our model, we create a topology for preliminary evaluation. Figure 6 shows this topology implemented in ns-3 [18], in which we use 802.15.4 in the left side of the network to generate low bit-rate traffic. These nodes use 6LoWPAN as their network layer to provide IP connectivity. The nodes are connected to a LAN through a coordinator. The right side of the LAN is connected the other nodes with point-to-point links. We place two wireless networks, namely WS1 and WS2 in Figure 6, simulating gateways for high bit-rate traffic. In order to simulate the cloud, we connect a server to the network by two paths: one with high-bandwidth and low-delay, and the other with relatively low-bandwidth and high-delay link to represent distance of the cloud from the edge networks. We generate three on-off source-traffic TCP flows from various parts of the network. The network WS1 generates Flow 1. Flow 2 starts from WS2, and finally an 802.15.4 gateway generates Flow 3. The dynamic routing mechanism in ns-3 simply chooses the shortest path to the destination without considering any delay or bandwidth metrics. Therefore, Flows 1 and 3 take the 2.5 Mb/s link, and Flow 2 takes the 10 Mb/s link illustrated in Figure 6.

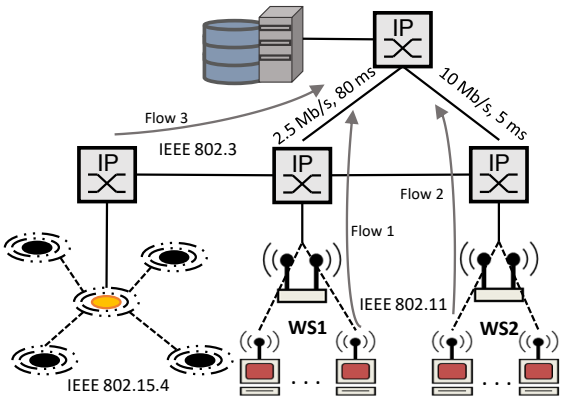
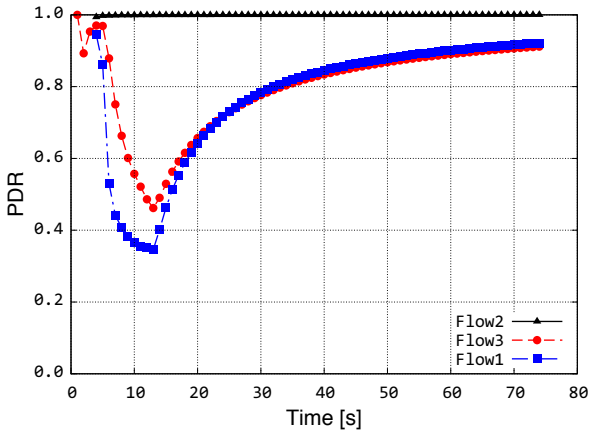
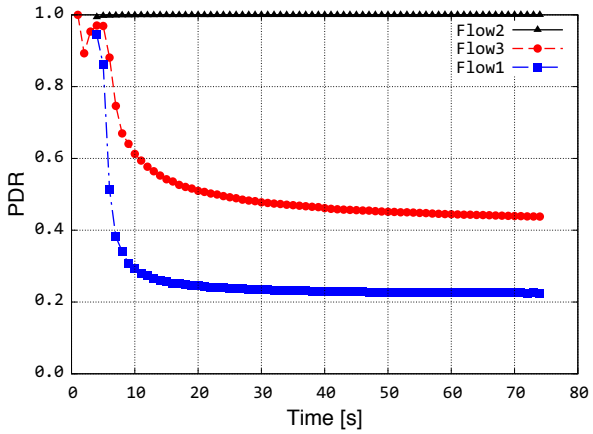


Figure 6: Simulation topology

The 802.15.4 network generates low bit-rate traffic representing the result of reading from sensors with small payload. We study the effect of various conditions on this flow. We conduct three scenarios: *lossless* without any error in the network, *lossy* with 1% BER (bit error rate) on the high-speed 10 Mb/s link, and *intermittent* with a 2 s disconnection every 20 s (but zero BER in the channel). For each scenario, two cases are run: 1.8 Mb/s load on the low-speed (2.5 Mb/s) link, and 2.0 Mb/s load on the low-speed link for Flow 1 experimentally chosen to just saturate. Table 1 shows the simulation parameters for each scenario.



