PROSE–Proactive Resilience in Internet of Things: Targeted Attacks and Countermeasures

Usman Ashraf, *Member, IEEE*

Abstract— **Internet of Things (IoT) is the frontier of wireless networking and provides unprecedented control and information over the network. In particular, the advent of Industrial IoTs and the use of IoT in security and military have necessitated the need to respect stringent delay and reliability constraints, while IoTs promise innovative solutions but their evolution also poses some concerns, with security being the foremost. Due to the fact that these systems operate on sensitive data and are often involved in industrial production processes or critical battleground communication; therefore they are ideal targets for a range of network attacks. This paper explores the novel problem of the elimination of critical IoT nodes to minimize the data-carrying capacity of the IoT network resulting in denial of service. This paper proposes PROSE–a proactive network fortifying solution which focuses on designing resilient IoTs by proactively identifying critical nodes in the network so that they can be protected by installing backups. We assume a worst-case scenario with an adversary that has complete knowledge of the network topology and traffic patterns and can capture/disable a subset of nodes with the aim of minimizing the maximum network flow. PROSE contributes by proactively identifying the nodes that are most vulnerable to the throughput attack assuming a worst-case adversarial scenario and models the problem as a mixed integer linear program. In addition, we propose an efficient heuristic algorithm. Simulation results validate that PROSE efficiently identifies the most vulnerable IoT nodes.**

Index Terms— **Wireless mesh networks, interdiction, fortification.**

I. Introduction

INTERNET of Things (IoT) is a ground-breaking communication paradigm in which billions of smart devices connect to the Internet. Traditionally, end devices such as PCs, laptops and servers connect to the Internet, but in the IoT paradigm, common objects such as sensors, actuators, RFID tags, mobile phones and home appliances are equipped with sensing and processing capability along with the ability to connect to the Internet. Billions of these devices spread across the world in a diverse range of contexts can provide ubiquitous intelligence. The IoT will experience an explosive growth with an ever increasing number of smart devices being deployed across the world in several domains including industry, health-care, security and transportation. Moreover, the IoT paradigm is mainly focused at providing a smart system designed around devices who participate in collaborative environments.

Providing a diverse range of services - from industrial control to medical health care, these sensor based wireless multihop networks have become an integral part of modern industry. License-free wireless technologies have experienced tremendous with increasing speed and wireless coverage with reducing the hardware cost and increasing off-the-shelf availability. As a consequence, IoT networks are increasingly being used in security, rescue as well as military applications. However, perhaps one of the biggest applications of IoTs is in the industry. Due to their particular deployment, ensuring the security and reliability of these networks has become an important goal as more of these networks are deployed across the world in different scenarios with varied applications.

The IoT will revolutionize several areas of human life including industrial production, security, health-care and entertainment. Another reason for the stellar growth of the IoT is the fact that the wireless technologies such as ZigBee (802.15.4) and Wi-Fi (802.11) are license-free, cheap and commercially available off-the-shelf. Due to the tremendous benefit potential, we are today witnessing a proliferation of the IoT paradigm in a growing number of places around the world. Along with the tremendous promise of the IoT, there are several research issues that must be addressed before we can realize the full potential of IoT networks. This requires efforts at several frontiers concurrently, in order to effectively push the state-of-the-art in IoT. Some major issues facing IoTs include the issue of efficiency, interoperability, reliability and security at massive scales. The enormous deployment scale of IoT networks comprising of billions of heterogeneous devices will exacerbate these problems in the coming years. Security and robustness are some of the most critical research challenges for IoT networks. Thus, while the IoT paradigm has several application areas, but arguably, military and industry stand out as the most important. In both, security and robustness against failures due to natural or malicious reasons are of paramount importance. Industrial and security based IoT deployments require real-time performance and are therefore more vulnerable against several different types of network attacks.

Figure 1 shows the structure of Internet of Things including IoT gateways, relays and Coordinating Devices (CDs). The CDs are specialized devices which provide a connectivity structure for different types of end devices including RFID tags, Bluetooth, ZigBee and other Wi-Fi end devices. The IoT relays provide multihop connectivity for

Manuscript received July 15, 2018; revised August 27, 2018; accepted September 12, 2018. Date of publication September 20, 2018; date of current version November 16, 2018. The associate editor coordinating the review of this paper and approving it for publication was Prof. Vedran Bilas.

The author is with the Department of Computer Networks and Communications, King Faisal University, Hofuf 31982, Saudi Arabia (e-mail: uashraf@kfu.edu.sa).

Digital Object Identifier 10.1109/JSEN.2018.2871499

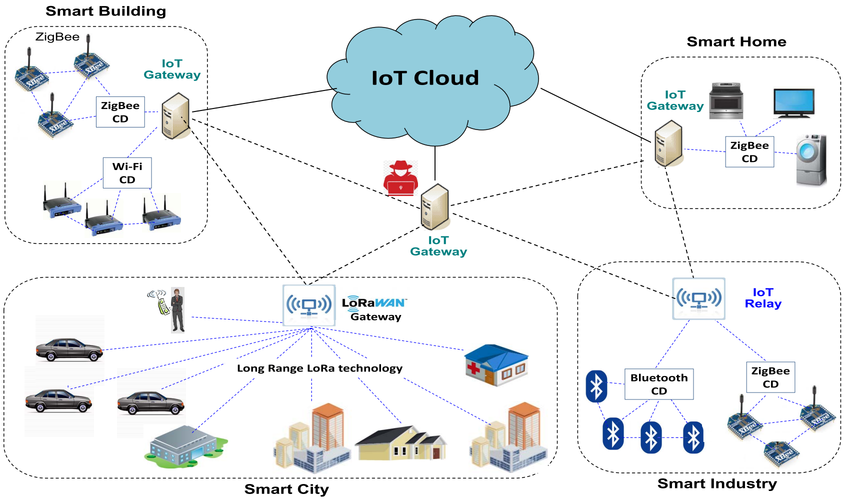


Fig. 1. IoT structure and critical attack position.

IoT gateways, while the IoT gateways provide the eventual access to the wired Internet. Attacks can target any node in this hierarchy.

IoTs are particularly vulnerable to Denial of Service (DoS) attacks. DoS attacks are primarily aimed at denying the legitimate users the provisioning of services as per the mutual agreement. These attacks have several different variations and mainly target at reducing the performance of the network in some way. For the particular case of IoTs, these networks have various attack surfaces involving both the hardware as well as the software. In particular, the electronic equipment in IoT devices are subject to physical attacks. For the software, malicious code, and viruses can affect the software. In terms of communication protocols, attacks such as man-in-the-middle-attack, black hole and white hole attacks are common.

