Analysis of Temporal Robustness in Massive Machine Type Communications

Debjani Goswami®, Merim Dzaferagic®, Harun Siljak®, Senior Member, IEEE, Suvra Sekhar Das, and Nicola Marchetti®, Senior Member, IEEE

Abstract—The evolution of fifth-generation (5G) networks needs to support the latest use cases, which demand robust network connectivity for the collaborative performance of the network agents, such as multirobot systems and vehicle-to-anything (V2X) communication. Unfortunately, the user device’s limited communication range and battery constraint confirm the unfitness of known robustness metrics suggested for fixed networks, when applied to time-switching communication graphs. Furthermore, the calculation of most of the existing robustness metrics involves nondeterministic polynomial (NP)-time complexity, and hence are best fitted only for small networks. Despite a large volume of works, the complete analysis of a low-complexity temporal robustness metric for a communication network is absent in the literature, and the present work aims to fill this gap. More in detail, our work provides a stochastic analysis of network robustness for a massive machine-type communication (mMTC) network. The numerical investigation corroborates the exactness of the proposed analytical framework for the temporal robustness metric. Along with studying the impact on network robustness of various system parameters, such as cluster head (CH) probability, power threshold value, network size, and node failure probability, we justify the observed trend of numerical results probabilistically.

Index Terms—Base station (BS), cluster head (CH), connectivity robustness, constrained devices, massive Machine Type Communications (mMTCs), non-CH (NCH).

I. INTRODUCTION

Due to the fast pace of technological advancement, current fifth-generation (5G) systems need to support various brand-new network service requirements. In this context, the international telecommunication union (ITU) has categorized all 5G use cases into three broad service classes, i.e., enhanced mobile broadband (eMBB), ultrareliable low latency communication (URLLC), and massive machine type communication (mMTC) [1]. The use of multiple antennas at both the transmitter and receiver sides, densifying networks with many small base stations (BSs), and exploiting nonorthogonality in the access scheme [2], are identified as the forefront techniques to boost the spectral efficiency (SE) in 5G systems. Along with the three-fold SE requirement compared to 4G (eMBB service requirement), 5G also needs to support one million connections per square kilometer for the mMTC use case. Moreover, URLLC applications demand a 99.999% reliability for transferring information within a 1 millisecond (ms) user plane latency. Two of the services mentioned above, i.e., URLLC and mMTC, exploit the Internet of Things (IoT) networks formed by a group of wirelessly interconnected MTC devices (MTCDs). The small battery constraints of sensor nodes necessitate energy-efficient communication for the IoT use cases as the wireless sensor nodes act as MTCDs. Furthermore, many diverse application scenarios of 5G systems, e.g., multirobot systems [3], unmanned aerial vehicles (UAVs) [4], on-road-sensor networks (ORSNs) [5], air transportation system [6], smart grids, vehicular networks, all require a robust network to exploit the collaborative performance of sensor nodes. In this context, to enhance the connection robustness, 3GPP Rel 13 [7] has introduced the concept of dual connectivity that allows a single user to access two serving nodes or cell groups simultaneously.

The URLLC and mMTC service classes will soon agglomerate into critical mMTC (eMTC) services with important use cases, such as wide-area disaster monitoring, wireless factory automation, etc., for beyond 5G networks [8]. The white paper on critical and mMTC toward sixth generation (6G) [9] confirms the requirement for ultrareliable wireless communications and massive connectivity availability for cMTC services [10]. Moreover, many new application areas, such as augmented and virtual reality, future industrial communication and control, haptics, robotics, autonomous vehicles, automated guided vehicles, UAVs, and tactile Internet in large factory networks, require robust network infrastructure to ensure reliable collaborative performance among the network agents [8], [11]. Besides the use cases mentioned above, robust wireless connectivity is equally crucial for different mMTC applications in smart cities also. More in detail, to enable efficient exchange of messages among different components of the systems, multiple smart city use cases, like, intelligent traffic light control, smart energy services, structural health monitoring, real-time monitoring of water networks, bridges,
tunnels, trains, subway rails, oil and gas pipelines, and environmental monitoring, require reliable and robust communication infrastructures [12]. Among all the mMTC use cases described above, multiple application scenarios, such as autonomous vehicles, automated guided vehicles, UAVs, etc. exhibit temporal variations in the network topology. Unlike the infrastructure network, the limited transmission range caused by the low transmitted power of sensor nodes limits the link connectivity in the communication network. Moreover, the random fading effect and the high mobility in vehicular networks results in communication link variation over both the nodes and time instants. Furthermore, as sensor nodes are operated automatically without human intervention, a frequent recharge of battery or replacement is difficult for sensor node-assisted applications. Consequently, a fast battery draining and physical damage in sensor nodes introduce random node failure, thereby significantly hampering networks’ standard operation. These fundamental causes of network disruption raise the gateway failure robustness requirement for mMTC [13], and the need for mobility robustness in the vehicle to anything (V2X) services [14] in 5G systems. Additionally, due to the recent paradigm shift from centralized to distributed, the robustness metric significantly evaluates any distributed algorithm’s efficiency. For example, achieving a standard time scale within the network agents for exploiting the best benefit from the SE boosting techniques, requires a robust distributed timing synchronization solution for large networks [15]. The discussion above sheds light on the fact that irrespective of the service classes of 5G systems, robustness is one of the most desirable features for any communication network. In particular, the robustness metric captures the ability of a network to continue the normal operations in the presence of various disruptions and challenges. Although network robustness has gained extensive research attention in the last two decades, the above-mentioned new application scenarios and their unique service requirements necessitate a reinvestigation of this domain. Hence, we now turn to discuss the motivation of our work in the context of existing network robustness metrics and their limitations in communication networks.

