Reliability in Internet of Things: Current Status and Future Perspectives

Liudong Xing, *Senior Member, IEEE*

***Abstract*—The Internet of Things (IoT) aims to transform the human society toward becoming intelligent, convenient, and efficient with potentially enormous economic and environmental benefits. Reliability is one of the main challenges that must be addressed to enable this revolutionized transformation. Based on the layered IoT architecture, this article first identifies reliability challenges posed by specific enabling technologies of each layer. This article then presents a systematic synthesis and review of IoT reliability-related literature. Reliability models and solutions at four layers (perception, communication, support, and application) are reflected and classified. Despite the rich body of works performed, the IoT reliability research is still in its early stage. Challenging research problems and opportunities are then discussed in relation to current underexplored behaviors and future new aspects of evolving IoT system complexity and dynamics.**

***Index Terms*—Application reliability, cloud computing, communication reliability, Internet of Things (IoT), perception reliability, support reliability, wireless sensor network (WSN).**

Acronyms

AC	Application communication.
ACK	Acknowledgment.
ACR	Application communication reliability.
AL	Application layer.
ARQ	Automatic repeat query.
BDD	Binary decision diagram.
BPSN	Battery-powered sensor node.
BSN	Body sensor network.
CL	Communication layer.
CRA	Co-resident attack.
CTMC	Continuous-time Markov chain.
DFT	Dynamic fault tree.
ECC	Error control code.
EHSN	Energy harvesting sensor node.
ESS	Energy storage system.
FC	Fiber channel.
FDEP	Functional dependency.
GR	Greatest reliability.
ICE	Intelligent, convenient, and efficient.
IC	Infrastructure communication.
ICR	Infrastructure communication reliability.
IoT	Internet of Things.
LCPC	Low-complexity parity check.
LDPC	Low-density parity check.
MDD	Multivalued decision diagram.
MH-GR	Minimum-hop greatest reliability.
MH-RT	Minimum-hop reliability threshold.
MICM	Modular imperfect coverage model.
MVMP	Multiversion multipath.
PBE	Probability of bit error.
PDR	Packet delivery ratio.
PHEV	Plug-in hybrid electric vehicles.
PL	Perception layer.
QoS	Quality of Service.
RBD	Reliability block diagram.
RS	Reed–Solomon.
SAN	Storage area network.
SINR	Signal-to-interference and noise ratio.
SL	Support layer.
UAV	Unmanned aerial vehicle.
VM	Virtual machine.
WSN	Wireless sensor network.

Manuscript received March 5, 2020; revised April 23, 2020; accepted May 5, 2020. Date of publication May 7, 2020; date of current version August 12, 2020. This work was supported in part by the U.S. National Science Foundation under Grant 1112947.

The author is with the Department of Electrical and Computer Engineering, University of Massachusetts Dartmouth, Dartmouth, MA 02747 USA (e-mail: lxing@umassd.edu).

Digital Object Identifier 10.1109/JIOT.2020.2993216

I. Introduction

As a key driver of the social evolution, the Internet has transformed the way people communicate with each other. The IoT aims to take this stride further to seamlessly connect people and various things, transforming the society toward becoming ICE with potentially enormous economic and environmental benefits. In the past decade, the IoT has developed rapidly, spanning diverse application domains from healthcare to home automation, environmental monitoring to smart energy, intelligent transportation to smart buildings, smart manufacture to smart agriculture, and smart military to smart ocean [1], [2].

Due to the safety-critical or mission-critical nature of the IoT applications, it is imperative that the IoT systems operate reliably throughout the intended mission time. In other words, reliability is one of the crucial requirements for adoption of the IoT in critical applications [3]–[10]. Malfunctions of supporting IoT devices (e.g., wearable medical devices), failing to capture critical data, any network outage, data corruption, or loss during transmission or storage may cause catastrophic effects, such as mission failure, financial loss, and harm to people and environments. From the viewpoint of researchers, developers, and even consumers, reliability analysis and design are, therefore, an indispensable step before

IoT systems can be widely deployed for safety-critical and mission-critical applications.

This article presents a state-of-the-art survey on the IoT reliability modeling, analysis, and design methods and solutions. Reliability models aim to represent the system failure criteria in a systematic and logical manner, which help to understand all possible ways in which a system can fail (e.g., dynamic fault trees [11]) or function (e.g., reliability block diagrams [12]). Reliability analysis aims to quantify the probability that a system performs its intended function correctly throughout its mission time, or its complement value, that is, the probability of the system failure during the mission time (i.e., system unreliability). Representative reliability analysis methods include simulations, and analytical modeling methods that further include combinatorial models (e.g., binary decision diagrams [13], [14]) and state-space-based models (e.g., Markov processes [15]). Reliability design is concerned with choosing proper components, redundancies, and system configurations to ensure that a system can meet its reliability requirements under its operating environment for a certain time period. While using redundancies can make a system tolerate hardware faults or software errors, it does not necessarily guarantee a highly reliable system [16]. Likewise, a highly reliable system does not necessarily use redundancies or possess the attribute of fault tolerance. Thus, it is critical to perform reliability modeling and analysis during the reliability design process to make sure that the system design meets desired reliability and fault-tolerance requirements.

Note that many review articles on IoT have recently been published. Some provide comprehensive discussions on different aspects of the IoT research developments and directions [1], [17], [18]. Such general reviews are also available for IoT of particular types or countries, e.g., social IoT [19], military IoT [20], underwater IoT [21], and IoT in China [22] or India [23]. There also exist surveys focusing on a specific aspect of the IoT design and development, including but not limited to:

1) IoT security and privacy [24]–[29], and related, such as cryptographic algorithms [30], digital forensics [31]–[34], access control mechanisms [35], and trust management techniques [36]–[39];
2) IoT enabling technologies in general [40], [41], or focusing on one particular technology, such as fog computing [42]–[45], edge computing [46], [47], cloud computing [48], [49], blockchains [50]–[54], WSNs [55], [56], BSNs [57], machine learning [58], [59], data fusion [60], [61], 5G wireless technology [62], and Bluetooth low-energy beacons [63];
3) IoT applications in general [64], or focusing on a particular application domain, such as agriculture [65], smart grid/energy [66]–[68], industries [69], [70], smart manufacture [71], supply chains managements [72], education [73], food safety [74], healthcare [75], smart home [76], smart buildings [77], UAV [78], disaster management [79], and geohazards prevention (e.g., earthquakes and landslides) [80];
4) IoT experimental environment, testbed, or facilities [81], [82];
5) IoT fault tolerance, fault detection, and anomaly detection [83]–[85].

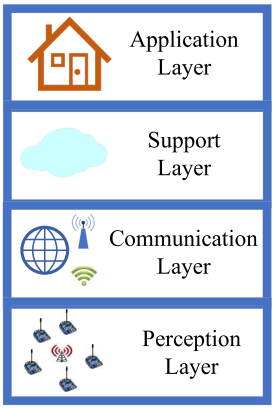

Fig. 1. Four-layer architecture of IoT.

To the best of our knowledge, there exist no surveys providing a systematic and state-of-the-art coverage on the reliability aspect of IoT. In this article, some major challenges in the reliability modeling, analysis, and design of IoT systems are first identified in the context of a four-layered IoT architecture. A systematic review of the existing solution methods for reliability modeling, analysis, and design is then conducted in categories, including IoT perception technologies reliability, IoT communication and transport reliability, IoT support technologies reliability, and IoT applications and services reliability. Directions of future developments in the IoT reliability are discussed at the end.

II. IoT Architecture and Reliability Challenges

There are different layered models of IoT systems [24], [86]. To facilitate discussions of reliability challenges and solutions in this article, we consider a four-layered architecture [87]. As demonstrated in Fig. 1, the four generic layers include the PL or sensing layer (e.g., sensors and sensor networks), the CL or transport layer (e.g., wired and wireless networks), the SL (e.g., cloud computing and SANs), and the AL or service layer (e.g., smart home and smart healthcare). Each of these layers has its specific technologies that pose reliability issues and challenges.

The PL typically contains multiple sensor nodes deployed to perform different measurements (e.g., temperature, humidity, ECG, and EMG). The sensor nodes, and in general, IoT devices are heterogeneous with diverse sensing, processing, communication and coverage profiles, thus different failure or reliability behaviors. In addition, sensor nodes are deployed in large numbers for some IoT applications [88], posing challenges to the traditional network reliability analysis methods (applicable to networks of small or moderate size).

Due to limited resources (power, computation, storage, and communication capacity), IoT devices especially those operating in harsh and unattended environments are prone to failures. They often communicate through wireless links that are also error prone due to noises, signal attenuations, or channel fading. Thus, the topology of the IoT communication and

networking is very dynamic due to malfunctions of the IoT devices and communication links.

Advances in various IoT enabling technologies are making the IoT systems more powerful and intelligent. On the other hand, the cooperation and interaction among the system components become more complicated, creating new and unknown dependencies. For example, different components at the SL may behave dependently. Specifically, the servers and storage arrays in an IoT SAN are typically located in remote sites and can be accessible through FC switches; in other words, they have FDEP on the switches [89]. In the case of switches failing, the servers and storage arrays connected to them become inaccessible or isolated. In this FDEP relationship, the switch is referred to as the *trigger* component, the servers and storage arrays are referred to as the *dependent components*. Similarly, in a cloud-RAID (redundant array of independent/inexpensive disks) storage system, the disk arrays have FDEP on the RAID controller [90]. Such an FDEP behavior also exists in the AL. For example, solar panels in a smart home have FDEP on the ESS; in the case of ESS malfunctioning, the energy produced from the solar panels becomes unusable [91].

The FDEP in the above examples takes place deterministically. It may also happen in a probabilistic manner in the IoT system [11]. For example, a sensor often transmits its sensed data to the sink node or base station via a relay node, that is, the sensor (dependent component) has FDEP on the relay (trigger) [92], [93]. However, in the case of the relay node malfunctioning, the sensor may improve its transmitting power to enable a direct communication to the base station with a certain probability that relies on the sensor's remaining battery power. In this case, when the relay fails, it is not necessarily that the sensor becomes isolated.

In both deterministic and probabilistic FDEP systems, competitions may exist between different failure modes of the trigger and dependent components, specifically between local failures of the trigger component and propagated failures of the dependent components. While a local failure only causes the outage of the affected component itself, a propagated failure may cause extensive damages and even crash the entire system [94]. In the FDEP system, a propagated failure originating from a dependent component may have dynamic impacts, dependent on its occurrence time. If it happens before the local failure of the corresponding trigger component, the failure propagation effect takes place crashing the system. However, if the trigger's local failure happens earlier, all the dependent components are isolated preventing their propagated failures from affecting the rest of the system (deterministically or probabilistically). Such sequence-dependent and dynamic competing processes pose unique challenges to the IoT reliability analysis.

For critical IoT devices, standby spares are typically utilized to achieve fault tolerance and high availability [91]. Depending on the recovery time requirement and resource constraint, three different standby modes are available: cold, hot, and warm [95], [96]. A cold standby component remains unpowered and thus often has a zero-failure rate before its use; it however requires long recovery time to restore the system function in the case of the primary online component failing. A hot standby component operates concurrently with the primary online unit enabling immediate recovery; it however consumes the same resource and has the same failure rate as the primary unit. A warm standby component is partially powered with a certain reduced failure rate before being activated to replace the failed primary component. The traditional reliability models assuming static component failure rates and mechanisms are not applicable to the standby components undergoing dynamic/changing failure rates before and after their activation.

The IoT system is also subject to the phased-mission behavior. During different phases, the system may need to perform different tasks or functions involving different subsets of system resources or components. These components may undergo different environment conditions and stress levels, thus have different failure rates or mechanisms during different phases [97]. For example, in a smart home, its power generation system uses solar energy and standard electricity [91]. Due to the changing brightness of the sun, the solar panels function with different production performance with time. During some time (e.g., afternoon), energy from the solar panels is sufficient to supply the electrical panel of the smart home (even with extra electricity being stored or sold to the public grid); during other time (e.g., evening), the solar panels can stop functioning and electricity stored and/or from the public grid has to be used to supply the smart home. For another example, a person wears a body sensor system to have his or her physiological and motion information monitored [98]. The daily cycle of this person consists of two phases: 1) inactive night sleep and 2) active daytime activities. During the night phase, only the physiological information (e.g., blood pressure and heart rates) is measured by biosensors; during the daytime phase, both the physiological and motion data are monitored by biosensors and motion sensors, respectively. In both examples during different phases, different subsets of system components (e.g., sensors) contribute to the system function, requiring a distinct reliability model to describe the system failure behavior at each phase.

In addition, the IoT devices and systems often perform at different levels, ranging from the perfect function to complete failure with multiple different degradation states in between [14], [99]. During the operation, fatal or nonfatal shocks may randomly happen to the IoT system and devices, causing immediate failure or acceleration of the degradation processes [100]. Both the multistate and the dependent degradation-shock processes render the challenges in the IoT reliability modeling and analysis activities.

The above-mentioned behaviors and features (representative rather than complete) all contribute to the difficulty in modeling and evaluating the IoT reliability. In the following sections, the existing reliability solutions to the IoT system are reviewed and analyzed, followed by discussions on open challenges, and new opportunities and directions for the IoT reliability research.

III. IoT Perception Technologies Reliability

At the bottom layer of the IoT, smart, low power, and microsensor devices are typically deployed to measure the physical conditions of the object or environment being monitored. These sensor devices are typically networked through wireless medium, forming a WSN.

In the past decade or so, considerable research efforts have been expended in modeling and designing the reliability of WSN systems at different levels, including component level, end-to-end path level, and system level [55]. Some representative works at each level are described in the following sections, followed by a summary of the WSN reliability analysis approaches in Section III-D.

A. Component-Level Reliability

At the component level, the reliability of a sensor node is modeled and analyzed. A typical sensor node contains four major components: 1) a sensing component for data acquisition; 2) a processing component for local data processing; 3) a radio or communication component for data communication; and 4) a power supply component [101]. Additional components like the location finding component and actuator (for sensor adjustment and movement) may also be available in some application-specific sensor nodes. Depending on the power supply sources, two types of sensor nodes are differentiated: 1) BPSN and 2) EHSN that can convert ambient energy to electrical energy [102].