Some attacks particularly focus on sabotaging the data carrying capacity of the network by identifying and attacking critical nodes and therefore steps must be taken to ensure the resilience of the network against these types of attacks. This family of attacks has been around for nearly a century with attacks aimed at reducing the capacity of networks. For IoT networks, the attacks can target bringing down or slowing critical nodes e.g. IoT gateways. In this paper, We focus on attacks which target key nodes in IoT networks with the aim of minimizing the flow of data across the network. By understanding how nodes of varying importance impact the network performance, focused resilience strategies such as installing backups or enhancing physical security of those selected nodes can be applied. Attacks aimed at eliminating critical sensor nodes are a relatively recently explored [1]–[11] phenomena and it was demonstrated that the elimination of nodes has a major impact on the network lifetime.

We argue that while network lifetime is an important criterion, but the data communication task carried out by the network is also critical, especially in the context of IoT deployments in military or industry where the importance of critical data reaching to sensitive locations is of central importance. Moreover, with the advent of new technologies such as LoRaWAN, they offer tremendous amount of lifetime and can cover extremely large distances. The problem of identifying critical nodes whose elimination will maximize the damage to the aggregate data carrying capacity of the network has not been explored in the context of IoT networks. With this goal in mind, this paper makes the following contributions:

- We discuss the vulnerability of IoT networks against critical nodes attack and highlight how an adversary can launch a node elimination attack on IoT networks to sabotage the data carrying capacity of the network
- We propose PROSE - a proactive network fortifying scheme which enhances resilience of IoT networks against worst-case adversarial attack by developing a Mixed Integer Linear Programming (MILP) model to identify the key IoT node positions
- The proposed exact optimization model is NP-Hard and we devise an efficient heuristic algorithm which can provide an approximate solution quickly using a utility function based on the aggregate flow traversing each node
- We implement the proposed solution for identifying critical network nodes along with two other related solutions and provide comparative simulation results evaluation.

The rest of the paper is organized as follows. Section II presents an overview of the start-of-the-art solutions related to critical node attacks in sensor and IoT networks along with a discussion of the different parameters that are targeted. Section III presents the motivation, the optimization model and the greedy heuristic algorithm. Section IV presents performance evaluation results against two existing solutions while Section V concludes the paper with future directions.

II. Related Work

Security concerns for IoTs in industrial or military situations are considerably more complex as they are being used to control physical devices and machines and the data is significantly more critical such that any loss can have a profound impact. Traditionally, authentication has been the classical technique used for providing effective security, and a large number of authentication schemes have been proposed to enhance the security of IoT networks [12]–[15]. However, there are several new challenges that cannot be resolved through authentication mechanisms alone. As the importance and pervasiveness of IoT networks has increased substantially, so have the number and type of attacks carried out against them. Network resilience against failures should be an integral part of network design for IoT networks and while a significant number of redundancy and recovery solutions for incorporating network resilience have been proposed in other domains, IoTs have peculiar characteristics which make their adoption difficult.

Recently, elimination and incapacitation attacks targeting critical nodes have been explored in the context of wireless sensor networks [3]–[10]. Most existing works in this domain focus on identifying critical nodes whose elimination will have a major impact on network lifetime. These works [3], [4] focus on the criticality aspect of sensor networks, and more specifically, identifying those nodes which have the highest degradation impact on the network performance, in particular, network lifetime. Yuksel *et al.* [3] limit their study to a single critical node while Yildiz *et al.* [4] explore two algorithms-sequential and bulk- for the identification of critical nodes. The difference between the two is that the sequential algorithm identifies critical nodes by removing them one by one from the network whereas Bulk algorithm finds critical nodes in one iteration. The sequential algorithm has a lower complexity whereas the bulk algorithm is more time consuming and complex. For our work, we recommend using a sequential algorithm for the exact solution, but propose a more efficient (albeit approximate) algorithm for the greedy algorithm.

Oteafy and Hassanein [5], [6] propose a resilient architecture that decouples operational processes from the nodes. In [7] a disaster resilient architecture is proposed for IoT networks used in health care. Han *et al.* [8] propose two algorithms for relay node placement to provide fault tolerance for heterogeneous wireless sensor network. In [9], an attack-resilient wireless sensor networks for smart electric vehicles. Kamruzzaman *et al.* [10] propose an algorithm for an ad hoc network formation linked to device-to-device communications for the creation of a robust post-disaster management framework. Kahjogh *et al.* [11] address the same problem of the impact of elimination of sensor nodes, but their focus is on how this affects the delay and how to minimize the delay. Authors propose a methodology to identify a group of critical nodes whose elimination results in the highest increase in the latency.

In a related thread of research, the concept of adding spare nodes to the network in order to augment the resilience has also been explored [16]–[18]. Niati *et al.* [16] explore adding spare nodes as relay nodes (mirror nodes) or as replacements for dead nodes. Authors show that both options improves lifetime. Singh and Buttar [17] introduce redundant spare nodes, improve on the LEACH protocol and combine it with spare node deployment which shows that using spare node deployment approach there is improvement in network lifetime and also redundant data transmission reduces. Bakr and Lilien [18] propose the LEACH-SM protocol which improves the LEACH protocol [19] by adding spare nodes such that both metrics of lifetime and latency are improved. Dagdeviren *et al.* [2] propose a computationally tractable algorithm based on connected dominating set theory to identify the critical nodes, which are located strategically such that their removal breaks the network into disconnected clusters. The neighbor degree of nodes is considered the prime motivating metric. However, the limitation is that only topological importance i.e. connectivity is considered without actual traffic patterns which may not be correlated with connectivity.

Some works address physical attacks [20], [21] on IoT networks. In [20] a lightweight Physically Unclonable Functions (PUFs) based authentication protocol has been proposed with the unique security feature of not storing secrets in the IoT devices while keeping the server storage requirements to a minimum. In [21] another lightweight and practical anonymous authentication protocol based on PUFs has been proposed which contributes to state-of-the-art by ensuring that protocols remain safe even if an adversary has physical access to RFID tags. Similar works [22] address the same line of research. Another interesting contribution in the area [23] addresses security and privacy concerns for IoT based Body Sensor Networks (BSNs) which includes a lightweight anonymous authentication protocol for ensuring mutual authentication and anonymity while thwarting attacks. An authenticated encryption scheme is also proposed based on offset codebook (OCB) mode. Their proposed scheme achieves mutual authentication, anonymity, secure localization, resistance to replay and forgery attacks while at the same time ensuring data security. Our proposed approach focuses more on topological aspects and advocates a proactive scheme which identifies and protects critical nodes through backup installations. We believe that the aforementioned paper makes a good contribution which is complementary to our approach as the two address different aspects of security in IoT networks.