The earliest works exploit graph topology for quantifying the network robustness, namely, the vertex (edge) connectivity [16], heterogeneity [17], clustering coefficient [18], closeness [19], betweenness [19], diameter [20], algebraic connectivity [21], network criticality [22], effective graph resistance [23], number of spanning trees [24], largest subgraph [25], etc. Later works introduce some advanced metrics of network robustness, such as toughness [26], scattering number [27], and tenacity [28], which quantify both the cost of damage and the degree of impairment in networks [29]. Unfortunately, as mentioned earlier, most of the existing robustness metric exhibit a nondeterministic polynomial (NP)-complete complexity, limiting the application of these metrics for large networks. Furthermore, the vertex or edge connectivity only partly reflects the disruption-withstanding capability of a network. Moreover, the algebraic connectivity for all disconnected graphs is zero [30]. The above limitations restrict the application of these metrics in many real networks. Furthermore, all the metrics above are suggested for fixed infrastructure networks, like the Internet. However, due to the random topology changes caused by fading, mobility, and energy constraints, the robustness analysis becomes challenging [31] for communication networks, as the network becomes a dynamic entity, driving the search for a candidate temporal robustness metric for switching networks.

Scellato et al. [32] confirmed that the static approximation of temporal robustness greatly overestimates the robustness of a time-switching network. Their investigation exhibits considerable gap (≈166%) between the temporal robustness measure and its static representation for the node failure probability of 0.4, as shown in Fig. 1. Moreover, Scellato et al. [32] confirmed that the static approximation for time-varying mobile networks can indicate robustness to be high even if the network is fragile in nature. The discussion above confirms the unsuitability of the static approximation strategy in measuring the robustness of time-switching networks. The observation above motivates Scellato et al. [32] to present a Markov-based temporal network model while considering the effect of temporal variation in robustness analysis for the first time in mobile and opportunistic networks, where they express the temporal efficiency in the observation time interval $[t_1, t_2]$ as the mean inverse temporal distances expecting over all pairs of nodes. However, that work assumes the presence of a complete graph, where each pair of distinct vertices is connected by a unique edge, which is not always ensured, especially in large networks. Unlike the Erdős–Rényi random graph model for the fixed network, which confirms the existence of some critical node failure probability beyond which a system breaks completely, the work in [32] demonstrates the smooth failure of a random model with the increase in the fraction of failing nodes when associated with the temporal variation. Therefore, an inaccurate static approximation and the smooth degradation in the network robustness aspect, make the temporal robustness metric different from the static measures of robustness. Later on, the same authors of [32] extend their work in [33], where they define a novel temporal robustness metric to measure the degree of network disruption due to different attacking strategies. This work confirms that intelligent attacks have a more substantial influence on temporal connectivity than random attacks in the networks. Motivated by the
fact above, a semi-supervised spatio-temporal deep learning-based intrusion detection scheme is proposed in [34]. Sano and Berton [35] investigated the temporal robustness metric for an air transport network, where they confirm that although the temporal variation cannot affect the traditional giant component [25], it has a more substantial effect on efficiency as described in [36]. Moreover, the authors report that the attacks based on the betweenness significantly degrade the temporal efficiency, or in other words, damage the network most. In the initial stage of the investigation, the temporal robustness evaluation follows the splitting of time switching graphs into a collection of static graphs, each for a single time instance and analyzing them one by one to produce the final result. A fast algorithm to evaluate the temporal robustness exploiting a single-stage computation is suggested by [37], thereby experiencing a lower time complexity than the previous approach. Feng et al. [38] applied temporal network theory for investigating the temporal features of railway transportation service networks, confirming the heterogeneous influence of different failing edges in the network. The work in [39] defines the temporal robustness metric as the ratio between the average degree of nodes after and before the network disruption. In the recent investigation in [40], the authors exploit various graphs to model the IoT network and provide the theoretical foundations of network criticality as a function of different network parameters. Although most of the works mentioned above come up with some foremost insights, none of the works described in [36], [37], [38], [39], and [40] consider the impact of transmission range although it has a significant influence on how well a network can combat disruption. Although [41] addresses the effect of random node distribution and node transmission range on network robustness in wireless sensor networks (WSNs) numerically, the mathematical analysis is beyond the scope of that work.