In [103], the reliability of a BPSN was modeled as the reliability of its battery component considering that the battery lifetime essentially decides the lifetime of the BPSN in many practical scenarios where it is impossible to recharge or replace the sensor battery during the course of the mission [104]. The BPSN reliability analysis was performed under three different working scenarios differentiated by sensor node modes (sleep or active) and alternating mechanisms between these modes in [103]. In [105], both BPSN and EPSN were modeled as multicomponent systems and their reliabilities were evaluated by considering the reliability of the energy flow and reliability of each constituent component of the sensor node. In [106], the BPSN reliability was evaluated by considering failures and dependencies of its four major constituent components.

Due to the constrained resources and often operating in harsh and unattended environments, sensor nodes are prone to failures, and thus their reliability (fault tolerance) designs are critical. To make WSN resilient to sensor node failures, in [107], several reliability designs using hot and cold standby sparing techniques were investigated and compared under a homogeneous or heterogeneous substituting scheme (a failed sensor can be replaced by a spare sensor of the same type or a different type). It was revealed that the cold standby technique is more reliable than the hot one; when sensors are configured in a series structure, the heterogeneous substitution scheme always provides higher reliability than the homogeneous one regardless of cold or hot standby being utilized; however, when sensors are configured in a parallel structure, under the hot standby, the two substitution schemes have the same reliability performance while under the cold standby, the homogeneous scheme provides higher reliability than the heterogeneous one.

Considering the crucial role of the sink node (base station) in WSNs and the need for fast recovery in the case of the failure of the primary sink node, the hot standby sparing design was considered in [108] to achieve a highly reliable sink node subsystem. In the same work [108], due to limited power resource, a cold standby sparing design was adopted for each cluster head in a hierarchical clustered WSN system. A CTMC method was applied to evaluate the reliability of the hot standby sink subsystem and the reliability of the cold standby cluster head subsystem, considering the failure of the switching mechanism involved in the standby designs. In [109], replicated sink nodes were used and deployed in different locations of a WSN to achieve the resilience to sink node failures.

As another component-level reliability research, the failure behavior of a wireless link connecting sensor nodes has been modeled and the link reliability has been analyzed. A wireless link is considered reliable if its radio attribute meets the minimum requirement for a successful communication between the two terminal nodes of the link. In [110], the reliability of a wireless link was analyzed through a time-dependent lognormal shadowing radio propagation model, which incorporates the consideration of battery discharge, power consumption under different sensor node modes (active and sleep), and conditions of the wireless channel for estimating link reliability. In the general literature of wireless networks, link reliability has also been studied. For example, in [111], a generic framework using internode interference, SINR, and PBE was suggested for reliability analysis of a wireless link between two nodes. In [112], the link reliability was estimated based on an intraframe SINR distribution using measurements on an empirical testbed.

The component-level reliability models aim to produce a realistic estimation of reliability or its related attributes of sensor nodes and links. These parameters' estimations are crucial to the reliability analysis at the end-to-end path level and the system level of WSNs.

B. End-to-End Path-Level Reliability

At the path level, the connectivity-based reliability of an end-to-end path (selected using a certain routing algorithm) is often modeled and analyzed [113]. For instance, in [105], the reliability of a communication path from a specific sensor node in an area being monitored by a WSN to the sink node was analyzed based on the reliability estimation of sensor nodes and links appearing on the path. One important application of the path-level reliability evaluation is to verify and compare the reliability performance of different routing protocols. For example, in [105], the end-to-end path reliability is one of the performance metrics used in the comparative study of the minimum-hop routing algorithm, the shortest path routing algorithm, and the GR routing algorithm for a hybrid WSN composed of both BPSNs and EHSNs.

The reliability design at the path level is often achieved through multipath routing protocols [114] or considering the link reliability or path reliability in the design of routing algorithms. Refer to Section IV for more details on the design of reliability-oriented routing algorithms.

C. System-Level Reliability

At the system level, the WSN reliability has been defined and modeled based on the function performed. Consider a WSN used in healthcare as an example. The caregiver or doctor sends a data transfer request through the sink node to biosensors (e.g, SpO2 and ECG) worn by a patient; these biosensors then transmit the sensed information to the sink node. The former phase is referred to as the IC; and the latter phase is referred to as the AC [115].

The IC is in general concerned with delivering maintenance, data acquisition request and configuration information from the sink node to sensor nodes in the targeted area being monitored by the WSN. The ICR has been modeled for different data delivery models, including sink unicast, sink anycast, sink multicast, sink manycast, and sink broadcast [116]–[118]. Under these models, the sink transmits data/messages to one particular sensor, any one out of a group of qualified sensors, all sensors within a specified group, any subset (with a certain size) out of a group of qualified nodes, and all sensors in the WSN, respectively.

The AC is, in general, concerned with acquiring information and transmitting the sensed information from sensor nodes involved to the sink node. While the information acquisition depends on the sensing coverage, the information delivery depends on the communication path connectivity. Thus, the ACR encompasses both coverage reliability and terminal network reliability; refer to [119]–[122] for the analysis of ACR in WSNs with different topologies (star, tree, mesh, and hierarchical clustering).

A complete function of WSNs typically involves both IC and AC as a two-phase communication task or even a multiphase task with more than one IC and/or AC phases. Correspondingly, a phased-mission reliability modeling methodology has been suggested in [123] to evaluate the WSN reliability involving both ICR and ACR while considering cross-phase dependencies of WSN components.

In addition to the above-mentioned reliability research focusing on the system-level basic functions, some complicated behaviors that introduce interactions and dependencies among the system components have been addressed in the WSN reliability analysis. For example, WSNs may undergo common-cause failures (CCFs), where multiple sensors fail at the same time due to a shared cause, such as extreme conditions, design deficiency, and humidity. The effects of CCFs have been addressed in the modeling and analysis of ICR [118] and ACR [124] of WSN systems. The probabilistic FDEP and associated competitions between the trigger and the dependent components (described in Section II) have also been addressed in the reliability analysis of a body area WSN system [92] and a multistate critical room monitoring WSN [99].

D. WSN Reliability Analysis Approaches

While in the most recent research, WSNs have been coupled with machine learning to estimate the reliability of data communication in the form of PDR [9], [127], simulations and analytical modeling are still major approaches for the WSN reliability analysis. Based on random samples of failures and responses of WSN components, simulations (e.g., NS-2 simulation [126], Monte Carlo simulation [127], AVRORA behavioral simulator [128], and OPNET [129]) provide approximate estimation of the WSN reliability. Both state space and combinatorial models belong to the analytical modeling approaches.

Examples of the state-space methods include, for example, the state-enumeration approach [130], Petri nets [131], and Markov chains [132], [133]. These approaches are typically powerful in modeling complex WSN behaviors. However, they are subject to the state-space explosion problem, restricting them to the reliability analysis of only small-scale WSN systems.

Examples of combinatorial models include, for example, those based on cut/path sets [106], [134], K-coverage sets [135], graph transformation [130], RBD [136], BDD [116]–[118], and MDD [137]. In addition, based on BDD or MDD, combinatorial approaches using the "divide-and-conquer" principle were also developed to address complex system behaviors, such as CCFs and competitions in the FDEP relation [92], [99], [118], [124]. As compared to the state-space models, combinatorial approaches are computationally more efficient and thus applicable to the reliability analysis of larger scale WSNs.

IV. IoT Communication and Transport Reliability

The CL is responsible for providing a ubiquitous access and networking environment for the PL. Specifically, the CL aims to transmit the sensed/aggregated data from the PL to the base station through Internet and/or wireless networks.

Routing algorithms and protocols play a crucial role in the reliability of the CL/networking layer. The routing algorithm used in the protocol determines the path of transmitting information from the source node to the destination node. In the case of a failure of a node or a link on the selected path, a reliable routing protocol is responsible for detecting the occurrence of the failure and finding an alternative path to accomplish the desired information transmission. In the following sections, different methods for reliable routing or data transmission are reviewed, including multipath routing, reliability-aware single-path routing, retransmissions, and coding-based fault-tolerant data transmission.

A. Multipath Routing

For failure resilient WSNs, multipath routing protocols have been designed, which use multiple alternative paths between the source and the destination to achieve high reliability [114]. The multiple paths may be link disjoint, node disjoint, or overlapped/correlated. They may be used in parallel, or in a standby style (in the case of one path failing, another

available path is used). For example, in [138], a query-based multipath routing protocol was proposed, which attempts to establish node-disjoint paths minimizing negative impacts from interferences. In [139], an energy-efficient multipath routing protocol was suggested, which searches several node-disjoint paths and distributes the traffic over each path selected using a load balancing method. In [140], a channel-aware reinforcement learning-based multipath adaptive routing protocol was proposed for multihop underwater WSNs; guided by a distributed reinforcement learning framework the protocol switches between single-path routing and multipath routing with the aim to improve the WSN performance in terms of energy consumption and PDR.

Based on the multipath routing, some data transmission mechanisms have been suggested to achieve both data reliability and data security at the same time. For example, in [141], a fault-intrusion-tolerant mechanism named MVMP was proposed as a concept, which combines multipath, data fragmentation, forward error correction erasure coding, and multiversion of cryptographic algorithms in the same protocol for reliable and secure data transmissions in WSNs. In [142], the MVMP mechanism was developed through incorporating the specific RS code at the packet or bit level.

B. Reliability-Aware Single-Path Routing

In addition to multipath routing, there also exist works on designing reliability into the single-path routing algorithms. For example, in [143], a lightweight routing protocol was proposed, which implements an adaptive selection of the routing path based on the link reliability or quality. In [105], three routing algorithms considering the link reliability or path reliability were designed, including the GR routing algorithm, the MH-GR routing algorithm, and the MH-RT algorithm. The GR algorithm finds the most reliable path (i.e., the path with the greatest end-to-end path reliability) between the source and the destination. The MH-GR algorithm finds the path with the minimum number of hops; in the case of multiple paths with the same minimum-hop counts existing, the most reliable path among them is selected. The MH-RT algorithm finds the minimum-hop count path using only links with reliability greater than a predefined threshold value. The performance comparison revealed that the GR appears the most reliable at the beginning of the mission time and after a certain time, the MH-RT becomes the most reliable due to dynamics in the reliability of links and nodes appearing on the selected paths. A dynamic routing that integrates both GR and MH-RT was further proposed to take advantage of both routing algorithms through the algorithm switching at a calculated time. In [144], a weighted cost function-based routing algorithm that integrates energy consumption, end-to-end path reliability, and implementation cost was designed for hybrid WSNs with both BPSNs and EHSNs. In [145], a routing protocol based on routing by energy and link quality was proposed, which selects paths considering the end-to-end link quality, hop count, and residual energy.

C. Retransmission-Based Mechanisms

Based on the ARQ protocol, the retransmission-based mechanism uses ACK and timeout to provide reliable data transmissions. Specifically, if the transmitter fails to receive an ACK before the prespecified timeout, it retransmits the packet until the transmitter gets an ACK or the number of retransmissions exceeds a predetermined maximum value.

The ARQ has several instances or variants, such as Go-Back-N ARQ, selective repeat ARQ, stop-and-wait ARQ, etc. [146]–[149]. Both the Go-Back-N and selective repeat ARQs may transmit N packets specified by a window size to the destination before requiring an ACK packet. With the Go-Back-N, all the packets must be received in order while with the selective repeat, the receiver can accept out-of-order packets and a single packet may be selectively rejected by the receiver and retransmitted alone. The stop-and-wait is the simplest ARQ with $N = 1$. All these retransmission mechanisms may operate in the hop-by-hop mode or the end-to-end path mode [150].

While the retransmission mechanism is simple to implement, it may incur a long delivery delay and increase the energy consumption of the node, especially in networks with low link reliability or quality. Thus, retransmissions are not desirable for IoT applications that have strict time requirements or constrained energy resources.

D. Coding-Based Fault-Tolerant Transmission

Channel coding or error control coding (ECC) is a technique used for tolerating errors during data transmissions over noisy channels. Through including redundancy to the transmitted data, the ECC enables the receiver/decoder to detect and correct a certain number of errors and recover the original data without any retransmissions. Moreover, in the case of some data getting lost during the transmission, the receiver may also retrieve the original data packets [151]. ECC is highly desirable for applications where retransmissions are impossible or costly (e.g., resource-constrained WSNs). As compared to the retransmission mechanism, the coded transmission typically involves shorter delivery delays.

Different ECC techniques have been investigated for IoT. For example, the MVMP mechanism (mentioned in Section IV-A) utilizes the RS code to tolerate transmission errors at the bit level and the packet level [142]. In [152], a hybrid cipher that combines the RS code and random selective encryption to tolerate both errors and security attacks for robust transmissions in WSNs. In [153], design parameters of the RS code were investigated for optimal bit error performance over two types of channels (additive white Gaussian noise channel and Rayleigh fading channel). In [154], the LCPC code was proposed for detecting and correcting nonconsecutive or consecutive bit errors in data transmissions; a comparative study using simulations was conducted demonstrating that the LCPC code outperforms the RS code, the LDPC code, and the Hamming code in terms of computational complexity and memory requirement. In [155], the cyclic redundancy check code was investigated for detecting erroneous packets and correcting the errors using

an iterative decoding technique. In [156], an error correction scheme based on redundant residue arithmetic was suggested for achieving reliable and energy-efficient data transmission for smart cities. In [157], a turbo channel code was proposed for reliable packet transmissions in narrowband IoT. In [158], an improved LDPC code with memory among different data transmissions was proposed to reduce the packet loss ratio of the traditional LDPC code for industry IoT. In [159], a rateless code that can adjust the rate on the fly was suggested for ensuring the QoS requirements in industry IoT.

There are also studies that integrate the coding and retransmission for achieving reliable data transmission [160]. For example, in [150], a hybrid transmission protocol was proposed, which combines the send–wait ARQ protocol in hotspot areas and the redundancy-based coding technique in nonhotspot areas to meet the reliability requirement. In [161], channel coding, retransmission, and compression were integrated to meet the quality requirements of the transmitted sensing data.