It is evident from a review of the state-of-the-art that few solutions focus on the resilience aspect of IoT networks. It is true that maximizing the network lifetime is important, but with the advent of new technologies, such as low power Wi-Fi and LoRaWAN, the energy consumption has been significantly reduced while range has been improved. Moreover, unlike traditional sensor networks which produced tiny amounts of data infrequently, IoT networks have gained spotlight as being enablers for multimedia communication [24]–[26] with high bandwidth usage and bulk traffic, especially in the context of industrial or security. The high throughput requirements will be further enforced for massive deployment of IoT in smart city scenarios in which the data carrying capacity of the network will become crucial. Towards this end, this paper fills the gap by contributing a solution which helps identify critical nodes in an IoT from the perspective of ensuring the protection of the data carrying capacity of the network by employing techniques such as installing backups at those locations etc. We modify and extend our previous solution of identifying critical nodes in SDNs [27] while leveraging the solution specifically for low power IoT networks.

III. PROSE–Proactive Resilience in IoT

We first present the motivation behind this contribution and show through simulation how eliminating critical nodes in an IoT ecosystem substantially impacts the data carrying capacity

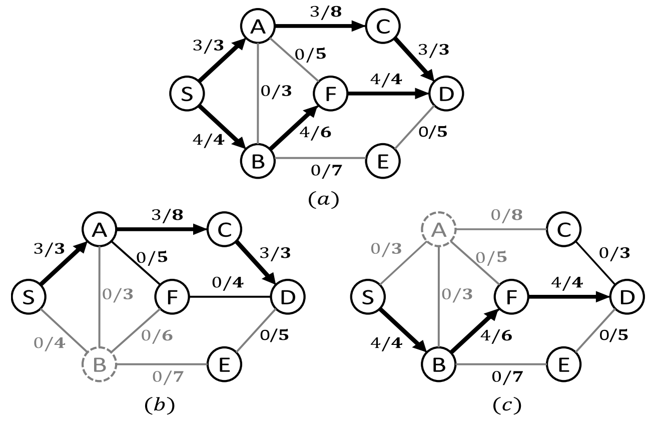


Fig. 2. Critical nodes in a network.

of the network as a whole as well as that of individual flows. Subsequently, we describe our link-centric interference model to capture interference in low power Wi-Fi IoT networks. Next, we mathematically formulate the problem with relevant constraints, and lastly, we devise a heuristic algorithm based on a utility function to efficiently solve large problem instances.

A. Motivation

We present our motivation by first illustrating the critical role that topological resilience plays in IoT networks. We begin with an exploration of the true nature of the problem of critical node elimination in IoT networks. The problem has been brought to light for sensor networks in several previous solutions [3], [4] which prove that an attack that targets critical nodes can impact network lifetime and delay significantly. However, it is arguable that while IoTs have some resemblance to sensor networks, but they have some inherent structural differences, such as the presence of Internet connected IoT gateways which poses unique challenges such as access to the Internet backbone, and different traffic patterns, especially in the context of multimedia, security and smart cities. Moreover, the extent of throughput degradation that critical node elimination in IoTs can cause remains to be investigated. In general, as the scale of IoT deployment is expanded, the role of topology becomes increasingly important.

Consider Figure 2, which shows maximum flow distribution over the network for a flow originating at node S and terminating at node D with an aggregate flow of 7 units. Assuming only a single node could be eliminated, node B is perhaps the one that can be eliminated to cause significant impact and reduce the flow to 3 units. By installing backup at node B, the aggregate flow rate can be maintained at 4 units as shown in the figure even if the critical node which is next in line according to importance, can be destroyed. We further motivate the research by carrying out a basic simulation based evaluation of the impact of critical node elimination in a sample 100 node IoT network. In order to explore the impact of the elimination of critical nodes on the data carrying capacity of the network, we carried out a simulation study for a low power Wi-Fi based IoT network with 100 nodes including IoT gateways, IoT relays, Coordinating Devices (CDs) along with some additional end devices. Figure 3(a) shows through traffic intensity map that traffic is unevenly distributed in the network and for more details, Figure 3(b) shows the traffic distribution over different nodes. We plot the reduction in the aggregate throughout along with the per-flow reduction in Figure 4 due to elimination of an increasing number of critical IoT nodes (gateways, relays or CDs). The nodes have been selected using brute force to find out the most critical nodes and they are taken out iteratively. As the figure shows, as increasing number of IoT nodes are eliminated (despite the fact that they are limited to a maximum of 5% of the total) the impact on the aggregate throughput performance is significantly impacted. Thus, we have illustrated that an adversary attack in which the most critical nodes are targeted in an IoT network, can substantially reduce the aggregate throughput of the network, thereby providing concrete motivation. Also, as discussed in Section II, while a number of solutions address cryptographic and physical security aspects, the particular concept of proactively introducing resilience in the topology of IoT network is the cornerstone of our motivation which may be used in addition to the solutions outlined previously.

B. Background and Terminology

The generic form of the identification (and subsequent protection) of critical nodes can be modeled as following:

$$\underset{x \in X}{max}\ \underset{y \in Y}{min}\ c(x)^T y \tag{1}$$

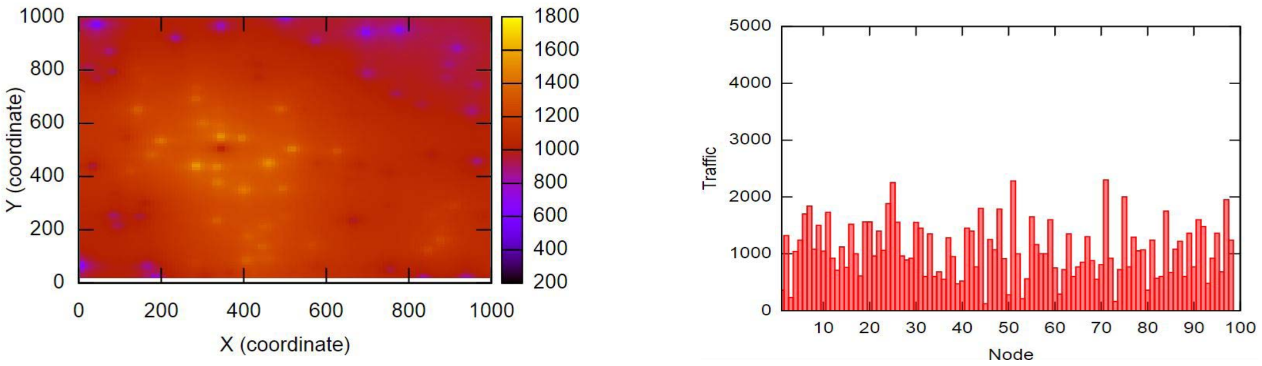
$$\text{subject to: } Ay \leq r(x) \tag{2}$$

$$y \geq 0 \tag{3}$$

where $x \in X$ is the attack variable i.e. the decision variable determining whether the given nodes are eliminated or not, and $y \in Y$ is flow variable for network operator who can use this to identify critical nodes. The first constraint represents limitations on the use of resources $r(x)$, representing limited resource(s) such as the total number of nodes that can be protected (e.g. by installing backups). The attack solution space can be formally defined as: $X \overset{def}{=} \{x : \sum_{(i,j)} c_i x_i \leq B, x_i \in \{0, 1\}\}$ where c_i is the cost to incapacitate node i and B is the total budget to eliminate nodes. Here, we would like to stress that eventually, it is not possible for an attack to eliminate all nodes and similarly, it is not possible for the network operator to install backups at all IoT node locations.

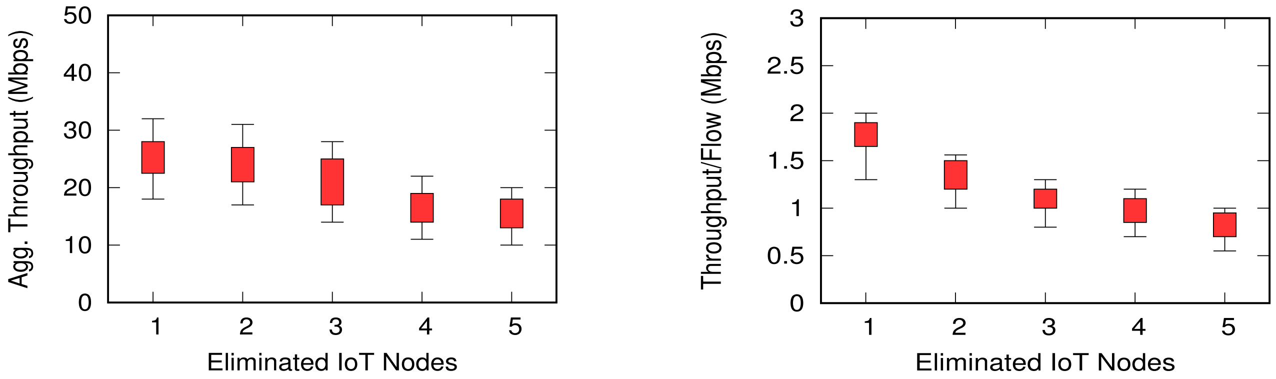
It is pertinent to elaborate that any particular protocol used for IoT will introduce its own peculiar vulnerabilities. In this paper, the motivation is to propose a generic solution without being tied to any particular protocol since the proposed approach is more of a topological approach rather than protocol approach. Further, in truly distributed environments, an adversary is very unlikely to be able to gather complete information (which is simpler in centralized systems with centralized repositories), but our motivation is to provide a lower bound on the achievable performance by employing the proposed resilience approach even in the unlikely event of an adversary somehow having omni knowledge about the network.

The IoT network is modeled as a directed graph $G = (N, A)$ where $n \in N$ represents the set of $|N|$ IoT backbone nodes (IoT gateways, IoT relays and CDs). The directed arc $(i, j) \in A$ represents a directional link between nodes i and j, $\psi(i, j)$ represents the capacity of directional



(a) (b)

Fig. 3. Uneven traffic distribution in the IoT network. (a) Traffic intensity plot. (b) Traffic distribution plot.



(a) (b)

Fig. 4. Impact of elimination of strategic IoT nodes. (a) Aggregate throughput reduction. (b) Per flow impact.

link (i, j) with $\psi_{(i,j)} \neq \psi_{(j,i)}$. The symbol $\mathbb{F}(i)$ of a node i is defined as the set: $\mathbb{F}(i) = \{(i, j) \in A :$ link (i, j) is an outgoing link at $i\}$. The *Reverse Set* of a node i is defined as the set: $\mathbb{R}(i) = \{(j, i) \in A :$ link (j, i) is an incoming link to node $i\}$.

We assume a multi-flow IoT network with multiple flows between different source-destination pairs in the network. In IoT networks, the bulk of traffic travels from the end devices across CDs, relays and gateways towards the cloud. Let $i \in S$ be the set of source nodes, while $j \in T$ be the set of destination nodes whereas $d_k \in D$ represents the set of demands for a set of different flows $k \in K$ in the network. The key point is that the network operator proactively installs backups in the network by perceiving in advance the key nodes which are the key positions for an attack. Since the network operator cannot install backups or protect all IoT nodes, therefore let B be the maximum number of backups that can be installed by the network operator. Let c_i be the cost of eliminating node i, then the solution space of the network operator is specified by:

$$X = \left\{x : \sum_{i \in N} c_i x_i \leq B, x_i \in \{0, 1\}\right\}$$

The decision variable x_i determines whether node i is eliminated or not. The decision variable x_i is defined as: $x_i = \{0 :$ node i is not eliminated, $1 :$ node i is eliminated$\}$.