The work [42] follows temporal efficiency definition of [32] to study the response of spatio-temporal networks to random errors and systematic attacks, where the authors considered the noninstantaneous interaction between nodes based on the space where they are positioned. In addition, the below section mentions some major aspects overlooked by most of the prior works, which are essential in controlling the network robustness [43]. First, in real-networks, disruption may disable a link for a while, after which it may reappear. In addition, due to the continuous change in network connectivity, the failure duration plays a crucial role in determining the network’s robustness. The significant influence of the factors above on network vulnerability encourages [43] to develop a new survivability framework for time-varying networks. In particular, to evaluate the robustness of time-varying networks, the work in [43] proposes two metrics, namely, MinCut and MaxFlow. To deal with the NP-hardness of both metrics, the authors develop a greedy algorithm for \( \delta \)-MAXFLOW and a min-weight algorithm for the \( \delta \)-MINCUT problem. The time complexity for both the algorithms is \( O(|c|^3) \), where \( |c| \) is the total number of temporal edges in the time-varying graph. Therefore, the application of these metrics experiences a large computational complexity in the case of massive-connected communication networks.

Next, we discuss the work in [40], where the authors evaluate the temporal robustness by measuring network criticality in Internet of Things (IoT) networks. By modeling the IoT networks as an \( r \)-nearest neighbor graph, the authors provide the theoretical analysis of network robustness and evaluate the effect of nearest neighbors and network size on this metric. More specifically, in this work, the authors model 1-D IoT topology as an \( r \)-nearest neighbor cycle, where each node is connected to \( 2r \) nodes. However, in the case of 2-D 1-nearest neighbor torus network, they assume the presence of four neighbors for each node. Note that although the above configuration is well suited for wired networks, ensuring this setup is challenging for wireless network connection. Moreover, the spatial invariant torus lattice structure is not well-fitted for multiple 5G-mMTCs applications, like intelligent transportation systems (ITSs) [44], where many IoT devices are deployed in vehicles, thereby exhibiting both spatial and temporal variation. Unlike \( r \)-nearest neighbor networks, the random geometric graph is a spatial network, which allows the random placement of a node set in a confined area, where the threshold of transmission radius determines the network link connectivity, is therefore more suitable for modeling IoT networks.

The discussion above highlights the need for further research on the theoretical analysis of network robustness for random geometric graphs. A significant computational complexity in [43], the fixed network structure followed in [40], and the complete graph assumption in [32] make apparent the need for revisiting temporal robustness metric for massively connected network scenarios. Note that the massive connectivity requirement of mMTC and cMTC service classes rise the need for minimum signaling overhead-based energy-efficient transmission in the network. Clustering is an efficient technique that mitigates the congestion in evolved NodeB (eNB)’s access channel and ensures energy-efficient communication in mMTC networks. However, despite the large volume of works toward measuring network robustness, a detailed analysis of a suitable temporal robustness metric for a cluster-based communication network is still missing. The strong potential of cluster-based techniques in supporting the massive connectivity requirement, motivates us to investigate the network robustness of a cluster-based mMTC-network in this work. The contributions of our work can be summarized as follows.

1) We provide a stochastic analysis of the temporal robustness metric. Moreover, we validate the correctness of our numerical investigation measuring the temporal robustness metric, by comparing with a prior temporal robustness metric described in [39]. The good match of analytical and numerical analysis confirms the exactness of the derived analytical expression.