(a) 1.8 Mb/s load



(b) 2.0 Mb/s saturating load

Figure 7: Lossless scenario PDR

Parameters	Value
duration	75 sec
packet size – Flow 1,2	300 Bytes
packet size – Flow 3	50 Bytes
data rate – Flow 1	1.8 and 2.0 Mb/s
data rate – Flow 2	2.0 Mb/s
data rate – Flow 3	150 kb/s
BER	1% on high speed link
link disconnection	2 sec for each 20 sec
traffic-source	on-off TCP

Table 1: Simulation Parameters

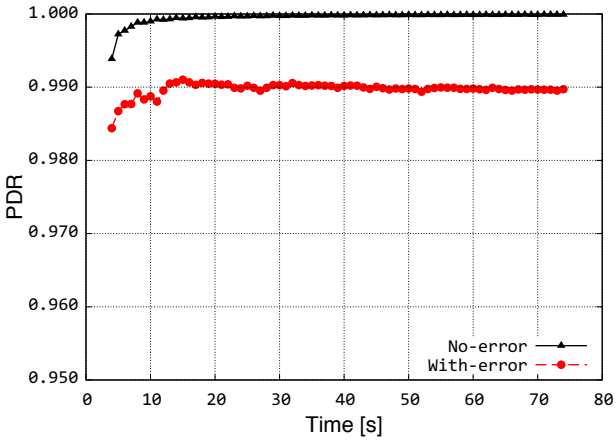


Figure 8: PDR – Lossless vs. lossy for Flow 2

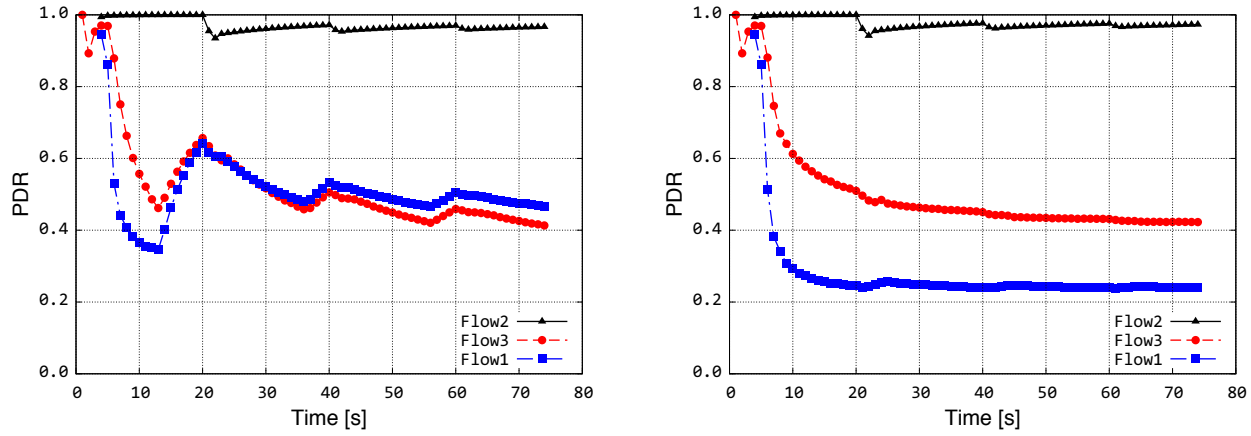
Figure 7a illustrates PDR (packet delivery ratio) for each flow in the lossless scenario with 1.8 Mb/s load for Flow 1. Both the high-speed and low-speed links have enough bandwidth capacity to carry all traffic. Hence, the packet size, traffic rate, and link delay are important factors in this scenario. Furthermore, there is some extra capacity on the high-speed link, therefore, there is no significant loss in Flow 2. On the other hand, the capacity of the low-speed link can barely carry both Flow 1 and 3. Hence, the PDR for both flows is lower than Flow 2. Since we use TCP traffic, we can expect fair sharing of the bandwidth usage and PDR.

Figure 7b shows PDR for lossless scenario when Flow 1 has 2.0 Mb/s load. This change does not affect Flow 2 that uses the high-speed link, but it causes significant degradation of PDR for both flows 1 and 3. However, Flow 1 is more impacted due to the higher bit rate, and consequently more packets are lost.

Figure 8 shows PDR for Flow 2 in both lossless and lossy scenarios. As it is observed, PDR decreases for Flow 2 in the lossy scenario, but it keeps using the same path throughout the simulation. Hence, it does not affect the other link even when there are bit errors.