C. Interference

Traditionally, ZigBee and related IEEE 802.15.4 protocols have been popular as the communication technology for IoT. While Wi-Fi had tremendous success for Wireless Local Area Networks (WLANs), but due to high energy consumption, its use has been limited to sensor and IoT networks. However, recently [28], [29] power-efficient Wi-Fi hardware have emerged as an alternative. Low power Wi-Fi offers years of battery life with seamless connectivity to existing IP infrastructure, which is a big selling point for IoT. Low power Wi-Fi comes in several flavors, including some supporting the high data rates of IEEE 802.11n [30] although with slightly higher energy consumption. Traffic patterns in IoT are different from traditional sensor networks since IoTs in smart cities produce significantly more data, more frequently. Therefore, low power Wi-Fi is perfectly suited to IoT. In low power Wi-Fi based IoT networks, due to the shared medium, the *Carrier Sensing Multiple Access* mechanism does not allow simultaneous transmissions since they result in collisions. Therefore, to achieve realistic results, we integrate interference constraints. To determine maximal cliques in the network, we employ a "*link-centric*" concept where the set of all the links within two hops of a given link are considered part of the maximal clique. Figure 5 shows the interference region of link (i, j) in a sample graph. Typically, the carrier sensing range is about twice the transmission range and links in this range mutually interfere, corresponding to a conflict graph, which models the links as nodes. In the conflict graph, links between nodes represent interference. Let $\mathbb{N}(i)$ be the set of neighbors of node i and let $\mathbb{S}(i) = \mathbb{R}(i) \cup \mathbb{F}(i)$ be the set of all incoming and outgoing links of node i, then for a

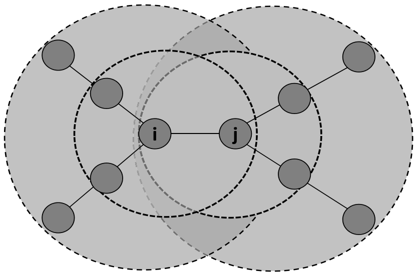


Fig. 5. Two hop interference neighborhood.

given link (i, j), the set of links in the maximal clique, $C_{(i,j)}$, is defined as:

$$\mathcal{C}_{(i,j)} = \bigcup_{m\in\mathbb{N}(i)} \mathbb{S}(m) \cup \bigcup_{n\in\mathbb{N}(j)} \mathbb{S}(n) \tag{4}$$

In order to integrate the impact of interference on the achievable throughput, the following constraint is devised:

$$\sum_{k\in K} \sum_{(i,j)\in\mathcal{C}_{(i,j)}} f_k^{(i,j)} \leq BW \quad \forall (i,j) \in A \tag{5}$$

where BW is the capacity of the clique and is typically considered to be equal to the channel capacity multiplied with a constant factor $0 \leq \sigma < 1$ (typically 0.45) to account for the possible MAC overheads [31] in communication.

D. Problem Formulation

We formally define the Critical Node Protection (CNOP) problem as follows:

$$\max_{\upsilon\in V,\ x\in X} \sum_{k\in K} d_k$$

$$\begin{aligned}
\text{subject to: } & \sum_{(i,j)\in\mathbb{F}(i)} f_{(k)}^{i,j} - \sum_{(j,i)\in\mathbb{R}(i)} f_{(k)}^{j,i} = d_k \\
& \forall i \in S, k \in K && (6)\\
& \sum_{(i,j)\in\mathbb{F}(i)} f_{(k)}^{i,j} - \sum_{(j,i)\in\mathbb{R}(i)} f_{(k)}^{j,i} = 0 \\
& \forall i \in N \setminus \{S, T\},\ k \in K && (7)\\
& \sum_{(i,j)\in\mathbb{F}(i)} f_{(k)}^{i,j} - \sum_{(j,i)\in\mathbb{R}(i)} f_{(k)}^{j,i} = -d_k \\
& \forall i \in T, k \in K && (8)\\
& \sum_{k\in K} \sum_{(i,j)\in\mathcal{C}_{(i,j)}} f_k^{(i,j)} \leq BW \quad \forall (i,j) \in A && (9)\\
& \sum_{k\in K} f_{(k)}^{i,j} \leq \psi(i,j)(1 - x_i) \\
& \forall (i,j) \in \mathbb{F}(i)i,\ j \notin \{S, T\} && (10)\\
& \sum_{k\in K} f_{(k)}^{i,j} \leq \psi(j,i)(1 - x_i) \\
& \forall (j,i) \in \mathbb{R}(i)j,\ i \notin \{S, T\} && (11)\\
& x_i = 1 - \upsilon_i \quad \forall i \in N && (12)\\
& \sum_{i\in N} x_i \leq B && (13)\\
& \sum_{i\in N} \upsilon_i \leq B && (14)\\
& x_i,\ \upsilon_i \in \{0, 1\} \quad \forall i \in N \\
& f_{(k)}^{i,j},\ \psi(i,j) \geq 0 \quad \forall (i,j) \in A \\
& d_k \geq 0 \quad \forall k \in K
\end{aligned}$$

Algorithm 1 Heuristic Algorithm to Identify Critical Nodes

```
procedure HEURISTIC
    Relax CNOP by removing integer constraint
    Solve the weakened CNOP
    for each node $i \in N$ do
        $\Phi(i) = \dfrac{\sum_{k\in K} \sum_{(i,j)\in\mathbb{F}(i)} f_{(k)}^{i,j}}{\sum_{\Phi(j)\in\Phi} \Phi(j)}$
    end for
    Sort nodes in decreasing order of $\Phi(i)$
    while each node $i \in$ among the first $B$ nodes in $N$ do
        Set $\upsilon_i = 1$
    end while
    Solve the complete Critical Node Protection problem
end procedure
```

The objective function is a simplification (single-level equivalent) of a multilevel optimization problem such that at the internal level, an attacker eliminates B nodes with the stipulation that the variable $\upsilon \in V$ represents the nodes that the upper level problem has selected for installing backups and therefore cannot be eliminated. The attack eliminates nodes (i.e. $x = 1$) other than those for which $\upsilon = 1$ with the aim of minimizing flow and then the upper level optimization problem attempts to maximize the aggregate network flow. Constraints (6-8) represent flow conservation constraints for the IoT network with the assumption that it predominantly comprises of traffic towards the IoT cloud. Constraint (9) captures the interference constraint for the wireless medium. Constraints (10-11) ensure that if a node has been eliminated, then it has zero flow across it. Constraint (12) ensures mutual exclusion of the variables x_i and υ_i in the sense that if a node has been selected to be protected by installing backups for instance, then it cannot be eliminated. Constraints (13-14) ensure that both the number of backups and the number of eventual nodes that can be eliminated are limited to B (although this stipulation can be relaxed to arbitrary numbers). Overall, the model identifies strategic nodes which play the most important role in the data carrying network capacity.