2) We investigate the behavior of network robustness versus different system parameters, i.e., cluster head (CH) probability and the number of nodes in the network for different values of power threshold. We repeat the investigation for a sparse network scenario and make some insightful observations on the parametric trends of temporal robustness. Moreover, the observed trends are justified in a probabilistic manner.
3) Unlike the other existing robustness metrics that experience NP-time complexity, our proposed metric has a complexity of $O(N^3)$ for the derived exact expression and $O(N^2)$ for its approximated form, making it suitable for large networks.

II. SYSTEM MODEL

The previous section confirms that a significant performance degradation caused by the limited communication range and tight energy constraint of sensor nodes in mMTC services necessitate gateway robustness in the mMTC network. Our work is motivated by the fact that the influence of these two aspects makes the robustness analysis challenging in mMTC networks. One possible way to mitigate the congestion in the eNB’s access channel [45] and exploiting the energy-efficient communication [46] is to group the MTCDs into smaller clusters. Motivated by that, we adopt the system model of a cluster-based mMTC network [47] to study the robustness of the network, as shown in Fig. 2.

In particular, this investigation considers a fixed network size of $N$ where we exclude the possibility of adding new nodes in the network. We assume that all $N$ nodes are uniformly distributed inside a square grid within the range $[-a, a]$, i.e., the area of the grid is $A = 4a^2$, and the density of the nodes is $\lambda = (N/A)$. Moreover, we assume the BS is placed in the center of the square grid (i.e., in the $(0, 0)$ coordinate). Fig. 2 depicts the grouping of MTCDs into multiple disjoint clusters, where each group consists of a single CH member and multiple noncluster head (NCH) members [as shown in Fig. 3(a)]. Moreover, CHs take charge of forwarding the data transmitted by the ordinary nodes in the network. To maximize the energy efficiency of the network, we prioritize the forwarding of NCH member’s data through any suitable CH. Failure to associate with all CHs allows a particular NCH to transmit its data directly to the BS. In this work, we assume that each node can participate in the CH election procedure and be elected as a CH or remain an NCH member with probabilities $p$ and $1-p$, respectively. Hence, the average number of CHs and NCHs for a network size of $N$ is equal to $\lfloor Np \rfloor$ and $(\lfloor N(1 − p) \rfloor)$, respectively, where $\lfloor x \rfloor$ indicates the floor function that captures the greatest integer less than or equal to $x$. We express the disruption of the network by random node removal, mainly caused by physical damage and the energy constraint of sensor nodes. More specifically, we define the temporal robustness metric ($R_N$) for a time-varying network as follows:

$$R_N = \frac{\mathbb{E}[N_{SuccDisrupted}]}{\mathbb{E}[N_{Succ}]}.$$  \hspace{1cm} (1)

The denominator of the robustness metric in (1) represents the mean number of successfully communicating nodes before any disruption in the network. Hence, it captures only the natural effect, like communication failure in the network. On the other hand, in the numerator we evaluate the mean number of successfully communicating nodes after the network is disrupted. In the next section, we start by analyzing the denominator of (1) and then focus on the numerator.

III. STOCHASTIC ANALYSIS OF TEMPORAL ROBUSTNESS METRIC

A. Expected Number of Successfully Communicating Nodes Before the Network Disruption

To evaluate the number of successfully communicating nodes in the presence of communication failure, we follow the association strategy of a typical NCH member when there are $\lfloor Np \rfloor$ CHs in the network, as shown in Fig. 3(b). We assume homogeneity in the network, where all nodes use the same transmitted power, and the received signal power decides the link presence/absence between nodes. We may note that best-SINR-based user association mechanism is one of the trendy methods (where load balancing is not a primary concern) followed by the long-term evolution (LTE) standardization [50]. In this context, the authors in [51] prove that the highest SINR association is equivalent to the strongest received signal power-based association. Motivated by the reality above, this work defines the link presence probability as a function of received signal power strength. Therefore, we can say, a typical NCH, $j$, fails to
transmit its data to the BS if both of the following events occur:

Event 1: The jth NCH fails to find any suitable CH for its association, or no link exists between the serving CH and the BS. In other words, the ith CH will not serve the jth NCH if either of the edges between ith CH to NCH j or between BS to CH i or both are absent.

Event 2: Due to the limited communication range, no direct connection is present between the NCH and the BS.