V. IoT Support Technologies Reliability

The SL is mainly responsible for storing and processing mass data in the IoT [162]. The safety-critical or mission-critical nature of the IoT applications and the rapid growth of data generated require highly reliable and efficient data storage and processing solutions. Cloud computing is one of such solutions that has played a crucial role in the recent IoT developments [48], [49]. Under the cloud computing paradigm, the cloud-RAID and SAN serve as popular reliable solutions for big data storage. Both cloud-RAID and SAN are featured with the storage virtualization [163], a technique of abstracting physical storage (a network of storage devices) from applications as a single logical drive viewed and accessed by users. In the following sections, reliability research in the cloud support technologies is reviewed and analyzed. Reliability studies for edge computing and fog computing, and variants of the cloud computing, are also reviewed.

A. Cloud Fault-Tolerance Techniques

Powered by the virtualization technology, the cloud computing paradigm has enabled on-demand and cost-effective resource sharing in terms of services among many users. In particular, users' service requests are honored through creating and running VMs on available physical servers. Thus, both VM failures and physical server failures may interrupt the execution of a cloud service and affect the cloud service reliability.

To enhance the cloud service reliability, diverse fault-tolerant techniques have been suggested, which use redundant resources (hardware, software, and time) to achieve resilience to failures [164], [165]. Examples include but not limited to:

1) *Retrying:* a failed service task is retried on the same resource;
2) *Alternate Resource:* a failed service task is retried on another resource;
3) *Replication:* multiple replicas of the same service task are performed on different resources in parallel;
4) *N-Version Programming (NVP):* multiple functionally equivalent versions of the same service are performed on different resources in parallel; the final output is determined by a voting on outputs of the multiple versions;
5) *Checkpointing:* a failed service task resumes its execution from the last successfully saved checkpoint on the same or different resources.

Performances of the cloud services under those different fault-tolerance techniques have been evaluated and compared. For example, in [166], the response time distribution of a cloud service was analyzed with the consideration of the checkpointing technique. In [164], the distribution and percentile of service response time for cloud with the retrying technique were evaluated and a comparative study between retrying and checkpointing was performed. The works in [164] and [166] did not address the service reliability directly. In [167] and [168], correlations among cloud service reliability, performance, and energy consumption were investigated under no fault-tolerant mechanism, the retrying mechanism, and the checkpointing mechanism. In particular, the cloud service reliability was modeled by a Markov process in [167] and [168].

B. Cloud Data Reliability Under Cyberattacks

VMs created for different users' service requests may be hosted on the same physical server in the cloud. Such a VM co-resident architecture poses unique reliability and security risks to cloud services. In particular, the CRA may be launched by malicious attackers, where VMs running the malware are co-located with a target user's VMs and a side channel can then be established to enable the data theft or corruption [169], [170]. Intensive works have been performed on the CRA mitigation mechanisms with a focus on enhancing the cloud service security, including, for example, mechanisms based on side-channel removal, VM allocations or migrations, and the game theory [171]–[174]. A review of these existing CRA defense mechanisms can be found in [165].

In the last few years, CRA mitigation strategies based on data partition, replication, combined partition and replication, and NVP have been proposed and analyzed using probabilistic combinatorial models while addressing data reliability or both data reliability and security. In particular, in [175], the data partition technique was investigated, which divides a user's data into several independent blocks and stores them in different locations/VMs. With the assumption that the data are useful only in its integrity, the data security can be improved since an attacker needs to access all the separate data blocks to use the information. However, the data reliability is reduced as if any data block is compromised or corrupted, the entire data become useless to its valid user. The number of data blocks used in the partition policy plays a crucial role; more data blocks make data corruption easier, but data theft harder. In [175], a probabilistic modeling method was suggested to evaluate both data reliability and security

and the optimal data partition policy was determined through formulating and solving constrained optimization problems, achieving a balance between data reliability and security.

In [176], the replication technique was investigated, which replicates a user's data multiple times and stores these replicas at different VMs. The number of data replicas created affects the data reliability and security in a different manner; more data replicas make data corruption harder, but data theft easier. The optimal data replication policy was investigated to balance the data reliability and security while minimizing the user's overhead of using the cloud service.

In [177], the data partition and replication were combined to mitigate the impacts of CRAs. In the combined technique, a user's data are divided into multiple independent blocks first. Each block is then replicated multiple (maybe different) times and each replica is stored on a different VM. An attacker may corrupt the information only when all replicas of the same data block are corrupted, and may steal the information when at least one replica of each block is stolen. Thus, more blocks make data corruption easier but data theft more difficult; more replicas per block make data theft easier but data corruption more difficult. The optimal data partition–replication policy was investigated in [177] to achieve a tradeoff among data reliability, data security, and user's overhead.

In [165], the NVP technique was utilized to defend CRAs in the cloud computing system, which runs multiple versions of the same service program (usually developed independently by different teams) by different VMs hosted on different physical servers. Upon completion of all the service versions a plurality voting is performed, which picks the alternative with the most votes as the final service output. The data reliability and the user's overhead associated with the data corruption and using the cloud service were analyzed. The optimal number of service versions was investigated to minimize the user's overhead. In [178], a stricter plurality voting mechanism considering a certain voting threshold and user's required service response time was modeled. The optimal policy studied includes the determination of the number of service versions and the threshold used for the voting.

C. Cloud-RAID Reliability

While the VM-based cloud computing paradigm lends itself to fault-tolerant storage based on techniques, such as replication, partition, and NVP, the ECC can also be applied to ensure the data reliability through, for example, the cloud-RAID architecture. The traditional RAID architecture has seven levels with level 0 implementing the data stripping technique and no redundancy, level 1 implementing the mirroring redundancy (duplicated data stripes), and levels 2–6 implementing different parity ECC techniques (e.g., level 2 uses the Hamming code, and level 5 uses the block-level distributed parity code) [179]. These different RAID levels have been investigated for the cloud computing platform in the past decade, and reliabilities of different cloud-RAID technologies have also been studied [180], [181]. The challenge in reliability analysis of cloud-RAID as compared to the traditional RAID lies in the heterogeneous disks (with different failure and recovery behaviors) that form the storage array.

In [182] and [183], reliabilities of cloud-RAID 5 and 6 were, respectively, investigated using a hierarchical method encompassing a CTMC at a lower disk level and a combinatorial MDD at a higher system level. In [184], the MDD model was extended to consider the imperfect coverage behavior in the reliability analysis of a cloud-RAID 6 system. The imperfect coverage is an inherent behavior of any fault-tolerant system with an automatic fault recovery mechanism, which is often imperfect and can cause extensive damage to the entire system when failing. Two different imperfect coverage models (element level and fault level) were addressed in [184]. In [90] and [185], the FDEP between the RAID controller and disks was addressed in the reliability analysis of cloud-RAID subject to the fault-level and element-level imperfect coverage, respectively. In [186] and [187], the cloud disk selection problem was formulated and solved to balance reliability and cost for cloud-RAID with the fault-level and element-level imperfect coverage, respectively.

In addition to the different types of parity codes used in the cloud-RAID, other types of codes have also recently been investigated to enhance the cloud storage reliability, for example, the RS-based code [188].

D. SAN Reliability

An SAN is a high-speed FC fabric capable of connecting any server and any storage element, allowing multiple storage resources to be accessed by multiple hosts simultaneously [189]. Despite its common use in practice, the literature on the SAN reliability research is still limited. The following presents several representative works.

In [190], the performance in terms of the throughput was modeled considering the effects of different unreliable packet delivery conditions over a long distance (hundred to thousands of kilometers) in SANs.

In [191], the SAN reliability was modeled as the reliability of an end-to-end network path with building blocks, such as access devices (FC switches), a core optical network, and fiber/cable links. Based on the assumption of independent component/block failures, the end-to-end path reliability was measured through adding predicted downtime (or service failure rate) of each building block appearing on the path.

In recent work [89], reliability modeling of a mesh SAN system has been addressed with the consideration of perfect links and imperfect links. Particularly, the failure behavior of the mesh SAN system under perfect links was modeled using a DFT, where the FDEP between switches and storage arrays (or servers) was explicitly modeled. Under imperfect links, a probabilistic network graph was used to model the SAN's reliability behavior. Based on the DFT or the network graph, the BDD-based combinatorial method [192], [193] was then applied to determine the reliability of the entire mesh SAN system. Impacts of link failures were investigated; numerical studies revealed that practical link failure probabilities (10^{-6}–10^{-4}) [194] have an insignificant influence on the

SAN reliability due to multiple communication paths existing between servers and storage arrays.

E. Edge and Fog Computing Reliability

As variants and extensions of the conventional cloud computing, edge computing and fog computing are gaining popularity for IoT applications due to their advantages in improving the response time (latency) and saving bandwidth [195]. Unlike the cloud computing that processes big data at centralized data centers, the data processing in edge computing is performed by IoT devices at the edge of the network where data were initially generated, while the data in fog computing are processed by fog nodes or IoT gateways situated at the local area network level of the system. Both fog and edge computing are not devised as competitors of the cloud computing, but as allies for a broad range of applications and use cases for which the conventional cloud computing is not sufficient [196].

Unlike the intensive works performed for the cloud computing reliability, reliability models and reliability-aware mechanisms for both edge computing and fog computing systems are still limited. Some representative works are discussed as follows.

For example, in [197], a simplified reliability model was used to compute the task reliability in edge computing, which considers only transient faults using Poisson processes; the minimum reliability of all tasks defines the total system reliability. An optimization model balancing system reliability, task execution time, energy consumption, and quality of experience was further suggested and solved for the edge computing system.

In [198], a reliability-based target tracking mechanism was proposed, which evaluates the reliability of a matching response region through a reliability network model and uses the reliability metric calculated for optimizing the track performance.

In [199], a Markov chain-based method was used to estimate the edge computing service reliability, which was then used as a performance metric to evaluate a decentralized authentication mechanism proposed in this article.

In [200], a network-wide power minimization problem was solved for task computation and offloading in the mobile-edge computing system considering constraints on delay, and unreliability (interpreted as the delay bound violation probability).

In [201], a task offloading failure probability considering both computation and communication reliabilities was modeled and minimized subject to certain latency constraints for mobile-edge computing. In particular, the computation reliability was estimated by assuming that both hardware and software failures follow Poisson processes.

In [202], a deviceless pipelining edge computing approach was proposed to provide reliability in spite of churn causing device failures, where computational resources are abstracted into functions and information associated with a failed function can be recovered from backup devices (cold or warm standby) without data loss.

In [203], the resource reliability was evaluated as an average of reliabilities of all paths connecting the resource requester and resource provider without considering dependencies among paths. The reliability values calculated were then fed into an edge computing scheduling algorithm to generate reliability-aware workflow schedules.

There also exist reliability-related studies for fog computing. For example, in [204], a software architecture to enable reliability and adaptability in Android for fog computing was proposed. In [205], the reliability of using fog computing for smart mobile applications was evaluated using two use cases from the public transportation (city traffic anomaly detection and bus stop arrival time estimation).

In [206], an architecture of fog computing-aided swarm of drones was proposed and a task allocation optimization problem was formulated and solved balancing reliability, latency, and energy consumption. The reliability model of [206] assumes exponential time-to-failure for drones and communication links.

In [207], a tradeoff analysis between cost and reliability was performed for fog resource provisioning in IoT. The reliability model of [207] assumes exponential time-to-failure for VMs running computation tasks and evaluates the IoT system unreliability as the ratio of the number of unsatisfied tasks (violating the QoS requirement) and the total number of tasks during a given time.

In [208], a power allocation problem was studied to achieve reliability-guaranteed communication in fog computing, where the transmission reliability was evaluated as the probability that a successful transmission probability exceeds a predefined threshold.

In [209], fault-tolerant techniques were discussed for assuring the reliability of fog services, including, for example, watchdog (monitoring a fog node by another fog node for fault detection) and replication (replicating a stateful fog service on another fog node).

VI. IoT Applications and Services Reliability

The IoT AL provides customized smart services according to users' needs. For example, it may provide air humidity and temperature measurements to users requesting such data. Diverse cases can be implemented at this layer, including, for example, smart homes, smart health care using BSNs, smart grids, smart parking, etc. This section discusses some example works on the reliability of the IoT application services.

A. Smart Home Reliability

Reliability has been recognized as one of the key requirements and challenges for the smart home application [76], [210], and [211]. In [212], a smart home was modeled as a cyber–physical system and a hierarchical and combinatorial reliability analysis method was proposed, which encompasses an MDD-based method for the physical subsystem and a combinatorial approach based on the total probability law for the cyber subsystem. In [91], dynamic and dependent failure behaviors of the smart home physical subsystem were carefully and thoroughly examined; a phase-modular approach

was further suggested, which combines MDDs and CTMCs for reliability analysis of the physical subsystem addressing effects of the failure behaviors identified. In [213], the reliability of the smart home cyber subsystem was investigated considering cascading deterministic FDEP and related competitions (described in Section II). In [214], the reliability model of [213] was extended to address cascading probabilistic FDEP.

In addition to the reliability modeling works mentioned above, some reliability-aware design mechanisms have also been studied for smart homes. For example, in [215], a trust-based transmission mechanism was proposed for enhancing reliability of the energy consumption management in the smart home. In [216], the optimal household electrical demand scheduling problem was formulated and solved to balance the customer energy consumption cost and reliability cost while considering time-varying electricity pricing.

B. Body Sensor Network Reliability

Due to the safety-critical applications of the BSN (e.g., healthcare and military), reliability modeling and design of BSNs have received good research attentions. In [92], the reliability of a BSN system subject to probabilistic FDEP and competing failure propagation and isolation effects was modeled and analyzed using a combinatorial method; the method accommodates multiple local failures of the same biosensor and different local failures having different statistical relationships with propagated failures originating from the same biosensor. In [98], the phased-mission behavior (described in Section II) was addressed in the reliability analysis of BSNs while considering the probabilistic FDEP and competitions.