E. Heuristic Algorithm

Mixed Integer Linear Programming problems are notoriously hard to solve and while a formal proof is not provide, but they are generally NP-Hard. To provide a tractable solution, we devise a heuristic based greedy algorithm which efficiently solves the problem with approximate results. We adopt the approach of calculating the greedy heuristic for all network nodes. The greedy heuristic $\Phi(i)$ of a node i measures the utility of node i which is basically a measure of the amount of flow passing across the node in comparison to aggregate network traffic and is defined as:

$$\Phi(i) = \frac{\sum_{k\in K} \sum_{(i,j)\in\mathbb{F}(i)} f_{(k)}^{i,j}}{\sum_{\Phi(j)\in\Phi} \Phi(j)} \tag{15}$$

In order to find the heuristic, we need to first find out the flow distribution under the optimal conditions. This can

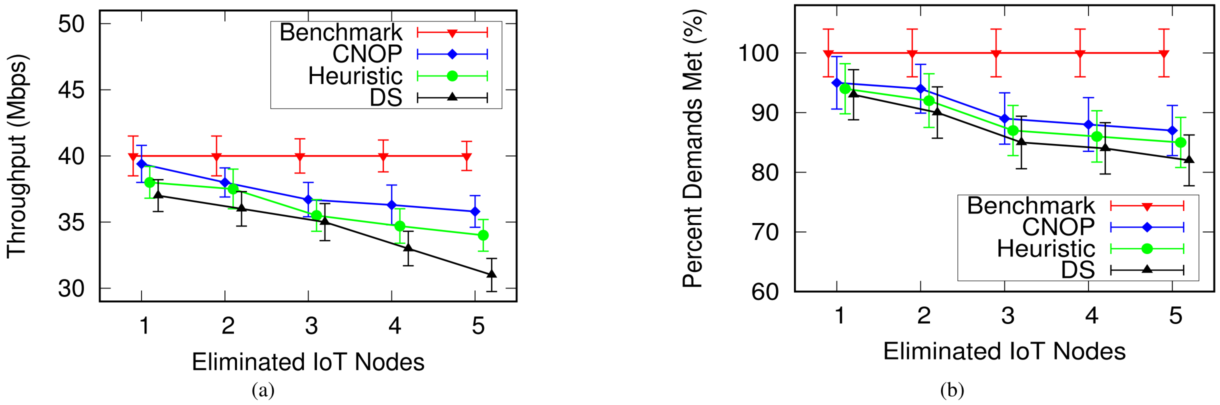


Fig. 6. Impact of elimination of strategic IoT nodes. (a) Aggregate throughput reduction. (b) Per flow percentage satisfied.

TABLE I

SIMULATION PARAMETER

Parameters	Values
Simulation time	1000s
Dimension	2000m x 1000m
Transport Layer Protocol	UDP
IoT Devices	100
Traffic Demand	10-50 Mbps
Packet size	1000 B
Traffic type	CBR
Eliminated Nodes	1-5
Wireless Technology	G2M5477 (Low Power Wi-Fi)
Power Consumption	90 mW (Wi-Fi active)

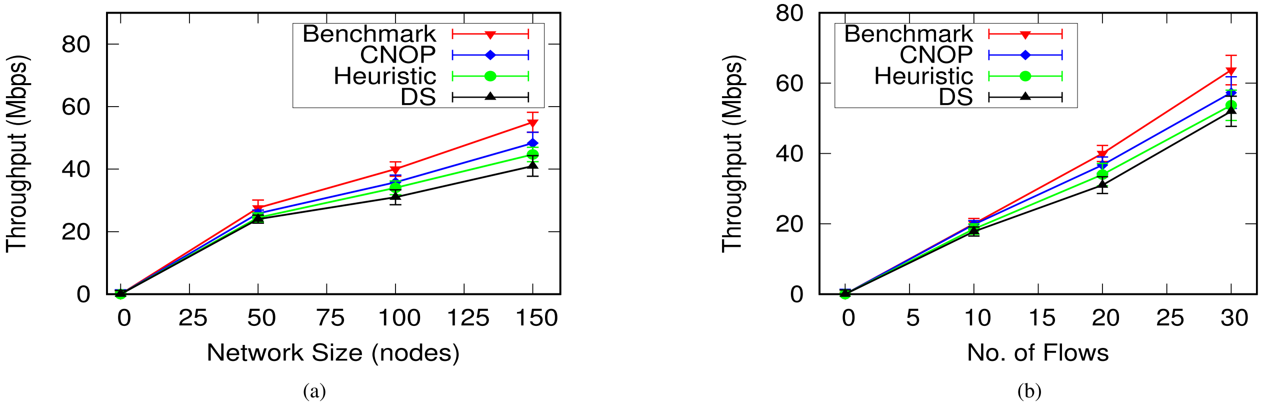
be achieved by “weakening” the MILP formulation which basically involves removing the integer constraints i.e. the integer variables. We achieve this temporary state by setting both x and υ to 0 for now. The resulting weakened formulation is solved and the greedy heuristic is calculated for each node based on the resultant flow distribution. By utilizing the greedy heuristic, the problem becomes tractable and can be solved in polynomial time even for large problem instances.

IV. Performance Evaluation

In this section, we discuss implementation details for the proposed solutions along with other existing solutions in the area. We use network simulator to simulate the network, while Java is used to create the optimization model by generating objective and constraints which are then passed on to the IBM CPLEX studio and the resulting values are subsequently passed on to the simulator which models the wireless channel for the IoT network. The simulation parameters are detailed in Table I. We implement four solutions to showcase the contribution of this paper. First, we have the Critical Node Protection (CNOP) problem which employs a sequential algorithm to iteratively identify the key critical node positions, the second solution is the Heuristic solution which employs the greedy utility function to efficiently identify the critical positions, the third [2] is a closely related solution in which authors propose installing backups at critical nodes in sensor networks based on the Dominating Set (DS) concept. It is otherwise an efficient solution, but does not capture the importance of network capacity since it is more focused on optimizing connectivity and the final solution is the Benchmark solution in which we calculate the maximum flow distribution (based on the MILP without the node elimination constraints) to gauge the performance of the network without elimination of nodes.

It is pertinent to mention that typically sensor devices have limited data rate, but as discussed previously, ultra-lower power Wi-Fi modules have made it possible to sustain much higher data rates at a fraction of battery usage. The lower-power Wi-Fi module G2M5477 mentioned in Table I (Simulation parameters) can provide throughputs of a few Mbps with very low battery consumption.