The probabilistic analysis of the two events mentioned above is expressed as follows. Therefore, the no-edge formation probability from ith CH to the jth NCH can be expressed as follows:

\[ P_i \left( \sqrt{(x_j-x_i)^2+(y_j-y_i)^2} \right)^{-\alpha} h_{ij} < P_{th} \]  (2)

where \( P_i \) is the transmit power of all nodes, and \((x_j, y_j)\) and \((x_i, y_i)\) are the coordinates of NCH j and CH i, respectively. \( \alpha \) denotes the path loss exponent. The \( h_{ij} \) represents the power gain of the Rayleigh fading channel between the ith CH and jth NCH, hence is expressed as exponentially distributed random variables with a mean of 1. Moreover, \( P_{th} \) denotes the received power threshold value that determines the network connectivity. To make the equation compact, from here onward we express \( \sqrt{(x_j-x_i)^2+(y_j-y_i)^2} \) as the distance between two vectors, i.e., \(|r_j - r_i|\). Hence, (2) can be rewritten as follows:

\[ P_i |r_j - r_i|^{-\alpha} h_{ij} < P_{th} \Rightarrow h_{ij} < \frac{P_{th}|r_j - r_i|^\alpha}{P_i}. \]  (3)

Similarly, from the perspective of the downlink transmission, it easily follows that there exists no edge between the BS and the ith CH iff:

\[ g_{ib} < \frac{P_{th}|r_i|^\alpha}{P_B} \]  (4)

where \( P_B \) is the transmit power of the BS. The \( g_{ib} \) represents the power gain of the Rayleigh fading channel between the ith CH and the BS. Equation (3) confirms that the connection probability between the ith CH and jth NCH is:

\[ \exp\left(-\frac{P_{th}|r_j - r_i|^\alpha}{P_i} \right). \]

Similarly, the connection probability between the BS and the ith CH from (4) can be expressed as:

\[ \exp\left(-\frac{P_{th}|r_i|^\alpha}{P_B} \right). \]

So, the jth NCH will not find the ith CH as a suitable one with the probability of

\[ 1 - \exp\left\{ -\left( \frac{P_{th}|r_j - r_i|^\alpha}{P_i} + \frac{P_{th}|r_i|^\alpha}{P_B} \right) \right\} \]

which is the probability that at least one edge is absent between the two edges mentioned above. Thus, the nonassociation probability of the jth NCH with either of the \([Np]\) CHs in the network is

\[ \prod_{i=1}^{[Np]} \left( 1 - \exp\left\{ -\left( \frac{P_{th}|r_j - r_i|^\alpha}{P_i} + \frac{P_{th}|r_i|^\alpha}{P_B} \right) \right\} \right) \]

where \( r_j \) and \( r_i \) represent the vectors corresponding to the coordinates of all CHs and the jth NCH in the network, respectively. As mentioned earlier, one NCH will attempt to transmit directly to the BS if it fails to associate with any of the CHs in the network. Therefore, the jth NCH is not directly connected to the BS iff

\[ P_B|r_j|^{-\alpha} k_{jb} < P_{th} \]

where \( k_{jb} \) represents the power gain of the Rayleigh fading channel between the jth NCH and the BS, which confirms that the probability that there is no direct connection between jth NCH and BS is:

\[ (1 - \exp\left(-\frac{P_{th}|r_j|^\alpha}{P_B} \right)). \]

So, the communication failure probability of a typical NCH, \( j \), or in other words, the probability that the jth NCH fails to transmit its data successfully through either way of transmission, can be expressed as follows:

\[ P_{FBE} = \left\{ \prod_{i=1}^{[Np]} \left( 1 - \exp\left\{ -\left( \frac{P_{th}|r_j - r_i|^\alpha}{P_i} + \frac{P_{th}|r_i|^\alpha}{P_B} \right) \right\} \right) \times \left( 1 - \exp\left(-\frac{P_{th}|r_j|^\alpha}{P_B} \right) \right) \} \]  (5)

Equation (5) is valid for fixed positions of all the CHs and the jth NCH. However, in this work, the NCHs and the CHs can be positioned anywhere within the grid dimension of \([-a, a]\). Hence, the mean failure probability of NCH \( j \), expecting over all grid positions of both jth NCH and all CHs, can be expressed as follows:

\[ P_{FNC} = \mathbb{E}_{r_i|r_j} \left[ P_{FBE} \right] \]  (6)

Similarly, the expected successful communication probability of CH \( i \), \( P_{SCH} \), over all possible grid positions is

\[ P_{SCH} = \mathbb{E}_{r_i} \left[ \exp\left(-\frac{P_{th}|r_i|^\alpha}{P_B} \right) \right]. \]