Figure 9 illustrates PDR for the intermittent scenario in which the high-speed link drops for 2 seconds in each 20 seconds. Figure 9a shows the PDR result when Flow 1 has 1.8 Mb/s load while Figure 9b illustrates the same result with 2.0 Mb/s saturating load for Flow 1. In both cases, the traffic is rerouted to the low-speed link during the disconnection, and returns to its original path as soon as the link is reconnected. However, this event affects the PDR of both Flow 1 and 3 significantly. Moreover, this event has more impact on the PDR of Flow 3. On the other hand, in the saturating case (Figure 9b), we observe the same trend when there are no errors on links. However, some small fluctuations are observed on Flow 1, particularly at the time of disconnection.

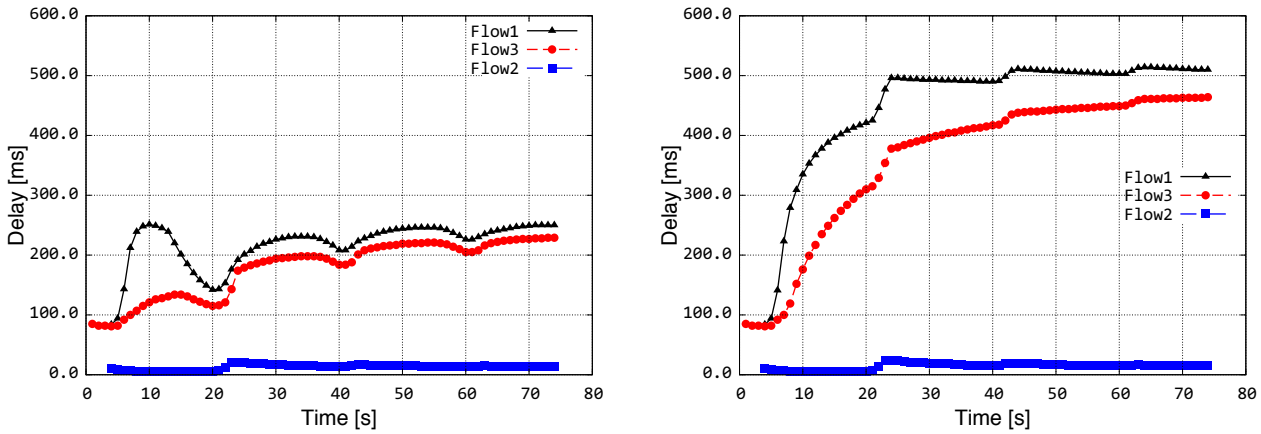
Figures 10a and 10b illustrate the delay results for the intermittent scenario for both cases 1.8 Mb/s and 2.0 Mb/s loads for Flow 1, respectively. While packet delivery is affected on both cases of the this scenario, delay also increases significantly. This is due to the fact that Flow 1 that has higher bit-rate suffers more packet drops than Flow 3, causing lower PDR and higher delay in the results. It



(a) 1.8 Mb/s load

(b) 2.0 Mb/s saturating load

Figure 9: Intermittent scenario PDR



(a) 1.8 Mb/s load

(b) 2.0 Mb/s saturating load

Figure 10: Intermittent scenario delay

is observed that the delay for Flow 3 that carries the low bit-rate traffic increases less than Flow 1. The lower delay for Flow 3 can be an advantage for the low-rate small-payload flows in IoT networks that may report sensor reading when these values are critical.

6 CONCLUSIONS AND FUTURE WORK

In this paper, we review the current IoT models, and propose a new model representing the *multilevel network structure* necessary for the provision and analysis of network resilience. We discuss how the ResiliNets D^2R^2 defend, detect, remediate, and recover strategy is applicable. This is work-in progress research, and more experiments are necessary to confirm the results that can lead us to design resilient networks for the IoT in which large fat non-critical flows consume the significant bandwidth. Furthermore, we plan rigorous challenge and failure analysis, along with insight on how to increase resilience to attacks and large-scale disasters. We are particularly interested in applying this to smart city scenarios.

REFERENCES

[1] Cisco. 2014. The Internet of Things Reference Model. White paper. (2014). http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf

[2] Cisco. 2015. Cisco Fog Computing: Unleash the Power of the Internet of Things. White paper. (2015). http://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf

[3] Dave Evans. 2011. The Internet of Things – How the Next Evolution of the Internet Is Changing Everything. White paper. (2011). https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[4] Dan Goodin. 2015. New Exploit Turns Samsung Galaxy Phones into Remote Bugging Devices. http://arstechnica.com/security/2015/06/new-exploit-turns-samsung-galaxy-phones-into-remote-bugging-devices/. (June 2015).