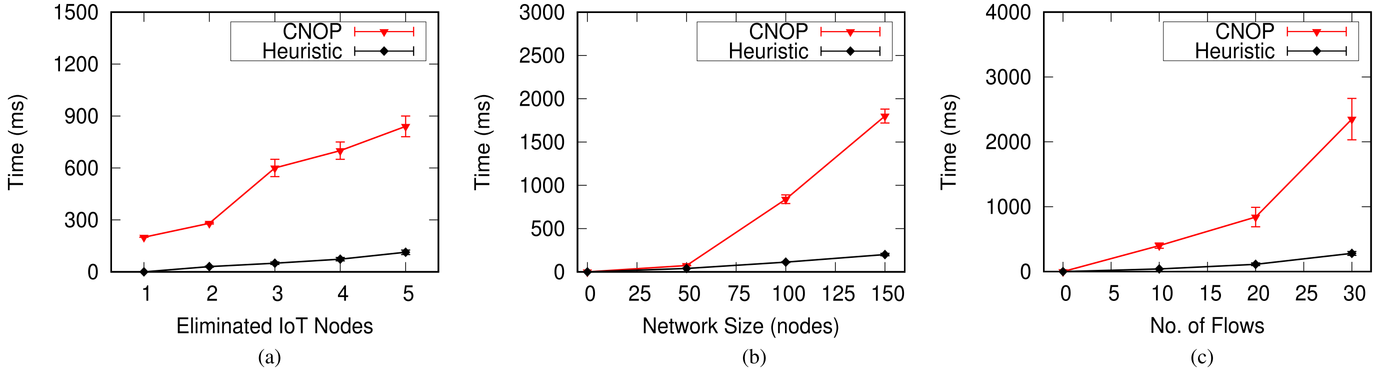
We first carry out the performance evaluation of the proposed scheme along with other schemes by varying the number of eliminated IoT nodes (with an equal number of backup installations) and study its impact on the aggregate throughput of the network and the percent of demand satisfied for each individual flow. Figure 6(a) shows the decrease in the aggregate throughput of the network as IoT node elimination is carried out ranging from 1-5 nodes. The “Benchmark” solution shows initial throughput without any impact, while for CNOP, Heuristic and DS represent the results for the other solutions. Both CNOP and Heuristic perform better than DS, although the performance difference between the greedy heuristic solution and the Dominating Set is small. Although DS is an elegant solution, but it focuses on topological aspects, and does not take into consideration the impact on aggregate throughput, therefore, it performs sub-optimally in contrast to CNOP which selects optimal nodes for backup based on mathematically calculated optimal positions. The greedy heuristic solution performs reasonably close to the optimal solution for all the cases, with a very close performance to optimal result for two nodes reading. In 6(b), the percent demands met for the four solutions is depicted. As the results show, CNOP meets the highest percent of per-flow demands followed by the greedy heuristic and then DS. The results show a very similar pattern to the aggregate throughput, while reinforcing the fact that the aggregate throughput impact is proportionately reflected in per-flow throughput reduction which was important to show as aggregate throughput results sometimes may not reflect uneven per-flow reduction. In 7(a), we fix the number of selected nodes for failure and backup to be equal to be 5 and vary the network size to study the performance of the four solutions when the network is scaled



(a)

(b)

Fig. 7. Impact of varying network size and flows. (a) Throughput reduction vs. network size. (b) Throughput vs. no. of flows.



(a)

(b)

(c)

Fig. 8. Time consumed vs. flows. (a) Time vs eliminated nodes. (b) Time vs network size. (c) Time vs flows.

to a larger size. As the graph depicts, the overall performance keeps the same trend as before and CNOP leads the performance due to its precise mechanism of selecting optimal backup positions followed by Heuristic and DS. However, the performance difference between Heuristic and DS is less pronounced as we have larger number of nodes which makes approximation less optimal. In 7(b), we vary the number of flows to see the impact on performance for larger number of flows. AS the results depict, CNOP again performs the best followed by Heuristic and DS.

Another important statistic which we need to evaluate is the computation time required by the exact MILP solution i.e. CNOP and the heuristic approximation. In 8, we show the time computation for varying number of eliminated nodes, network size and the number of flows. As the results depict for all three scenarios, the time consumed by the greedy solution increases exponentially as the network size, number of flows, or the number of eliminated nodes increase. This illustrates the fact that while the exact solution (CNOP) provides optimal result, but is computationally expensive, making the solution intractable for large problem instances. Moreover, since the underlying optimization problem may need to be solved repeatedly, therefore, an approximate solution is quite useful.

Finally, 9 shows the percentage cumulative distribution of links based on maximum end-to-end network delay. The figure evaluates what impact if any, does eliminating critical nodes cause on the IoT network. As shown, CNOP minimizes the maximum end-to-end delay compared to the other schemes, followed by the heuristic solution and the DS scheme.

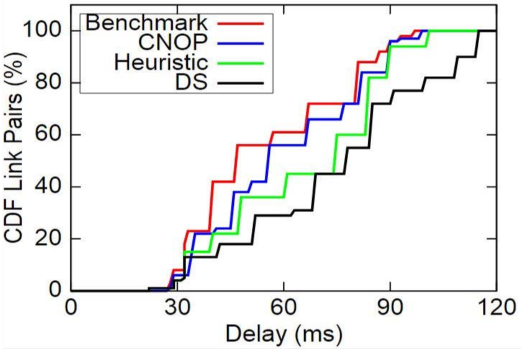


Fig. 9. CDF of end-to-end delays for links.

V. Conclusion

Internet of Things has become one of the most dominant technologies with tremendous applications worldwide. Their extraordinary utility also exposes their vulnerabilities to numerous threats and a large attack surface since the network is inherently very distributed. The state-of-the-art in security for IoT focuses more on cryptographic aspects, while inbuilt network resilience against node elimination attacks has been ignored. Resilience solutions exist for sensor networks, but their main concern is energy saving, which may not be the primary goal of certain IoT networks which support high bandwidth or multimedia applications using low power Wi-Fi. For these networks, protecting the data carrying capability of the network is important and towards this end, this paper explores a protective resilience solution in which optimal mathematical and heuristic algorithms are devised to identify the critical set of nodes ideal candidates for installing backups. Performance comparison with existing solutions show substantial performance improvement by the proposed solutions. For future, an interesting theme of is to explore a solution which jointly optimizes both energy and data carrying capacity of the network by using an multi-objective optimization approach.