Hence, for the given values of CHs (i.e., \( N_{CH} \)) and NCHs (i.e., \( N_{NCH} \)), the average number of successfully communicating NCHs and CHs in the network are equal to

\[ N_{SNCH} = N_{NCH}(1 - P_{FNC}) \& N_{SCH} = N_{CH}P_{SCH}. \]

So, before any node removal in the network, the total number of successfully communicating nodes in the network is equal to

\[ N_{SPA} = N_{NCH}(1 - P_{FNC}) + N_{CH}P_{SCH}. \]  (10)

Note that (10) is valid for a fixed number of CHs and NCHs in the network. However, in this work we allow the number of CHs and NCHs to vary between 0 and \( N \). Moreover, as the numbers of CHs and NCHs are dependent on each other, i.e., \( N_{CH} = N - N_{NCH} \), the expectation over any one of these two is sufficient to proceed further. The mean number of successfully communicating nodes expecting over all possible values of CHs is

\[ N_{ESP} = \mathbb{E}_{N_{CH}}[N_{NCH}(1 - P_{FNC}) + N_{CH}P_{SCH}] \]

\[ = [N(1 - p)](1 - P_{FNC}) + [Np]P_{SCH}. \]  (11)

Equation (11) represents the average number of successful nodes in the presence of communication failure only. In the next section, we will capture the effect of random node failure in the network.
B. Expected Number of Successfully Communicating Nodes in the Disrupted Network

To investigate the impact of the random node failure on the number of successfully communicating nodes, let us assume that at a particular instant of time, the number of failing nodes in the network is $K$, where $1 \leq K \leq N$ and $N = N_{CH} + N_{NCH}$. Let us suppose that among the $K$ failing nodes, there are $R$ CHs and $K-R$ NCHs removed from the network. Hence, the remaining number of CHs and NCHs after $K$ nodes removal are $N_{CH} - R$ and $N_{NCH} - K + R$, respectively. By following (10), the number of successfully communicating nodes among the $K$ nodes are removed from the network is equal to:

$$\mathbb{E}_0(K, R, N_{CH}) = [(N - N_{CH}) - (K - R)](1 - \mathbb{P}_{FNCH}) + (N_{CH} - R)\mathbb{P}_{CH}.$$  \hspace{1cm} \text{(12)}$$

Equation (12) is valid for fixed values of $K$, $R$, and $N_{CH}$. However, the stochastic analysis should express the mean robustness for all possible values of $K$, $R$, and $N_{CH}$, which we now look into. Note that for a given $K$, the value of $R$ can vary within a specific range, which is determined from $0 \leq R \leq K$, $0 \leq K \leq N_{CH}$, and $0 \leq K - R \leq N - N_{CH}$. From these conditions, one can easily derive that

$$R \leq \min(K, N_{CH}).$$

Hence, the expected number of successful nodes for all possible values of the number of removed CHs, $R$, is expressed as follows:

$$\mathbb{E}_1(K, N_{CH}) = \mathbb{E}[\mathbb{E}_0(K, R, N_{CH})] = \sum_{R=R_{min}}^{R_{max}} \mathbb{E}_0(K, R, N_{CH})\mathbb{P}_{CH}(K, R, N_{CH}).$$ \hspace{1cm} \text{(13)}$$

$\mathbb{P}_{CH}(R, K, N_{CH})$ represents the failure probability of $R$ CHs among the $K$ removed nodes, and can therefore be expressed as follows:

$$\mathbb{P}_{CH}(R, K, N_{CH}) = \frac{{N_{CH} \choose R}({N-N_{CH}} \choose K-R)}{\binom{N}{K}}.$$  \hspace{1cm} \text{(14)}$$

One can easily derive that the number of failing nodes is uniformly distributed and can take any value in $\kappa = \{1, 2, 3, \ldots, N\}$. Hence, expecting over all possible numbers of removed nodes, the number of successfully communicating nodes becomes

$$\mathbb{E}_2(N_{CH}) = \mathbb{E}_K[\mathbb{E}_1(K, N_{CH})] = \frac{1}{N} \sum_{K=1}^{N} \mathbb{E}_1(K, N_{CH})$$

where $\mathbb{P}_K(N) = (1/N)$ is the probability mass function (PMF) of the number of removed nodes in the network. Similarly, the expectation over the possible number of CHs gives

$$\mathbb{E}_3 = \sum_{N_{CH}=0}^{N} \mathbb{E}_2(N_{CH})\mathbb{P}_{NCH}(N, p)$$ \hspace{1cm} \text{(15)}$$

where $p$ is the CH probability and $\mathbb{P}_{NCH}(N, p)$ is the PMF of the number of CHs and NCH. As an individual node can be elected either as a CH or as an NCH member, the PMF of the number of CHs follows the binomial distribution, which can be expressed as follows:

$$\mathbb{P}_{NCH}(N, p) = \binom{N}{N_{CH}}p^{N_{CH}}(1-p)^{N-N_{CH}}.$$  \hspace{1cm} \text{(16)}$$