Examples of reliability-based mechanisms for BSNs include a cross-layer multihop protocol that handles both medium access and routing to improve the BSN reliability while achieving high energy efficiency [217]. In [218], a technique combining the coordinated duty cycle algorithm and the random linear network coding was proposed to reduce the energy consumption of biosensors while enhancing the transmission reliability in the bottleneck zone of a wireless BSN system. In [219], a BSN architecture based on the pyramid interconnection was suggested to reduce the energy consumption and data collection delay while increasing the system resiliency and reliability. In [220], a survey of reliability and fault-tolerance techniques (e.g., node isolation and replacement) was conducted for BSNs.

C. Smart Grid Reliability

As another important IoT application, smart grids aim to enable timely fault detection and self-healing without the intervention of technicians, thus ensuring a more reliable supply of electricity and more resilient to disasters or attacks than the traditional power grids. The reliability of the smart grid itself is of great importance [67], [68]. Considerable research efforts have been dedicated to the smart grid reliability.

For instance, in [221], the reliability of an example smart grid with a community structure was analyzed using a combinatorial BDD-based method [13]. In [222], a mathematical reliability model based on the state matrix was suggested and verified using Monte Carlo simulations; several load states reduction strategies were further proposed to improve the reliability evaluation efficiency. In [223], the state matrix-based analytical method was further extended for reliability analysis of smart grids considering uncertainties of PHEVs. In [224], the RBD-based method was applied to analyze the reliability of a smart grid without considering any dependencies of system components and was demonstrated through the reliability analysis of an electricity network in Algeria. In [225], Monte Carlo simulations were applied to assess the reliability of the smart grid communication network.

In addition to studies on the reliability modeling and analysis, various reliability-aware mechanisms have also been investigated for smart grids. For instance, in [226], an agent-based restoration strategy was suggested that aims to achieve a balance between the system reliability and load balancing. In [227], a secure and fault-tolerant data aggregation scheme was proposed for improving the reliability and practicability of smart grids. In [228], a reliability optimization problem was formulated and solved to determine optimal co-allocations of distributed generation units, protective devices, and charging stations for electric vehicles or PHEVs in the smart grid.

D. Reliability of Other IoT Applications

Reliability literature is also available for other specific IoT applications in industries, transportation, disaster management, etc. For example, in [229], the reliability of a coal mine IoT for safety management was assessed using a weighted evaluation method considering key reliability factors identified using the hazard theory, system security theory, and risk analysis theory. In [230], a reliable architecture to enable quick and robust data collection for anomaly detection in oil and gas industries was suggested.

In [231], a reliability conceptual framework in the context of car tracking was proposed, which encompasses perception reliability, transmission reliability, and processing reliability. In [232], the reliability analysis based on data generated in a smart parking system was performed to predict the error rate and common types of errors occurring in the system.

In [233], the long-range communication technology was applied to achieve reliable and low-power volcanic surveillance. In [234], a robust communication protocol was proposed for a flying UAV network in the disaster rescue operation to achieve reliable and timely transmission of critical rescue information.

VII. Persective for Future Development

The IoT reliability research discussed in the previous sections is representative rather than complete, providing awareness and highlights of some significant research that should be useful to the researchers and practitioners for future developments of robust IoT systems. Fig. 2 summarizes categories of example works reviewed in this article. Table I presents the applicability of some major solution methods to each of the four IoT layers (PL, CL, SL, and AL).

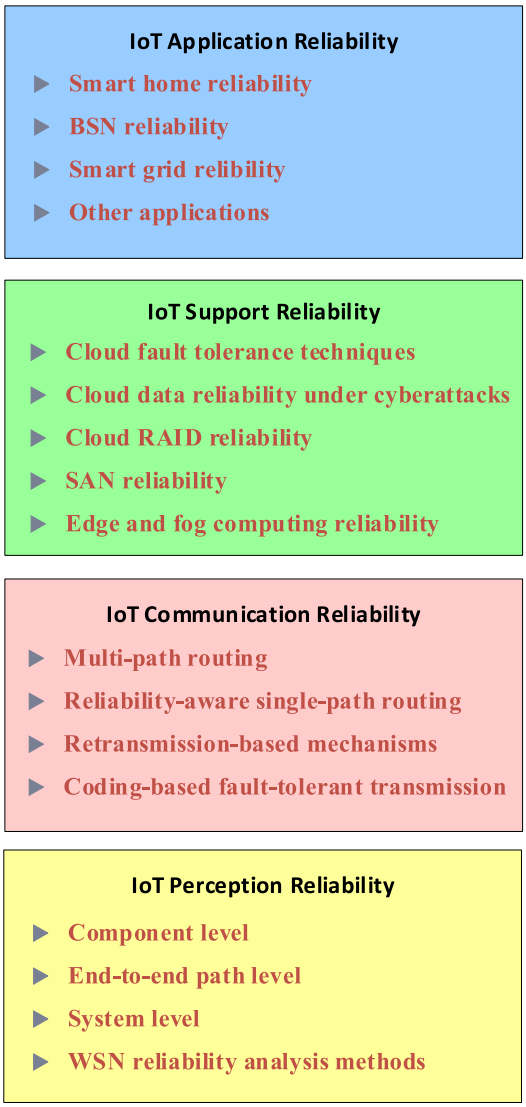

Fig. 2. Categories of IoT reliability research reviewed.

TABLE I
APPLICABILITY OF RELIABILITY SOLUTION METHODS

Solution Methods	PL	CL	SL	AL
Dynamic Fault Tree	√		√	√
Reliability Block Diagram	√			√
Network Graph Model	√	√	√	√
Decision Diagram (Binary, Multivalued)	√		√	√
Continuous-Time Markov Chain	√		√	√
Simulation	√	√	√	√
Probabilistic Combinatorial Model			√	
Redundant Design	√	√	√	√
Hardware Redundancy	√	√	√	√
Software Redundancy			√	
Information Redundancy	√	√	√	√
Data Redundancy			√	
Time Redundancy	√	√	√	

Despite the rich literature on reliability analysis and design methods, innovative and efficient reliability models and solutions will continue to remain in the high need for the next years in order to capture new features related to the growth and development of IoT systems in critical applications.

A. Modular Imperfect Coverage

As an example of complex behaviors that are still underexplored for IoT systems, imperfect coverage has been addressed in the reliability analysis of cloud-RAID systems where an uncovered disk fault causes a complete failure of the entire cloud storage system (Section V-C) [11]. This "kill-all" assumption may not be practical for hierarchical IoT systems with fault tolerance and automatic recovery implemented in multiple levels. Specifically, the hierarchical structure may aid in the fault coverage; when a fault happening in one level escapes from that level's recovery mechanism, it may be detected and covered by the higher level's recovery mechanism. A more detailed and accurate coverage model is necessary to capture the multiple levels of damages from an uncovered component fault. Such a model can be found in [235] for computer systems, which is referred to as the MICM. One direction of future developments can be applying and adapting MICM for IoT systems and considering the effects of MICM in the reliability analysis and design of IoT systems exhibiting hierarchical structures.

B. Cascading Failures

Another behavior still underexplored is cascading failures [236]. Driven by factors such as dynamic changes in network workloads caused by a component failure (e.g., the failure of a sensor node in WSNs [237] and the failure of a transmission line in smart grids [67]), a chain reaction or domino effect takes place causing extensive damage and even outage of the entire network. The cascading failure behavior has been intensively studied for traditional electrical power grids, see [238]–[241]. It is still a challenge to address its impacts in the reliability analysis of IoT networks, particularly, smart grids that unify traditional power grids, renewable energy, WSNs, and smart devices and appliances to improve energy efficiency [67], [242]. Interplays among these different smart grid components must be addressed while modeling the cascading overload failures in the system reliability analysis and design. In addition, the cascading failure process takes time and it usually lasts until system components have been remarkably compromised or the system can be functionally isolated from the source of the workload. Thus, it should be useful to develop effective in-process maintenance strategies [243] to prevent the propagation of cascading failures, limiting the scope and extent of their damages.

C. Different Types of Competitions

In addition to the competitions between different failure modes of the trigger and dependent components (i.e., competitions between failure isolation and failure propagation effects) in IoT systems with deterministic or probabilistic FDEP (Section II) [92], [98], [213], competitions may also take place between different failure processes or causes (e.g., degradations and shocks) of the same IoT component [100]. Moreover, these competing failure processes may be dependent; for example, random shocks may accelerate the degradation process [244]–[246]. It is necessary to develop a unified

framework to consider the effects of different types of competing failures and their dependencies in the IoT reliability modeling and analysis activities.

D. Reliability and Maintenance Co-Design for Resilience

Due to the mission-critical or safety-critical nature of the IoT applications [22], [51], [64], it is paramount that the IoT system be resilient to hazards or failures. This poses a great demand for resilience-based reliability metrics, models, analysis, and design methods, with the aim of capturing not only the complex IoT reliability/failure behavior but also the system restoration behavior when failures or hazards take place in the system. As one direction of future developments toward resilience, it is desirable to couple the IoT reliability modeling and analysis considering dynamic and dependent behaviors (modular imperfect coverage, cascading failures, competitions, etc.) with various types of maintenance planning activities (e.g., preventive maintenance, corrective maintenance, and opportunistic maintenance [247]) through a holistic framework. For instance, such an integration can be achieved through utilizing the IoT reliability as the objective or a constraint during the maintenance optimization process.

E. Co-Optimization of Multiple Design Factors

While reliability is a critical design requirement, other factors, such as security, safety, energy consumption, performance (e.g., response time and throughput), and cost must also be considered for practical IoT system designs and operation. Very often different requirements constitute conflicting design goals. As discussed in Section V-B, different redundancy techniques (replication, partition, and NVP) suggested in literature may enhance reliability but lower security; or enhance security but reduce reliability at the same time. Hence, optimizations have been performed to achieve a trade-off between the conflicting requirements. A comprehensive optimization framework is needed to co-consider and balance all those different design factors, providing optimal QoS to IoT applications.

F. Cross-Domain Dependency

Existing reliability research has mostly assumed that different IoT component domains (particularly, hardware, software, and human) are independent [248]–[250]. Thus, reliability metrics of different domains have often been modeled, evaluated, and optimized in a separate or independent manner. As a matter of fact, components from different domains may interact significantly [251]–[254]. Examples of interactions between human and hardware/software technological elements are abundant. Humans often make mistakes associated with the incomplete or inaccurate interpretation of system input or output; flaws in hardware and software designs may limit or reduce the performance of human users [255]. Structure interactions between hardware and software components take place in many IoT systems. For example, in the cloud computing system, software service programs are distributed to different VMs hosted on physical servers; in the event of the server malfunction, the execution of software running on the server also fails. For another example, tight interactions exist between trusted hardware and software in the software-defined WSN to ensure that behaviors of sensor nodes comply to regulations [256]. The cross-domain interplays should be explicitly modeled for the IoT reliability analysis and optimization.

G. Cross-Layer Dependency

While the majority of the existing reliability research has focused on one layer of the IoT architecture, there also exist limited research on the reliability analysis of an overall IoT system covering multiple layers. However, these works assume different IoT layers behave independently in the system reliability modeling and analysis [212], [257]. Consequently, the entire system reliability is obtained by simply multiplying the reliability of each layer. Based on the independent assumption, the reliability of each layer can be optimized separately to maximize the entire IoT system reliability. However, different layers within the IoT work cooperatively, where data and information generated in one layer are often shared among different layers for further transmission or processing [258], [259]. Malfunctions in one layer (e.g., sensors at the PL) may lead to incorrect information shared with the SL and AL, causing wrong actions or failed services. In addition, CCFs (e.g., earthquakes and lightning strikes) and cascading failures may affect components from different IoT layers simultaneously. Therefore, it is crucial to consider multiple layers from a holistic viewpoint addressing the cross-layer dependencies in the system reliability modeling, analysis, and design optimization.

H. Conclusion

Despite the rich and fast-growing body of works on IoT, the reliability research is still in its early stage. As IoT systems and applications evolve, additional new aspects of system complexity and dynamics may arise, making the existing reliability models and solutions inadequate or inaccurate. New and efficient reliability models and tools are expected for capturing the new features and behaviors, leading to more effective and accurate IoT system reliability analysis, optimization, and design. The ultimate goal is to transform our society toward being ICE.

REFERENCES

[1] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014, doi: 10.1109/JIOT.2014.2312291.

[2] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," *Internet Things*, to be published. [Online]. Available: https://doi.org/10.1016/j.iot.2019.100111

[3] J. Kempf, J. Arkko, N. Beheshti, and K. Yedavalli. *Thoughts on Reliability in the Internet of Things*. Accessed: May 2020. [Online]. Available: https://pdfs.semanticscholar.org/32f3/ddb8fe2d6acc0f04c9d515edd4913d7afabf.pdf

[4] A. Kulkarni and S. Sathe, "Healthcare applications of the Internet of Things: A review," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 5, pp. 6229–6232, 2014.

[5] C. Han, J. M. Jornet, E. Fadel, and I. F. Akyildiz, "A cross-layer communication module for the Internet of Things," *Comput. Netw.*, vol. 57, no. 3, pp. 622–633, 2013.

[6] M. R. Palattella *et al.*, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.

[7] T. T. Zin, P. Tin, and H. Hama, "Reliability and availability measures for Internet of Things consumer world perspectives," in *Proc. IEEE 5th Global Conf. Consum. Electron.*, 2016, pp. 1–2, doi: 10.1109/GCCE.2016.7800446.

[8] B. Safaei, A. M. H. Monazzah, M. B. Bafroei, and A. Ejlali, "Reliability side-effects in Internet of Things application layer protocols," in *Proc. 2nd Int. Conf. Syst. Rel. Safety (ICSRS)*, 2017, pp. 207–212, doi: 10.1109/ICSRS.2017.8272822.

[9] M. Ateeq, F. Ishmanov, M. K. Afzal, and M. Naeem, "Multi-parametric analysis of reliability and energy consumption in IoT: A deep learning approach," *Sensors*, vol. 19, no. 2, p. 309, Jan. 2019.

[10] S. Pasricha, "Overcoming energy and reliability challenges for IoT and mobile devices with data analytics," in *Proc. IEEE 31st Int. Conf. VLSI Design 17th Int. Conf. Embedded Syst. (VLSID)*, Pune, India, 2018, pp. 238–243, doi: 10.1109/VLSID.2018.69.