References

[1] C.-P. Chen, S. C. Mukhopadhyay, C.-L. Chuang, M.-Y. Liu, and J.-A. Jiang, "Efficient coverage and connectivity preservation with load balance for wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 1, pp. 48–62, Jan. 2015.

[2] O. Dagdeviren, V. K. Akram, B. Tavli, H. U. Yildiz, and C. Atilgan, "Distributed detection of critical nodes in wireless sensor networks using connected dominating set," in *Proc. IEEE SENSORS*, Oct./Nov. 2016, pp. 1–3.

[3] A. Yuksel, E. Uzun, and B. Tavli, "The impact of elimination of the most critical node on wireless sensor network lifetime," in *Proc. IEEE SAS*, Apr. 2015, pp. 1–5.

[4] H. U. Yildiz, B. Tavli, B. O. Kahjogh, and E. Dogdu, "The impact of incapacitation of multiple critical sensor nodes on wireless sensor network lifetime," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 306–309, Jun. 2017.

[5] S. M. A. Oteafy and H. S. Hassanein, "Component-based wireless sensor networks: A dynamic paradigm for synergetic and resilient architectures," in *Proc. IEEE LCN*, Oct. 2013, pp. 735–738.

[6] S. M. A. Oteafy and H. S. Hassanein, "Resilient IoT architectures over dynamic sensor networks with adaptive components," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 474–483, Apr. 2017.

[7] M. Gusev, S. Ristov, R. Prodan, M. Dzanko, and I. Bilic, "Resilient IoT eHealth solutions in case of disasters," in *Proc. 9th Int. Workshop Resilient Netw. Design Modeling (RNDM)*, Sep. 2017, pp. 1–7.

[8] X. Han, X. Cao, E. L. Lloyd, and C.-C. Shen, "Fault-tolerant relay node placement in heterogeneous wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 5, pp. 643–656, May 2010.

[9] M. M. Rana, "Attack resilient wireless sensor networks for smart electric vehicles," *IEEE Sensors Lett.*, vol. 1, no. 2, Apr. 2017, Art. no. 5500204.

[10] M. Kamruzzaman, N. I. Sarkar, J. Gutierrez, and S. K. Ray, "A study of IoT-based post-disaster management," in *Proc. IEEE ICOIN*, Jan. 2017, pp. 406–410.

[11] B. O. Kahjogh, I. Demirkol, D. Careglio, and J. D. Pascual, "The impact of critical node elimination on the latency of wireless sensor networks," in *Proc. ICUFN*, Jul. 2017, pp. 182–187.

[12] P. Gope, J. Lee, and T. Q. S. Quek, "Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks," *IEEE Sensors J.*, vol. 17, no. 2, pp. 498–503, Jan. 2016.

[13] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for Internet of things," in *Proc. IEEE ISNE*, May 2014, pp. 1–2.

[14] X. Yao, X. Han, X. Du, and X. Zhou, "A lightweight multicast authentication mechanism for small scale IoT applications," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3693–3701, Oct. 2013.

[15] Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, "A trust-based resilient routing mechanism for the Internet of Things," in *Proc. ACM Conf. ARES*, 2017, Art. no. 27.

[16] R. Niati, N. Yazdani, and M. Nourani, "Deployment of spare nodes in wireless sensor networks," in *Proc. IEEE Conf. IFIP*, Apr. 2006, p. 5.

[17] P. Singh and A. S. Buttar, "Spare node deployment approach for the improvement of the lifetime of wireless sensor networks," *Int. J. Adv. Res. Comput. Sci.*, vol. 5, no. 6, pp. 95–99, 2014.

[18] B. A. Bakr and L. T. Lilien, "Extending lifetime of wireless sensor networks by management of spare nodes," *Procedia Comput. Sci.*, vol. 34, pp. 493–498, Dec. 2014.

[19] M. J. Handy, M. Haase, and D. Timmermann, "Low energy adaptive clustering hierarchy with deterministic cluster-head selection," in *Proc. IEEE Int. Workshop Mobile Wireless Commun. Netw.*, Sep. 2002, pp. 368–372.

[20] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1327–1340, Oct. 2017.

[21] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2831–2843, Nov. 2018.

[22] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2846299.

[23] P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[24] O. Said, Y. Albagory, M. Nofal, and F. Al Raddady, "IoT-RTP and IoT-RTCP: Adaptive protocols for multimedia transmission over Internet of things environments," *IEEE Access*, vol. 5, pp. 16757–16773, 2017.

[25] W. Jiang and L. Meng, "Design of real time multimedia platform and protocol to the Internet of Things," in *Proc. IEEE TrustCom*, Jun. 2012, pp. 1805–1810.

[26] W. Wang, Q. Wang, and K. Sohraby, "Multimedia sensing as a service (MSaaS): Exploring resource saving potentials of at cloud-edge IoT and fogs," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 487–495, Apr. 2017.

[27] U. Ashraf and C. Yuen, "Capacity-aware topology resilience in software-defined networks," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2017.2726680.

[28] S. Tozlu, M. Senel, W. Mao, and A. Keshavarzian, "Wi-Fi enabled sensors for Internet of things: A practical approach," *IEEE Commun. Mag.*, vol. 50, no. 6, pp. 134–143, Jun. 2012.

[29] *G2m5477 Preliminary Datasheet*, G2 Microsyst., Oakland, CA, USA, May 2009.

[30] *Gs1500m Product Brief—Preliminary*, GainSpan Corp., San Jose, CA, USA, Apr. 2012. [Online]. Available: http://www.gainspan.com

[31] X. Cheng, P. Mohapatra, S.-J. Lee, and S. Banerjee, "MARIA: Interference-aware admission control and QoS routing in wireless mesh networks," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 2865–2870.

Usman Ashraf received the B.S. degree in computer science from FAST Lahore in 2003 and the M.S. and Ph.D. degrees in computer networks from INSA Toulouse, France, in 2006 and 2010, respectively. He was an Assistant Professor and the Director of the Network Research Laboratory, Air University, Islamabad. He is currently with the College of Computer Sciences and Information Technology, King Faisal University. He has more than seven years of teaching and research experience. He is involved in several consultancy projects with the industry related to computer networks, Internet of Things, blockchain, and cybersecurity. He has several publications in prestigious international journals, including the IEEE COMMUNICATIONS LETTERS and the IEEE TRANSACTIONS ON MOBILE COMPUTING.