Now, by following (1), (11), and (14), the temporal robustness metric can be expressed as:

$$R = \frac{\mathbb{E}_3}{\mathbb{E}_{ESP}}.$$ \hspace{1cm} \text{(17)}$$

Note that the first factor of the exact expression of temporal robustness expressed in (7), shown at the bottom of the page, exhibits the form of $\mathbb{E}[f(r_1, r_2, \ldots, f(r_{[N]}))$, where the presence of the common variable, $r_j$ in all the terms in the product form makes their separation difficult. The dependency on this variable, $r_j$, complicates the evaluation of (7) for a higher number of CHs. Therefore, to make the equation simpler, we use two levels of approximation.

Approximation 1: The above discussion confirms that (15) becomes intractable for a large number of CHs in the
network. However, to simplify the equation, \[E_{GOSWAMI et al.: ANALYSIS OF TEMPORAL ROBUSTNESS IN MASSIVE MACHINE TYPE COMMUNICATIONS 6921}\] follows:

\[\approx \mathbb{E}[f(\mathbf{r}_j, \mathbf{r}_1)] \times \cdots \times \mathbb{E}[f(\mathbf{r}_j, \mathbf{r}_[\lfloor N_p \rfloor])].\] (16)

Note that all the \([N_p]\) elements of the first factor in (7) end up having the same expected values due to positioning within the same grid range from \(-a\) to \(a\). Hence, the above expression is approximated in (8), shown at the bottom of the previous page.

**Approximation 2:** Note that (14) can be represented in the form of \[\mathbb{E}_{NCH}[f(N_{CH})].\] By using the following approximation \[\mathbb{E}_{NCH}[f(N_{CH})] \approx f(\mathbb{E}_{NCH}[N_{CH}]) = f(\lfloor N_p \rfloor)\] (as we define earlier that the \(\mathbb{E}[N_{CH}] = \lfloor N_p \rfloor\)), (14) can be approximated as follows:

\[L_3 \approx L_2(N_{CH} = \lfloor N_p \rfloor).\]

**IV. NUMERICAL INVESTIGATION**

This section investigates the effectiveness of the proposed analytical model described in Section III. More specifically, to corroborate the exactness of the analytical expression derived in this work, we here compare the analytical results with the ones we obtain from the numerical investigation. The system parameter values used in this investigation are listed in Table I. Our numerical investigation is performed for the time switching graph over 10,000 realizations corresponding to different node positions, the number of failing nodes, all possible numbers of CHs in the network, and the number of CHs removed due to network disruption. Moreover, in the below section, we assume a node density value in line with the current requirement of supporting one million devices per km² for mMTC services. We assume that all nodes can participate in the CH election procedure, where they generate random numbers between \([0, 1]\) and elect themselves as CH members only if the outcome is less than \(p\). Once the election procedure is over, all NCHs prefer to send their data through a suitable CH to maximize the networks’ energy efficiency. If an NCH member fails to associate with all the available \([N_p]\) CHs, only then it attempts to transmit to the BS directly. Note that, unlike an infrastructure network, the radio link in a communication network ensures an effortless reassociation to the network connectivity. Hence, we allow the network reconnection after a disruption occurs. Moreover, we consider a downlink mMTC network that enables the BS to operate as a transmitter for determining the connectivity between BS and a node.

Fig. 4 performs a comparative study between the analytical and the numerical investigation. Note that in Fig. 4, we compare the result of the exact form of the network robustness [i.e., (7)] with the numerical one. The overlapping curves corresponding to the exact form of analytical expression and numerical investigation validate the derived analytical framework. As explained earlier, to circumvent the intractability of (7), we present a comparatively low complexity two-level approximated form of the exact expression in (8), which we have exploited in the below section for further investigation.

We now evaluate the trend of the network robustness and the number of successful nodes as a function of various system parameters. By considering the quantity defined in [39], we express the mean node degree \(\langle K \rangle\) of a time-varying switching graph as follows:

\[K(t) = \frac{1}{N} \sum_{i=1}^{N} k_i(t); \quad \langle K \rangle = \frac{1}{T} \sum_{t=1}^{T} K(t)\] (17)

where \(t = \{1, 2, \ldots, T\}\) is the collection of the observation time instants and \(k_i(t)\) represents the in-degree of the \(i\)th node at the \(t\)th instant of time. We compare the numerical investigation result with the network robustness metric described in (17).