[11] L. Xing, G. Levitin, and C. Wang, *Dynamic System Reliability: Modeling and Analysis of Dynamic and Dependent Behaviors*. Hoboken, NJ, USA: Wiley, Mar. 2019.

[12] R. Robidoux, H. Xu, L. Xing, and M. Zhou, "Automated verification of dynamic reliability block diagrams using colored Petri nets," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 40, no. 2, pp. 337–351, Mar. 2010.

[13] L. Xing and S. V. Amari, *Binary Decision Diagrams and Extensions for System Reliability Analysis*, Cambridge, MA, USA: Wiley-Scrivener, 2015.

[14] L. Xing and Y. Dai, "A new decision diagram based method for efficient analysis on multi-state systems," *IEEE Trans. Depend. Secure Comput.*, vol. 6, no. 3, pp. 161–174, Jul.–Sep. 2009.

[15] M. Rausand and A. Hoyland, *System Reliability Theory: Models, Statistical Methods, and Applications*, 2nd ed. New York, NY, USA: Wiley, 2003.

[16] B. W. Johnson, *Design and Analysis of Fault Tolerant Digital Systems*. Reading, MA, USA: Addison-Wesley, 1989.

[17] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.

[18] J. H. Nord, A. Koohang, and J. Paliszkiewicz, "The Internet of Things: Review and theoretical framework," *Expert Syst. Appl.*, vol. 133, pp. 97–108, Nov. 2019.

[19] M. S. Roopa, S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions," *Comput. Commun.*, vol. 139, pp. 32–57, May 2019.

[20] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, "A review on Internet of Things for defense and public safety," *Sensors*, vol. 16, no. 10, p. 1644, 2016. [Online]. Available: https://doi.org/10.3390/s16101644

[21] M. C. Domingo, "An overview of the Internet of underwater things," *J. Netw. Comput. Appl.*, vol. 35, no. 6, pp. 1879–1890, 2012.

[22] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China perspective," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 349–359, Aug. 2014, doi: 10.1109/JIOT.2014.2337336.

[23] E. P. Yadav, E. A. Mittal, and H. Yadav, "IoT: Challenges and issues in Indian perspective," in *Proc. 3rd Int. Conf. Internet Things Smart Innov. Usages (IoT-SIU)*, 2018, pp. 1–5, doi: 10.1109/IoT-SIU.2018.8519869.

[24] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018, doi: 10.1109/JIOT.2017.2767291.

[25] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[26] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[27] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019, doi: 10.1109/JIOT.2018.2869847.

[28] M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, "Enforcing security in Internet of Things frameworks: A systematic literature review," *Internet Things*, vol. 6, Jun. 2019, Art. no. 100050.

[29] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in Internet of Things (IoT): A review," *J. Comput. Netw. Commun.*, vol. 2019, Jan. 2019, Art. no. 9629381. [Online]. Available: https://doi.org/10.1155/2019/9629381

[30] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet Things*, to be published. [Online]. Available: https://doi.org/10.1016/j.iot.2019.100075

[31] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, "Internet of Things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Gener. Comput. Syst.*, vol. 92, pp. 265–275, Mar. 2019.

[32] J. Hou, Y. Li, J. Yu, and W. Shi, "A survey on digital forensics in Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 1–15, Jan. 2020.

[33] N. Koroniotis, N. Moustafa, and E. Sitnikova, "Forensics and deep learning mechanisms for botnets in Internet of Things: A survey of challenges and solutions," *IEEE Access*, vol. 7, pp. 61764–61785, 2019.

[34] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches and open issues," *IEEE Commun. Surveys Tuts.*, early access, Jan. 6, 2020, doi: 10.1109/COMST.2019.2962586.

[35] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," *J. Netw. Comput. Appl.*, vol. 144, pp. 79–101, Oct. 2019.

[36] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.

[37] I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019, doi: 10.1109/ACCESS.2018.2880838.

[38] A. Altaf, H. Abbas, F. Iqbal, and A. Derhab, "Trust models of Internet of smart things: A survey, open issues, and future directions," *J. Netw. Comput. Appl.*, vol. 137, pp. 93–111, Jul. 2019.

[39] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9326–9337, Dec. 2019, doi: 10.1109/JIOT.2019.2933518.

[40] M. Imran, S. Jabbar, N. Chilamkurti, and J. J. P. C. Rodrigues, "Enabling technologies for social Internet of Things," *Future Gener. Comput. Syst.*, vol. 92, pp. 715–717, Mar. 2019.

[41] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015, doi: 10.1109/COMST.2015.2444095.

[42] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, Dec. 2016, doi: 10.1109/JIOT.2016.2584538.

[43] P. Bellavista, J. Berrocal, A. Corradi, S. K. Das, L. Foschini, and A. Zanni, "A survey on fog computing for the Internet of Things," *Pervasive Mobile Comput.*, vol. 52, pp. 71–99, Jan. 2019.

[44] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. F. Rana, "Fog computing for the Internet of Things: A survey," *ACM Trans. Internet Technol.*, vol. 19, no. 2, 2019, Art. no. 18. [Online]. Available: https://doi.org/10.1145/3301443

[45] Z. B. Valojerdi, G. Rodriguez-Navas, and H. Hansson, "Dependable fog computing: A systematic literature review," in *Proc. 45th Euromicro Conf. Softw. Eng. Adv. Appl. (SEAA)*, 2019, pp. 395–403. [Online]. Available: https://doi.org/10.1109/SEAA.2019.00066

[46] P. P. Ray, D. Dash, and D. De, "Edge computing for Internet of Things: A survey, e-healthcare case study and future direction," *J. Netw. Comput. Appl.*, vol. 140, pp. 1–22, Aug. 2019.

[47] V. Prokhorenko and M. A. Babar, "Architectural resilience in cloud, fog and edge systems: A survey," *IEEE Access*, vol. 8, pp. 28078–28095, 2020, doi: 10.1109/ACCESS.2020.2971007.

[48] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-based big data storage systems in cloud computing: Perspectives and challenges," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 75–87, Feb. 2017, doi: 10.1109/JIOT.2016.2619369.

[49] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016.

[50] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.

[51] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019, doi: 10.1109/JIOT.2019.2922538.

[52] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.

[53] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.

[54] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *J. Ind. Inf. Integr.*, vol. 15, pp. 21–28, Sep. 2019.

[55] L. Xing, "Reliability modeling of wireless sensor networks: A review," in *Recent Patents on Engineering*, Hilversum, The Netherlands: Bentham Sci., 2019, doi: 10.2174/1872212113666191209091947.

[56] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[57] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Netw.*, vol. 153, pp. 113–131, Apr. 2019.

[58] F. Samie, L. Bauer, and J. Henkel, "From cloud down to things: An overview of machine learning in Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4921–4934, Jun. 2019, doi: 10.1109/JIOT.2019.2893866.

[59] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Netw.*, vol. 151, pp. 147–157, Mar. 2019.

[60] W. Ding, X. Jing, Z. Yan, and L. T. Yang, "A survey on data fusion in Internet of Things: Towards secure and privacy-preserving fusion," *Inf. Fusion*, vol. 51, pp. 129–144, Nov. 2019.

[61] B. P. L. Lau *et al.*, "A survey of data fusion in smart city applications," *Inf. Fusion*, vol. 52, pp. 357–374, Dec. 2019.

[62] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[63] K. E. Jeon, J. She, P. Soonsawad, and P. C. Ng, "BLE beacons for Internet of Things applications: Survey, challenges, and opportunities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 811–828, Apr. 2018, doi: 10.1109/JIOT.2017.2788449.

[64] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, "Internet of Things applications: A systematic review," *Comput. Netw.*, vol. 148, pp. 241–261, Jan. 2019.

[65] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, "An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3758–3773, Oct. 2018, doi: 10.1109/JIOT.2018.2844296.

[66] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 847–870, Apr. 2018, doi: 10.1109/JIOT.2018.2802704.

[67] M. Ourahou, W. Ayrir, B. E. L. Hassouni, and A. Haddi, "Review on smart grid control and reliability in presence of renewable energies: Challenges and prospects," *Math. Comput. Simulat.*, vol. 167, pp. 19–31, Jan. 2020.

[68] F. Al-Turjman and M. Abujubbeh, "IoT-enabled smart grid via SM: An overview," *Future Gener. Comput. Syst.*, vol. 96, pp. 579–590, Jul. 2019.

[69] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[70] W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, "Industrial Internet of Things: Recent advances, enabling technologies and open challenges," *Comput. Elect. Eng.*, vol. 81, Jan. 2020, Art. no. 106522.

[71] H. Yang, S. Kumara, S. T. S. Bukkapatnam, and F. Tsung, "The Internet of Things for smart manufacturing: A review," *IISE Trans.*, vol. 51, no. 11, pp. 1190–1216, 2019, doi: 10.1080/24725854.2018.1555383.

[72] M. Ben-Daya, E. Hassini, and Z. Bahroun, "Internet of Things and supply chain management: A literature review," *Int. J. Prod. Res.*, vol. 57, nos. 15–16, pp. 4719–4742, 2019, doi: 10.1080/00207543.2017.1402140.

[73] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, "A survey of Internet of Things (IoT) in education: Opportunities and challenges," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications* (Studies in Computational Intelligence), vol. 846, A. Hassanien, R. Bhatnagar, N. Khalifa, and M. Taha, Eds. Cham, Switzerland: Springer, 2020.

[74] Y. Bouzembrak, M. Klüche, A. Gavai, and H. J. P. Marvin, "Internet of Things in food safety: Literature review and a bibliometric analysis," *Trends Food Sci. Technol.*, vol. 94, pp. 54–64, Dec. 2019.

[75] H. Habibzadeh, K. Dinesh, O. R. Shishvan, A. Boggio-Dandry, G. Sharma, and T. Soyata, "A survey of healthcare Internet of Things (HIoT): A clinical perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 53–71, Jan. 2020, doi: 10.1109/JIOT.2019.2946359.

[76] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Cleaner Prod.*, vol. 140, no. 3, pp. 1454–1464, Jan. 2017.

[77] M. Jia, A. Komeily, Y. Wang, and R. S. Srinivasan, "Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications," *Autom. Construct.*, vol. 101, pp. 111–126, May 2019.

[78] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5G and beyond: Recent advances and future trends," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019, doi: 10.1109/JIOT.2018.2887086.

[79] P. P. Ray, M. Mukherjee, and L. Shu, "Internet of Things for disaster management: State-of-the-art and prospects," *IEEE Access*, vol. 5, pp. 18818–18835, 2017, doi: 10.1109/ACCESS.2017.2752174.

[80] G. Mei, N. Xu, J. Qin, B. Wang, and P. Qi, "A survey of Internet of Things (IoT) for geo-hazards prevention: Applications, technologies, and challenges," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4371–4386, May 2020, doi: 10.1109/JIOT.2019.2952593.

[81] L. E. Lima, B. Y. L. Kimura, and V. Rosset, "Experimental environments for the Internet of Things: A review," *IEEE Sens. J.*, vol. 19, no. 9, pp. 3203–3211, May 2019, doi: 10.1109/JSEN.2019.2894127.

[82] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental Internet of Things research," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 58–67, Nov. 2011, doi: 10.1109/MCOM.2011.6069710.

[83] A. Rullo, E. Serra, and J. Lobo, "Redundancy as a measure of fault-tolerance for the Internet of Things: A review," in *Policy-Based Autonomic Data Governance* (LNCS 11550). Cham, Switzerland: Springer, 2019.

[84] A. Cook, G. Mısırlı, and Z. Fan, "Anomaly detection for IoT time-series data: A survey," *IEEE Internet Things J.*, early access, Dec. 6, 2019, doi: 10.1109/JIOT.2019.2958185.

[85] M. T. Moghaddam and H. Muccini, "Fault-tolerant IoT," in *Software Engineering for Resilient Systems SERENE 2019* (LNCS 11732), R. Calinescu and F. Di Giandomenico, Eds. Cham, Switzerland: Springer, 2019.

[86] M. Burhan, R. A. Rehman, B. Kim, and B. Khan, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors*, vol. 18, no. 9, p. 2796, 2018, doi: 10.3390/s18092796.

[87] D. Darwish, "Improved layered architecture for Internet of Things," *Int. J. Comput. Acad. Res.*, vol. 4, no. 4, pp. 214–223, 2015.

[88] A. C. Djedouboum, A. A. A. Ari, A. M. Gueroui, A. Mohamadou, and Z. Aliouat, "Big data collection in large-scale wireless sensor networks," *Sensors*, vol. 18, no. 12, p. 4474, 2018, doi: 10.3390/s18124474.

[89] L. Xing, M. Tannous, V. M. Vokkarane, H. Wang, and J. Guo, "Reliability modeling of mesh storage area networks for Internet of Things," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2047–2057, Dec. 2017.

[90] L. Mandava, L. Xing, and C. Wang, "Fault-level coverage analysis for multi-state cloud-RAID storage systems," *Eng. Rep.*, vol. 1, no. 3, Oct. 2019, Art. no. e12045.

[91] L. Xing, G. Zhao, and Y. Xiang, "Phased-mission modeling of physical layer reliability for smart homes," in *Stochastic Models in Reliability Engineering*. Boca Raton, FL, USA: CRC Press, 2020, ch. 20.

[92] Y. Wang, L. Xing, H. Wang, and G. Levitin, "Combinatorial analysis of body sensor networks subject to probabilistic competing failures," *Rel. Eng. Syst. Safety*, vol. 142, pp. 388–398, Oct. 2015.

[93] A. Chugh and S. Panda, "Strengthening clustering through relay nodes in sensor networks," *Procedia Comput. Sci.*, vol. 132, pp. 689–695, Jun. 2018.

[94] G. Levitin and L. Xing, "Reliability and performance of multi-state systems with propagated failures having selective effect," *Rel. Eng. Syst. Safety*, vol. 95, no. 6, pp. 655–661, 2010.

[95] G. Levitin, L. Xing, Y. Dai, and V. M. Vokkarane, "Dynamic checkpointing policy in heterogeneous real-time standby systems," *IEEE Trans. Comput.*, vol. 66, no. 8, pp. 1449–1456, Aug. 2017.