[5] Chris Greer. 2014. The Internet's Next Big Idea: Connecting People, Information, and Things. (2014). http://www.nist.gov/el/20140611_internets_next_big_idea.cfm

[6] Bluetooth Special Interest Group. 2015. Bluetooth. http://www.bluetooth.com/what-is-bluetooth-technology/bluetooth. (2015).

[7] Grant Hernandez, Orlando Arias, Daniel Buentello, and Yier Jin. 2014. Smart Nest Thermostat: A Smart Spy in Your Home. *Black Hat USA* (2014).

[8] J. Hui and P. Thubert. 2011. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. RFC 6282. (Sept. 2011). https://tools.ietf.org/html/rfc6282

[9] IEEE. 2011. IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR- WPANs). *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)* (Sept 2011), 1–314. https://doi.org/10.1109/IEEESTD.2011.6012487

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

[11] ITU. 2012. Overview of the Internet of Things. https://www.itu.int/rec/T-REC-Y.2060-201206-I. (June 2012).

[12] ITU. 2012. Terms and Definitions for the Internet of Things. https://www.itu.int/rec/T-REC-Y.2069-201207-I/en. (July 2012).

[13] David Lake, Ammar Rayes, and Monique Morrow. 2012. The Internet of Things. *The Internet Protocol Journal* (2012).

[14] Alliance LoRa. 2016. LoRa Alliance. https://www.lora-alliance.org/What-Is-LoRa/Technology. (2016).

[15] Alliance LoRa. 2016. LoRaWAN Specification. https://www.lora-alliance.org/For-Developers/LoRaWANDevelopers. (2016).

[16] Ludovic Le Moan. 2017. Sigfox Website. https://www.sigfox.com/en. (2017). https://www.sigfox.com/en

[17] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. 2007. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944. (Sept. 2007). https://tools.ietf.org/html/rfc4944

[18] ns-3. 2016. ns-3 website. https://www.nsnam.org/. (2016). https://www.nsnam.org/

[19] Barack Obama. 2015. Presidential Proclamation – Critical Infrastructure Security and Resilience Month, 2015. https://www.whitehouse.gov/the-press-office/2015/10/29/presidential-proclamation-critical-infrastructure-security-and/. (Oct. 2015).

[20] Mark Roberti. 2005. The History of RFID Technology. *RFID Journal* (2005).

[21] Monica Rozenfeld. 2014. Special Report: The Internet of Things. *The Institute, IEEE* (March 2014). http://theinstitute.ieee.org/technology-topics/internet-of-things/setting-the-stage-for-the-internet-of-things

[22] Z. Shelby, S. Chakrabarti, and E. Nordmark andC. Bormann. 2012. Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). RFC 6775. (Nov. 2012). https://tools.ietf.org/html/rfc6775

[23] James P.G. Sterbenz and David Hutchison. 2006. ResiliNets: Multilevel Resilient and Survivable Networking Initiative. http://wiki.ittc.ku.edu/resilinets. (2006). http://wiki.ittc.ku.edu/resilinets

[24] James P. G. Sterbenz, Egemen K. Çetinkaya, Mahmood A. Hameed, Abdul Jabbar, Qian Shi, and Justin P. Rohrer. 2011. Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation (invited paper). *Springer Telecommunication Systems* 52, 2 (February 2011), 705–736. published online 2011.

[25] James P. G. Sterbenz, David Hutchison, Egemen K. Çetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Schöller, and Paul Smith. 2014. Redundancy, Diversity, and Connectivity to Achieve Multilevel Network Resilience, Survivability, and Disruption Tolerance (invited paper). *Telecommunication Systems* 56, 1 (2014), 17–31.

[26] James P. G. Sterbenz, David Hutchison, Egemen K Çetinkaya, Abdul Jabbar, Justin P Rohrer, Marcus Schöller, and Paul Smith. 2010. Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines. *Computer Networks* 54, 8 (2010), 1245–1265.

[27] J. P. G. Sterbenz and P. Kulkarni. 2013. Diverse Infrastructure and Architecture for Datacenter and Cloud Resilience. In *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*. 1–7. https://doi.org/10.1109/ICCCN.2013.6614125

[28] Alex Wright. 2011. Hacking Cars. *Commun. ACM* 54, 11 (Nov. 2011), 18–19. https://doi.org/10.1145/2018396.2018403