[96] L. Xing, A. Shrestha, and Y. Dai, "Exact combinatorial reliability analysis of dynamic systems with sequence-dependent failures," *Rel. Eng. Syst. Safety*, vol. 96, no. 10, pp. 1375–1385, Oct. 2011.

[97] L. Xing and J. B. Dugan, "Analysis of generalized phased mission system reliability, performance and sensitivity," *IEEE Trans. Rel.*, vol. 51, no. 2, pp. 199–211, Jun. 2002.

[98] Y. Wang, L. Xing, G. Levitin, and N. Huang, "Probabilistic competing failure analysis in phased-mission systems," *Rel. Eng. Syst. Safety*, vol. 176, pp. 37–51, Aug. 2018.

[99] Y. Wang, L. Xing, and L. Mandava, "Probabilistic competing failure analysis in multi-state wireless sensor networks," in *Proc. 64th Annu. Rel. Maintain. Symp. (RAMS)*, Reno, NV, USA, Jan. 2018, pp. 1–7.

[100] E. Zio, "Some challenges and opportunities in reliability engineering," *IEEE Trans. Rel.*, vol. 65, no. 4, pp. 1769–1782, Dec. 2016, doi: 10.1109/TR.2016.2591504.

[101] G. Anastasi, M. Conti, M. D. Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad Hoc Netw.*, vol. 7, no. 3, pp. 537–568, May 2009.

[102] S. Sudevalayam and P. Kulkarni, "Energy harvesting sensor nodes: Survey and implications," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 3, pp. 443–461, 3rd Quart., 2011, doi: 10.1109/SURV.2011.060710.00094.

[103] C. Wang, L. Xing, V. M. Vokkarane, and Y. Sun, "Reliability and lifetime modeling of wireless sensor nodes," *Microelectron. Rel.*, vol. 54, no. 1, pp. 160–166, Jan. 2014.

[104] T. He *et al.*, "VigilNet: An integrated sensor network system for energy-efficient surveillance," *ACM Trans. Sensor Netw.*, vol. 2, no. 1, pp. 1–38, 2006.

[105] A. E. Zonouz, L. Xing, V. M. Vokkarane, and Y. Sun, "Reliability-oriented single-path routing protocols in wireless sensor networks," *IEEE Sens. J.*, vol. 14, no. 11, pp. 4059–4068, Nov. 2014.

[106] D. Deif and Y. Gadallah, "A comprehensive wireless sensor network reliability metric for critical Internet of Things applications," *EURASIP J. Wireless Commun. Netw.*, vol. 2017 p. 145, Aug. 2017. [Online]. Available: https://doi.org/10.1186/s13638-017-0930-3

[107] L. Xing, H. Li, and H. E. Michel, "Fault-tolerance and reliability analysis for wireless sensor networks," *Int. J. Performability Eng.*, vol. 5, no. 5, pp. 419–431, Oct. 2009.

[108] L. Xing and A. Shrestha, "QoS reliability of hierarchical clustered wireless sensor network," in *Proc. 25th IEEE Int. Perform. Comput. Commun. Conf.*, Apr. 2006, pp. 641–646.

[109] H. Lee, A. Klappenecker, K. Lee, and L. Lin, "Energy efficient data management for wireless sensor networks with data sink failure," in *Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst. Conf.*, 2005, p. 7, doi: 10.1109/MAHSS.2005.1542801.

[110] A. E. Zonouz, L. Xing, V. M. Vokkarane, and Y. Sun, "A time-dependent link failure model for wireless sensor networks," in *Proc. Annu. Rel. Maintainability Symp.*, Colorado Springs, CO, USA, Jan. 2014, pp. 1–7.

[111] O. Salami, A. Bagula, and H. A. Chan, "Framework for link reliability in inter-working multi-hop wireless networks," *Math. Comput. Model.*, vol. 53, nos. 11–12, pp. 2219–2228, 2011.

[112] S. Woo and H. Kim, "Estimating link reliability in wireless networks: An empirical study and interference modeling," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1–5, doi: 10.1109/INFCOM.2010.5462250.

[113] M. A. Mahmood, W. K. G. Seah, and I. Welch, "Reliability in wireless sensor networks: A survey and challenges ahead," *Comput. Netw.*, vol. 79, pp. 166–187, Mar. 2015.

[114] Y. Huang, J.-F. Martínez, J. Sendra, and L. López, "Resilient wireless sensor networks using topology control: A review," *Sensors*, vol. 15, no. 10, pp. 24735–24770, Oct. 2015.

[115] S. Tilak, N. B. Abu-Ghazaleh, and W. Heinzelman, "A taxonomy of wireless micro-sensor network models," *Mobile Comput. Commun. Rev.*, vol. 6, no. 2, pp. 28–36, 2002.

[116] A. Shrestha, L. Xing, and H. Liu, "Infrastructure communication reliability of wireless sensor networks," in *Proc. 2nd IEEE Int. Symp. Depend. Auton. Secure Comput.*, Sep./Oct. 2006, pp. 250–257.

[117] C. Wang, L. Xing, V. M. Vokkarane, and Y. Sun, "Manycast and anycast-based infrastructure communication reliability for wireless sensor networks," in *Proc. 18th ISSAT Int. Conf. Rel. Qual. Design*, Boston, MA, USA, Jul. 2012, pp. 227–231.

[118] A. Shrestha, L. Xing, Y. Sun, and V. M. Vokkarane, "Infrastructure communication reliability of wireless sensor networks considering common-cause failures," *Int. J. Performability Eng.*, vol. 8, no. 2, pp. 141–150, Mar. 2012.

[119] A. Shrestha and L. Xing, "Quantifying application communication reliability of wireless sensor networks," *Int. J. Performability Eng.*, vol. 4, no. 1, pp. 43–56, Jan. 2008.

[120] A. Shrestha, L. Xing, and H. Liu, "Application communication reliability of wireless sensor networks," in *Proc. 12th ISSAT Int. Conf. Rel. Qual. Design*, Chicago, IL, USA, Aug. 2006, pp. 430–435.

[121] A. E. Zonouz, L. Xing, V. M. Vokkarane, and Y. Sun, "Application communication reliability of wireless sensor networks," *IET Wireless Sensor Syst.*, vol. 5, no. 2, pp. 58–67, Apr. 2015.

[122] A. E. Zonouz, L. Xing, V. M. Vokkarane, and Y. Sun, "Application communication reliability of wireless sensor networks supporting *k*-coverage," in *Proc. IEEE Int. Conf. Distrib. Comput. Sensor Syst.*, Cambridge, MA, USA, 2013, pp. 430–435.

[123] C. Wang, L. Xing, A. E. Zonouz, V. M. Vokkarane, and Y. Sun, "Communication reliability analysis of wireless sensor networks using phased-mission model," *Qual. Rel. Eng. Int.*, vol. 33, no. 4, pp. 823–837, Jun. 2017.

[124] A. Shrestha, L. Xing, and H. Liu, "Modeling and evaluating the reliability of wireless sensor networks," In *Proc. 53rd Annu. Rel. Maintainability Symp.*, Orlando, FL, USA, Jan. 2007, pp. 827–834.

[125] X. Fafoutis and L. Marchegiani, "Rethinking IoT network reliability in the era of machine learning," in *Proc. Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, Atlanta, GA, USA, 2019, pp. 1112–1119.

[126] X. Zhu, Y. Lu, J. Han, and L. Shi, "Transmission reliability evaluation for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 2, pp. 1–10, 2016.

[127] Y. Jin, H. Lin, Z. Zhang, Z. Zhang, and X. Zhang, "Estimating the reliability and lifetime of wireless sensor network," in *Proc. 4th Int. Conf. Wireless Commun. Netw. Mobile Comput.*, 2008, pp. 1–4.

[128] C. Di Martino, M. Cinque, and D. Cotroneo, "Automated generation of performance and dependability models for the assessment of wireless sensor networks," *IEEE Trans. Comput.*, vol. 61, no. 6, pp. 870–884, Jun. 2012.

[129] C. Kamyod, "End-to-end reliability analysis of an IoT based smart agriculture," in *Proc. Int. Conf. Digit. Arts Media Technol. (ICDAMT)*, 2018, pp. 258–261, doi: 10.1109/ICDAMT.2018.8376535.

[130] H. M. F. AboElFotoh, S. S. Iyengar, and K. Chakrabarty, "Computing reliability and message delay for cooperative wireless distributed sensor networks subject to random failures," *IEEE Trans. Rel.*, vol. 54, no. 1, pp. 145–155, Mar. 2005.

[131] S. Distefano, "Evaluating reliability of WSN with sleep/wake-up interfering nodes," *Int. J. Syst. Sci.*, vol. 44, no. 10, pp. 1793–1806, 2013.

[132] A. Munir and A. Gordon-Ross, "Markov modeling of fault-tolerant wireless sensor networks," in *Proc. 20th IEEE Int. Conf. Comput. Commun. Netw.*, Jul./Aug. 2011, pp. 1–6.

[133] J. Zhu, L. Tang, H. Xi, and Z. Zhang, "Reliability analysis of wireless sensor networks using Markovian model," *J. Appl. Math.*, vol. 2012, Jun. 2012, Art. no. 760359.

[134] I. Silva, L. A. Guedes, P. Portugal, and F. Vasques, "Reliability and availability evaluation of wireless sensor networks for industrial applications," *Sensors*, vol. 12, no. 1, pp. 806–838, 2012.

[135] A. E. Zonouz, L. Xing, V. M. Vokkarane, and Y. Sun, "K-coverage reliability evaluation for wireless sensor networks," in *Proc. 18th ISSAT Int. Conf. Rel. Qual. Design*, Boston, MA, USA, Jul. 2012, Art. no. 18113.

[136] A. Dâmaso, N. Rosa, and P. Maciel, "Reliability of wireless sensor networks," *Sensors*, vol. 14, no. 9, pp. 15760–15785, 2014.

[137] Y. Mo, L. Xing, and J. Jiang, "Modeling and analyzing linear wireless sensor networks with backbone support," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, Jul. 18, 2018, doi: 10.1109/TSMC.2018.2849707.

[138] I. Jemili, G. Tekaya, and A. Belghith, "A fast multipath routing protocol for wireless sensor networks," in *Proc. IEEE/ACS 11th Int. Conf. Comput. Syst. Appl. (AICCSA)*, 2014, pp. 747–754, doi: 10.1109/AICCSA.2014.70732.

[139] Y. M. Lu and V. W. S. Wong, "An energy-efficient multipath routing protocol for wireless sensor networks," *Int. J. Commun. Syst.*, vol. 20, no. 7, pp. 747–766, 2007.

[140] V. Di Valerio, F. Lo Presti, C. Petrioli, L. Picari, D. Spaccini, and S. Basagni, "CARMA: Channel-aware reinforcement learning-based multi-path adaptive routing for underwater wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 11, pp. 2634–2647, Nov. 2019.

[141] R. Ma, L. Xing, and H. E. Michel, "Fault-intrusion tolerant techniques in wireless sensor networks," in *Proc. 2nd IEEE Int. Symp. Depend. Auton. Secure Comput.*, Sep./Oct. 2006, pp. 85–94.

[142] R. Ma, L. Xing, T. Jin, and T. Song, "A data transmission mechanism for survivable sensor networks," in *Proc. IEEE Int. Conf. Netw. Archit. Storage*, Zhang Jia Jie, China, Jul. 2009, pp. 9–15.

[143] N. Maalel, E. Natalizio, A. Bouabdallah, P. Roux, and M. Kellil, "Reliability for emergency applications in Internet of Things," in *Proc. IEEE Int. Conf. Distrib. Comput. Sensor Syst.*, Cambridge, MA, USA, 2013, pp. 361–366, doi: 10.1109/DCOSS.2013.40.

[144] A. E. Zonouz, L. Xing, V. M. Vokkarane, and Y. Sun, "Hybrid wireless sensor networks: A reliability, cost and energy-aware approach," *IET Wireless Sensor Syst.*, vol. 6, no. 2, pp. 42–48, Apr. 2016.

[145] K. Machado, D. Rosário, E. Cerqueira, A. Loureiro, A. Neto, and J. N. De Souza, "A routing protocol based on energy and link quality for Internet of Things applications," *Sensors*, vol. 13, no. 2, pp. 1942–1964, 2013.

[146] D. Han, P. Cheng, J. Chen, and L. Shi, "An online sensor power schedule for remote state estimation with communication energy constraint," *IEEE Trans. Autom. Control*, vol. 59, no. 7, pp. 1942–1947, Jul. 2014.

[147] X. Liu, "Deployment strategy for multiple types of requirements in wireless sensor networks," *IEEE Trans. Cybern.*, vol. 45, no. 10, pp. 2364–2376, Oct. 2015.

[148] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2013–2027, Sep. 2016.

[149] Z. Rosberg, R. P. Liu, T. L. Dinh, Y. F. Dong, and S. Jha, "Statistical reliability for energy efficient data transport in wireless sensor networks," *Wireless Netw.*, vol. 16, no. 7, pp. 1913–1927, 2010.

[150] A. Liu, Q. Zhang, Z. Li, Y.-J. Choi, J. Li, and N. Komuro, "A green and reliable communication modeling for industrial Internet of Things," *Comput. Elect. Eng.*, vol. 58, pp. 364–381, Feb. 2017.

[151] C. Wu, Y. Ji, J. Xu, S. Ohzahata, and T. Kato, "Coded packets over lossy links: A redundancy-based mechanism for reliable and fast data collection in sensor networks," *Comput. Netw.*, vol. 70, pp. 179–191, Sep. 2014.

[152] R. Ma, L. Xing, H. E. Michel, and H. Wang, "Survivable data transmission via selective hybrid cipher in sensor networks," *Int. J. Performability Eng.*, vol. 7, no. 4, pp. 303–312, Jul. 2011.

[153] R. Ma, L. Xing, and Y. Wang, "Performance analysis of Reed–Solomon codes for effective use in survivable wireless sensor networks," *Int. J. Math. Eng. Manag. Sci.*, vol. 5, no. 1, pp. 13–28, Feb. 2020.

[154] S. A. Alabady, M. F. M. Salleh, and F. Al-Turjman, "LCPC error correction code for IoT applications," *Sustain. Cities Soc.*, vol. 42, pp. 663–673, Oct. 2018.

[155] E. Tsimbalo, X. Fafoutis, and R. J. Piechocki, "CRC error correction in IoT applications," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 361–369, Feb. 2017, doi: 10.1109/TII.2016.2605628.

[156] C. Mahapatra, Z. Sheng, V. C. M. Leung, and T. Stouraitis, "A reliable and energy efficient IoT data transmission scheme for smart cities based on redundant residue based error correction coding," in *Proc. 12th Annu. IEEE Int. Conf. Sens. Commun. Netw. Workshops (SECON Workshops)*, Seattle, WA, USA, 2015, pp. 1–6.

[157] R. S. Zakariyya, M. K. H. Jewel, O. J. Famoriji, and F. Lin, "Channel coding analysis for NB-IoT up-link transport channel," in *Proc. IEEE MTT-S Int. Wireless Symp. (IWS)*, Guangzhou, China, 2019, pp. 1–3.

[158] S. Zhao, J. Wen, S. Mumtaz, S. Garg, and B. J. Choi, "Spatially coupled codes via partial and recursive superposition for industrial IoT with high trustworthiness," *IEEE Trans. Ind. Informat.*, early access, Jan. 13, 2020, doi: 10.1109/TII.2020.2965952.

[159] S. Jain and R. Bose, "Rateless codes-based secure cooperative transmission scheme for industrial IoT," *IEEE Internet Things J.*, early access, Jan. 28, 2020, doi: 10.1109/JIOT.2020.2969955.

[160] A. Yatribi, F. Ayoub, Z. M'rabet, A. Azouaoui, and M. Belkasmi, "Hybrid automatic repeat request protocols: Turbo-codes against cyclic binary low-density parity-check codes," in *Proc. 5th Workshop Codes Cryptography Commun. Syst. (WCCCS)*, 2014, pp. 86–91.

[161] C. Pielli, È. Stefanović, P. Popovski, and M. Zorzi, "Joint compression, channel coding, and retransmission for data fidelity with energy harvesting," *IEEE Trans. Commun.*, vol. 66, no. 4, pp. 1425–1439, Apr. 2018.

[162] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in *Proc. Int. Conf. Comput. Sci. Electron. Eng.*, Hangzhou, China, 2012, pp. 648–651, doi: 10.1109/ICCSEE.2012.373.

[163] R. Nachiappan, B. Javadi, R. N. Calheiros, and K. M. Matawie, "Cloud storage reliability for big data applications: A state of the art survey," *J. Netw. Comput. Appl.*, vol. 97, pp. 35–47, Nov. 2017.

[164] C. Wang, L. Xing, H. Wang, Y. Dai, and Z. Zhang, "Performance analysis of media cloud-based multimedia systems with retrying fault-tolerance technique," *IEEE Syst. J.*, vol. 8, no. 1, pp. 313–321, Mar. 2014.

[165] L. Xing, G. Levitin, and Y. Xiang, "Defending N-version programming service components against co-resident attacks in IoT cloud systems," *IEEE Trans. Services Comput.*, early access, Mar. 13, 2019, doi: 10.1109/TSC.2019.2904958.

[166] B. Yang, F. Tan, and Y. Dai, "Performance evaluation of cloud service considering fault recovery," *J. Supercomput.*, vol. 65, pp. 426–444, Jul. 2013.

[167] X. Qiu, Y. Dai, Y. Xiang, and L. Xing, "Correlation modeling and resource optimization for cloud service with fault recovery," *IEEE Trans. Cloud Comput.*, vol. 7, no. 3, pp. 693–704, Jul.–Sep. 2019.

[168] X. Qiu, Y. Dai, Y. Xiang, and L. Xing, "A hierarchical correlation model for evaluating reliability, performance, and power consumption of a cloud service," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 3, pp. 401–412, Mar. 2016.

[169] G. Levitin, L. Xing, and Y. Dai, "Optimal data partitioning in cloud computing system with random server assignment," *Future Gener. Comput. Syst.*, vol. 70, pp. 17–25, May 2017.

[170] G. Levitin, L. Xing, and H. Huang, "Security of separated data in cloud systems with competing attack detection and data theft processes," *Risk Anal.*, vol. 39, no. 4, pp. 846–858, Apr. 2019.

[171] Y. Han, J. Chan, T. Alpcan, and C. Leckie, "Using virtual machine allocation policies to defend against co-resident attacks in cloud computing," *IEEE Trans. Depend. Secure Comput.*, vol. 14, no. 1, pp. 95–108, Jan./Feb. 2017.

[172] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," in *Proc. 16th ACM Conf. Comput. Commun. Security*, 2009, pp. 199–212.

[173] A. O. F. Atya, Z. Qian, S. V. Krishnamurthy, T. La Porta, P. McDaniel, and L. M. Marvel, "Catch me if you can: A closer look at malicious co-residency on the cloud," *IEEE/ACM Trans. Netw.*, vol. 27, no. 2, pp. 560–576, Apr. 2019.

[174] Y. Han, J. Chan, T. Alpcan, and C. Leckie, "A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 556–570, Mar. 2016.

[175] L. Xing and G. Levitin, "Balancing theft and corruption threats by data partition in cloud system with independent server protection," *Rel. Eng. Syst. Safety*, vol. 167, pp. 248–254, Nov. 2017.

[176] L. Luo, L. Xing, and G. Levitin, "Optimizing dynamic survivability and security of replicated data in cloud systems under co-residence attacks," *Rel. Eng. Syst. Safety*, vol. 192, Dec. 2019, Art. no. 106265.

[177] G. Levitin, L. Xing, and Y. Dai, "Co-residence based data vulnerability vs. security in cloud computing system with random server assignment," *Eur. J. Oper. Res.*, vol. 267, no. 2, pp. 676–686, Jun. 2018.

[178] G. Levitin, L. Xing, and Y. Xiang, "Optimization of time constrained N-version programming service components with competing task execution and version corruption processe," *Rel. Eng. Syst. Safety*, vol. 193, Jan. 2020, Art. no. 106666.

[179] T. Jin, L. Xing, and Y. Yu, "A hierarchical Markov reliability model for data storage systems with media self-recovery," *Int. J. Rel. Qual. Safety Eng.*, vol. 18, no. 1, pp. 25–41, 2011.

[180] J. Li, P. Li, R. Stones, G. Wang, Z. Li, and X. Liu, "Reliability equations for cloud storage systems with proactive fault tolerance," *IEEE Trans. Depend. Secure Comput.*, early access, Nov. 21, 2018, doi: 10.1109/TDSC.2018.2882512.

[181] M. Schnjakin and C. Meinel, "Implementation of cloud-RAID: A secure and reliable storage above the clouds," in *Grid and Pervasive Computing* (LNCS 7861), J. J. H. Park, H. R. Arabnia, C. Kim, W. Shi, and J. M. Gil, Eds. Heidelberg, Germany: Springer, 2013.

[182] Q. Liu and L. Xing, "Hierarchical reliability analysis of multi-state cloud-RAID storage system," in *Proc. IEEE Int Conf. Qual. Rel. Risk Maintenance Safety Eng.*, Beijing, China, Jul. 2015, pp. 1–7.

[183] Q. Liu and L. Xing, "Reliability modeling of cloud-RAID-6 storage system," *Int. J. Future Comput. Commun.*, vol. 4, no. 6, pp. 415–420, Dec. 2015.

[184] L. Mandava and L. Xing, "Reliability analysis of cloud-RAID 6 with imperfect fault Coverage," *Int. J. Performability Eng.*, vol. 13, no. 3, pp. 289–297, May 2017.

[185] L. Mandava, L. Xing, V. M. Vokkarane, and O. Tannous, "Reliability analysis of multi-state cloud-RAID with imperfect element-level coverage," in *Reliability Engineering: Theory and Applications*, I. Vonta and M. Ram, Eds. Hoboken, NJ, USA: CRC Press, Oct. 2018, ch. 4, pp. 61–82.

[186] L. Mandava and L. Xing, "Balancing reliability and cost in Cloud-RAID systems with fault-level coverage," *Int. J. Math. Eng. Manag. Sci.*, vol. 4, no. 5, pp. 1068–1080, Oct. 2019.

[187] L. Mandava and L. Xing, "Optimizing imperfect coverage cloud-RAID systems considering reliability and cost," *Int. J. Rel. Qual. Safety Eng.*, vol. 27, no. 2, 2020, Art. no. 204001. [Online]. Available: https://doi.org/10.1142/S021853932040001X

[188] J. Gu *et al.*, "Optimizing the parity check matrix for efficient decoding of RS-based cloud storage systems," in *Proc. IEEE Int. Parallel Distrib. Process. Symp. (IPDPS)*, Rio de Janeiro, Brazil, 2019, pp. 533–544, doi: 10.1109/IPDPS.2019.00063.

[189] R. Barker and P. Massiglia, *Storage Area Network Essentials: A Complete Guide to Understanding and Implementing SANs*. Hoboken, NJ, USA: Wiley, 2002, p. 198.

[190] R. Telikepalli, T. Drwiega, and J. Yan, "Storage area network extension solutions and their performance assessment," *IEEE Commun. Mag*, vol. 42, no. 4, pp. 56–63, Apr. 2004.

[191] X. Qiu, R. Telikepalli, T. Drwiega, and J. Yan, "Reliability and availability assessment of storage area network extension solutions," *IEEE Commun. Mag.*, vol. 43, no. 3, pp. 80–85, Mar. 2005.

[192] L. Xing, "An efficient binary-decision-diagram-based approach for network reliability and sensitivity analysis," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 38, no. 1, pp. 105–115, Jan. 2008.

[193] A. Shrestha and L. Xing, "DNA: A tool for network reliability and sensitivity analysis," in *Proc. 4th Int. Conf. Qual. Rel. (ICQR4)*, 2005, pp. 1–10.

[194] G. W. Scheer and R. E. Moxley, "Digital communications improve contact I/O reliability," in *Proc. Power Syst. Conf. Adv. Metering Protect. Control Commun. Distrib. Resour*, Clemson, SC, USA, 2006, pp. 363–377.

[195] N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob, and M. Imran, "The role of edge computing in Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 110–115, Nov. 2018, doi: 10.1109/MCOM.2018.1700906.

[196] M. Yannuzzi, R. Milito, R. Serral-Gracià, D. Montero, and M. Nemirovsky, "Key ingredients in an IoT recipe: Fog computing, cloud computing, and more fog computing," in *Proc. IEEE 19th Int. Workshop Comput.-Aided Model. Design Commun. Links Netw. (CAMAD)*, 2014, pp. 325–329, doi: 10.1109/CAMAD.2014.7033259.

[197] H. Liu, L. T. Yang, M. Lin, D. Yin, and Y. Guo, "A tensor-based holistic edge computing optimization framework for Internet of Things," *IEEE Netw.*, vol. 32, no. 1, pp. 88–95, Jan./Feb. 2018, doi: 10.1109/MNET.2018.1700193.

[198] S. Liu, C. Guo, F. Al-Turjman, K. Muhammad, and V. H. C. de Albuquerque, "Reliability of response region: A novel mechanism in visual tracking by edge computing for IIoT environments," *Mech. Syst. Signal Process.*, vol. 138, Apr. 2020, Art. no. 106537.

[199] B. Han, S. Wong, C. Mannweiler, M. R. Crippa, and H. D. Schotten, "Context-awareness enhances 5G multi-access edge computing reliability," *IEEE Access*, vol. 7, pp. 21290–21299, 2019, doi: 10.1109/ACCESS.2019.2898316.

[200] C.-F. Liu, M. Bennis, and H. V. Poor, "Latency and reliability-aware task offloading and resource allocation for mobile edge computing," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Singapore, 2017, pp. 1–7, doi: 10.1109/GLOCOMW.2017.8269175.

[201] J. Liu and Q. Zhang, "Reliability and latency aware code-partitioning offloading in mobile edge computing," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Marrakesh, Morocco, 2019, pp. 1–7, doi: 10.1109/WCNC.2019.8885778.

[202] N. Vance, M. T. Rashid, D. Zhang, and D. Wang, "Towards reliability in online high-churn edge computing: A deviceless pipelining approach," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Washington, DC, USA, 2019, pp. 301–308, doi: 10.1109/SMARTCOMP.2019.00066.

[203] Q. Peng, H. Jiang, M. Chen, J. Liang, and Y. Xia, "Reliability-aware and deadline-constrained workflow scheduling in mobile edge computing," in *Proc. IEEE 16th Int. Conf. Netw. Sens. Control (ICNSC)*, Banff, AB, Canada, 2019, pp. 236–241, doi: 10.1109/ICNSC.2019.8743291.

[204] K. Dantu, S. Y. Ko, and L. Ziarek, "RAINA: Reliability and adaptability in Android for fog computing," *IEEE Commun. Mag.*, vol. 55, no. 4, pp. 41–45, Apr. 2017, doi: 10.1109/MCOM.2017.1600901.

[205] J. Pereira, L. Ricardo, M. Luís, C. Senna, and S. Sargento, "Assessing the reliability of fog computing for smart mobility applications in VANETs," *Future Gener. Comput. Syst.*, vol. 94, pp. 317–332, May 2019.

[206] X. Hou, Z. Ren, J. Wang, S. Zheng, W. Cheng, and H. Zhang, "Distributed fog computing for latency and reliability guaranteed swarm of drones," *IEEE Access*, vol. 8, pp. 7117–7130, 2020, doi: 10.1109/ACCESS.2020.2964073.

[207] J. Yao and N. Ansari, "Fog resource provisioning in reliability-aware IoT networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8262–8269, Oct. 2019, doi: 10.1109/JIOT.2019.2922585.

[208] J. Wang, K. Liu, B. Li, T. Liu, R. Li, and Z. Han, "Delay-sensitive multi-period computation offloading with reliability guarantees in fog networks," *IEEE Trans. Mobile Comput.*, early access, May 27, 2019, doi: 10.1109/TMC.2019.2918773.

[209] N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "Towards fault tolerant fog computing for IoT-based smart city applications," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, 2019, pp. 752–757, doi: 10.1109/CCWC.2019.8666447.

[210] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, "Smart homes and their users: A systematic analysis and key challenges," *Pers. Ubiquitous Comput.*, vol. 19, no. 2, pp. 463–476, 2015.

[211] L. Jiang, D. Liu, and B. Yang, "Smart home research," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 2. Shanghai, China, 2004, pp. 659–663, doi: 10.1109/ICMLC.2004.1382266.

[212] G. Zhao, L. Xing, Q. Zhang, and X. Jia, "A hierarchical combinatorial reliability model for smart home systems," *Qual. Rel. Eng. Int.*, vol. 34, no. 1, pp. 37–52, Feb. 2018.

[213] G. Zhao and L. Xing, "Competing failure analysis considering cascading functional dependence & random failure propagation time," *Qual. Rel. Eng. Int.*, vol. 35, no. 7, pp. 2327–2342, 2019. [Online]. Available: https://doi.org/10.1002/qre.2513

[214] G. Zhao and L. Xing, "Competing failure analysis in IoT systems with cascading probabilistic function dependence," *Rel. Eng. Syst. Safety*, vol. 198, Jun. 2020, Art. no. 106812. [Online]. Available: https://doi.org/10.1016/j.ress.2020.106812

[215] U. S. Premarathne, I. Khalil, and M. Atiquzzaman, "Trust based reliable transmissions strategies for smart home energy consumption management in cognitive radio based smart grid," *Ad Hoc Netw.*, vol. 41, pp. 15–29, May 2016.

[216] M. Rastegar, M. Fotuhi-Firuzabad, and H. Zareipour, "Home energy management incorporating operational priority of appliances," *Int. J. Elect. Power Energy Syst.*, vol. 74, pp. 286–292, Jan. 2016.

[217] B. Braem, B. Latré, C. Blondia, I. Moerman, and P. Demeester, "Improving reliability in multi-hop body sensor networks," in *Proc. 2nd Int. Conf. Sensor Technol. Appl. (SENSORCOMM)*, 2008, pp. 342–347, doi: 10.1109/SENSORCOMM.2008.47.

[218] H. Alshaheen and H. Takruri-Rizk, "Energy saving and reliability for wireless body sensor networks (WBSN)," *IEEE Access*, vol. 6, pp. 16678–16695, 2018, doi: 10.1109/ACCESS.2018.2817025.

[219] H. N. Almajed, A. S. Almogren, and A. Altameem, "A resilient smart body sensor network through pyramid interconnection," *IEEE Access*, vol. 7, pp. 51039–51046, 2019, doi: 10.1109/ACCESS.2019.2909557.

[220] M. Salayma, A. Al-Dubai, I. Romdhani, and Y. Nasser, "Wireless body area network (WBAN): A survey on reliability, fault tolerance, and technologies coexistence," *ACM Comput. Surveys*, vol. 50, no. 1, p. 3, 2017.

[221] Y. Mo, L. Xing, W. Guo, S. Cai, Z. Zhang, and J. Jiang, "Reliability analysis of IoT networks with community structures," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 304–315, Jan.–Mar. 2020, doi: 10.1109/TNSE.2018.2869167.

[222] H. Hashemi-Dezaki, A. M. Hariri, and M. A. Hejazi, "Impacts of load modeling on generalized analytical reliability assessment of smart grid under various penetration levels of wind/solar/non-renewable distributed generations," *Sustain. Energy Grids Netw.*, vol. 20, Dec. 2019, Art. no. 100246.

[223] A. M. Hariri, H. Hashemi-Dezaki, and M. A. Hejazi, "A novel generalized analytical reliability assessment method of smart grids including renewable and non-renewable distributed generations and plug-in hybrid electric vehicles," *Rel. Eng. Syst. Safety*, vol. 196, Apr. 2020, Art. no. 106746.

[224] B. Bousshoua and A. Elmaouhab, "Smart grid reliability using reliable block diagram case study: Adrar's isolated network of Algeria," in *Proc. Int. Conf. Power Gener. Syst. Renew. Energy Technol. (PGSRET)*, Istanbul, Turkey, 2019, pp. 1–6, doi: 10.1109/PGSRET.2019.8882711.

[225] B. Appasani, D. K. R. Mohanta, "Chapter 4—Monte-Carlo simulation models for reliability analysis of low-cost IoT communication networks in smart grid," in *Advances in Ubiquitous Sensing Applications for Healthcare, Real-Time Data Analytics for Large Scale Sensor Data*, vol. 6, H. Das, N. Dey, and V. E. Balas, Eds. London, U.K.: Academic, 2020, pp. 73–96.

[226] Y. Ren, D. Fan, Q. Feng, Z. Wang, B. Sun, and D. Yang, "Agent-based restoration approach for reliability with load balancing on smart grids," *Appl. Energy*, vol. 249, pp. 46–57, Sep. 2019.

[227] H. Bao and R. Lu, "A new differentially private data aggregation with fault tolerance for smart grid communications," *IEEE Internet Things J.*, vol. 2, no. 3, pp. 248–258, Jun. 2015.

[228] A. M. Hariri, M. A. Hejazi, and H. Hashemi-Dezaki, "Reliability optimization of smart grid based on optimal allocation of protective devices, distributed energy resources, and electric vehicle/plug-in hybrid electric vehicle charging stations," *J. Power Sources*, vol. 436, Oct. 2019, Art. no. 226824.

[229] P. Kunkun and L. Xiangong, "Reliability evaluation of coal mine Internet of Things," in *Proc. IEEE Int. Conf. Identification Inf. Knowl. Internet Things*, Beijing, China, 2014, pp. 301–302, doi: 10.1109/IIKI.2014.68.

[230] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, M. S. Hossain, and M. Atiquzzaman, "A reliable Internet of Things based architecture for oil and gas industry," in *Proc. IEEE 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 705–710, doi: 10.23919/ICACT.2017.7890184.

[231] M. O. Thomas and B. B. Rad, "Reliability evaluation metrics for Internet of Things, car tracking system: A review," *Int. J. Inf. Technol. Comput. Sci.*, vol. 2, pp. 1–10, Feb. 2017, doi: 10.5815/ijitcs.2017.02.01.

[232] A. Araújo, R. Kalebe, G. Giraõ, I. Filho, K. Gonçalves, and B. Neto, "Reliability analysis of an IoT-based smart parking application for smart cities," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Boston, MA, USA, 2017, pp. 4086–4091, doi: 10.1109/BigData.2017.8258426.

[233] S. Awadallah, D. Moure, and P. Torres-González, "An Internet of Things (IoT) application on volcano monitoring," *Sensors*, vol. 19, no. 21, p. 4651, 2019. [Online]. Available: https://doi.org/10.3390/s19214651

[234] T. Ahn, J. Seok, I. Lee, and J. Han, "Reliable flying IoT networks for UAV disaster rescue operations," *Mobile Inf. Syst.*, vol. 2018, Aug. 2018, Art. no. 2572460. [Online]. Available: https://doi.org/10.1155/2018/2572460

[235] L. Xing, "Reliability modeling and analysis of complex hierarchical systems," *Int. J. Rel. Qual. Safety Eng.*, vol. 12, no. 6, pp. 477–492, Dec. 2005.

[236] L. Xing, B. A. Morrissette, and J. B. Dugan, "Combinatorial reliability analysis of imperfect coverage systems subject to functional dependence," *IEEE Trans. Rel.*, vol. 63, no. 1, pp. 367–382, Mar. 2014.

[237] X. Fu, H. Yao, and Y. Yang, "Modeling cascading failures for wireless sensor networks with node and link capacity," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7828–7840, Aug. 2019.

[238] L. Chang and Z. Wu, "Performance and reliability of electrical power grids under cascading failures," *Int. J. Elect. Power Energy Syst.*, vol. 33, no. 8, pp. 1410–1419, 2011.

[239] H. Ren and I. Dobson, "Using transmission line outage data to estimate cascading failure propagation in an electric power system," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 55, no. 9, pp. 927–931, Sep. 2008.

[240] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," *Int. J. Elect. Power Energy Syst.*, vol. 28, no. 9, pp. 627–633, 2006.

[241] L. Chen, D. Yue, C. Dou, Z. Cheng, and J. Chen, "Robustness of cyber-physical power systems in cascading failure: Survival of interdependent clusters," *Int. J. Elect. Power Energy Syst.*, vol. 114, Jan. 2020, Art. no. 105374.

[242] M. Adnan and M. Tariq, "Cascading overload failure analysis in renewable integrated power grids," *Rel. Eng. Syst. Safety*, vol. 198, Jun. 2020, Art. no. 106887.

[243] C. Liu, D. Li, E. Zio, and R. Kang, "A modeling framework for system restoration from cascading failures," *PLoS ONE*, vol. 9, no. 12, 2014, Art. no. e112363.

[244] J. Tang, C. Chen, and L. Huang, "Reliability assessment models for dependent competing failure processes considering correlations between random shocks and degradations," *Qual Rel. Eng. Int.*, vol. 35, no. 1, pp. 179–191, 2019.

[245] H. Che, S. Zeng, J. Guo, and Y. Wang, "Reliability modeling for dependent competing failure processes with mutually dependent degradation process and shock process," *Rel. Eng. Syst. Safety*, vol. 180, pp. 168–178, Dec. 2018.

[246] J. Shen, A. Elwany, and L. Cui, "Reliability analysis for multi-component systems with degradation interaction and categorized shocks," *Appl. Math. Model.*, vol. 56, pp. 487–500, Apr. 2018.

[247] C. Zhang, W. Gao, T. Yang, and S. Guo, "Opportunistic maintenance strategy for wind turbines considering weather conditions and spare parts inventory management," *Renew. Energy*, vol. 133, pp. 703–711, Apr. 2019.

[248] S. B. Grimsmo, "Reliability issues when providing M2M services in the Internet of Things" M.S. thesis, Dept. Telematics, Norwegian Univ. Sci. Technol., Trondheim, Norway, 2009. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/262009

[249] S. Sinche *et al.*, "Assessing redundancy models for IoT reliability," in *Proc. IEEE 19th Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, 2018, pp. 14–15, doi: 10.1109/WoWMoM.2018.8449816.

[250] S. Pokorni, "Reliability and availability of the Internet of Things," *Mil. Tech. Courier*, vol. 67, no. 3, p. 588, 2019, doi: 10.5937/vojtehg67-21363.

[251] M. Ahmad, "Reliability models for the Internet of Things: A paradigm shift," in *Proc. IEEE Int. Symp. Softw. Rel. Eng. Workshops*, 2014, pp. 52–59, doi: 10.1109/ISSREW.2014.107.

[252] Y. Zeng, L. Xing, Q. Zhang, and X. Jia, "An analytical method for reliability analysis of hardware-software co-design system," *Qual. Rel. Eng. Int.*, vol. 35, no. 1, pp. 165–178, Feb. 2019.

[253] K. Kanoun and M. Borrel, "Dependability of fault-tolerant systems-explicit modeling of the interactions between hardware and software components," in *Proc. IEEE Int. Comput. Perform. Depend. Symp.*, 1996, pp. 252–261, doi: 10.1109/IPDS.1996.540226.

[254] X. Deng and W. Jiang, "Dependence assessment in human reliability analysis using an evidential network approach extended by belief rules and uncertainty measures," *Ann. Nucl. Energy*, vol. 117, pp. 183–193, Jul. 2018.

[255] S. Vukadinovic, I. Macuzic, M. Djapan, and M. Milosevic, "Early management of human factors in lean industrial systems," *Safety Sci.*, vol. 119, pp. 392–398, Nov. 2019.

[256] A. Anadiotis, L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, "SD-WISE: A software-defined wireless sensor network," *Comput. Netw.*, vol. 159, pp. 84–95, Aug. 2019.

[257] Y. Li and L. Tian, "Comprehensive evaluation method of reliability of Internet of Things," in *Proc. IEEE 9th Int. Conf. P2P Parallel Grid Cloud Internet Comput.*, 2014, pp. 262–266, doi: 10.1109/3PGCIC.2014.74.

[258] B. Alla. (2018). *Cross-Layer Design in Internet of Things (IoT): Issues and Possible Solutions*. [Online]. Available: https://www.researchgate.net/publication/329970086_Cross-layer_design_in_Internet_of_things_IoT_Issues_and_possible_solutions

[259] V. G. Guimaraes, R. M. de Moraes, K. Obraczka, and A. Bauchspiess, "A novel IoT protocol architecture: Efficiency through data and functionality sharing across layers," in *Proc. IEEE 28th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Valencia, Spain, 2019, pp. 1–9, doi: 10.1109/ICCCN.2019.8846919.

Liudong Xing (Senior Member, IEEE) received the B.E. degree in computer science from Zhengzhou University, Zhengzhou, China, in 1996, and the M.S. and Ph.D. degrees in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in 2000 and 2002, respectively.

She is a Professor with the Department of Electrical and Computer Engineering, University of Massachusetts (UMass) Dartmouth, Dartmouth, MA, USA. She has published over 200 journal articles, and two books titled *Binary Decision Diagrams and Extensions for System Reliability Analysis* and *Dynamic System Reliability: Modeling and Analysis of Dynamic and Dependent Behaviors*. Her current research interests include reliability and resilience modeling, analysis, and optimization of complex systems and networks.

Prof. Xing was a recipient of the Leo M. Sullivan Teacher of the Year Award in 2014, the Scholar of the Year Award in 2010, the Outstanding Women Award in 2011 of UMass Dartmouth, the 2018 IEEE Region 1 Outstanding Teaching in an IEEE Area of Interest (University or College) Award, the 2015 ChangJiang Scholar Award by the Ministry of Education of China, and the 2007 IEEE Region 1 Technological Innovation (Academic) Award. She was also a co-recipient of the Best (Student) Paper Award at several conferences and journals. She is an Associate Editor or an Editorial Board Member of multiple journals, including *Reliability Engineering & System Safety* and the *International Journal of Systems Science*. She is a Fellow of the International Society of Engineering Asset Management.