The overlapping curves in Fig. 5 confirm the correlation of \(L_1\) between the temporal robustness value obtained from numerical investigation and the one achieved from [39], thereby establishing a direct relation between the two. In addition, Fig. 5 compares the results of the numerical investigation with the approximated analytical framework as a function of CH probability for different network sizes. To explain the reason for choosing the CH probability value in the range between

| Parameter | Value | Parameter | Value |
|-----------|-------|-----------|-------|
| Number of Nodes | 150 | Node Density | 1 Node/m²² |
| \(P_{th}\) | -111 dBm -141 dBm [52] | \(P_B\) | 46 dBm |
| \(P_i\) | 23 dBm [52] | Number of Iterations | 10,000 |

**Fig. 4.** Comparative study of network robustness as a function of network size.

**Fig. 5.** Network robustness comparison as a function of CH probability for different network sizes and power threshold values.
0.04 and 0.15, we would like to shed light on the fact that energy consumption and signaling overhead are critical challenges in mMTC networks. That motivates us to consider CH probability values which maximize the battery lifetime. In this context, the numerical investigation in [53] shows that one can guarantee 100% node coverage for the CH probability value of 0.15. Moreover, the authors confirm that increased number of CHs results in a linear rise in communication overhead. This discussion motivates us to restrict the CH probability value to 0.15. Furthermore, the numerical study in [54] shows that a low value of CH probability can ensure a higher network lifetime. Therefore, the combined observations from [53] and [54] motivate our choice to consider a CH probability between 0.04 and 0.15. Moreover, this figure exhibits the influence of the power threshold value on the parametric trend of the network robustness metric, which confirms a gap between the analytical and numerical investigation smaller than 1.5%, even in the presence of a higher value chosen from the realistic range of the power threshold. This gap becomes even more negligible (0.10%) for a comparatively lower power threshold value of $-141$ dBm. This minimal performance gap in Fig. 5 allows us to use the low complexity approximated form of (7) in turn increases the difference between the analytical and numerical investigation for a large number of CHs in the system. Furthermore, this figure exhibits the variation of network robustness as a function of the CH probability. We observe a negligible variation in the robustness metric value for a wide range of realistic power threshold values as a function of the number of CHs present in the network. The below discussion justifies the observed parametric trend. Note that the robustness metric in (15) is defined as the ratio between the number of successful nodes before and after the network disruption. Hence, depending on the nature of these two factors, the parametric trend of the network robustness metric varies with the system parameters.

To justify the above-mentioned observed trend in Fig. 5, Fig. 6 investigates the number of successful nodes before and after network disruption as a function of the number of CHs in the network. The comparable increment of both the factors (i.e., the pre- and post-disruption number of successful nodes) introduces a negligible variance in the network robustness for the different CH probability values. This observation is true for a wide range of realistic power threshold values (where the practical range of power threshold lies between $-84$ to $-141$ dBm [52]).

For an in-depth analysis of the observed trend in Fig. 5, Fig. 7 evaluates the impact of the network disruption as a function of the number of CHs for various network sizes and for different values of the power threshold. Fig. 7(a) confirms an increasing trend of the failing nodes as a function of the number of CHs only when the power threshold value is comparatively high (i.e., $-111$ dBm). In particular, we express the percentage of failing nodes as the ratio between the number of failing nodes due to the network disruption and the number of successful nodes before the network disruption. In contrast, the percentage of failing nodes exhibits a decreasing trend as a function of a number of CHs for a lower power threshold value of $-141$ dBm. Fig. 7(b) justifies the trend of Fig. 7(a) as it exhibits a similar trend of increasing and decreasing nature of the percentage of failing CHs, due to the network disruption as a function of CH probability in the presence of a power threshold value of $-111$ and $-141$ dBm, respectively. More specifically, the percentage of failing CHs is measured by the ratio between the number of failing CHs due to network disruption and the number of successful CHs under the network’s standard operation. The observed trends can be justified as follows: an increase in the CH probability indicates more CHs in the network, thereby decreasing the number of NCHs in the network as the sum of CHs and NCHs is equal to $N$. Note that the network connectivity only in the presence of a high received power demands a reliable channel between one device and BS for the successful transmission. An NCH member’s operation enables a node to either forward its data through a CH member or transmit its data directly to the BS if no suitable CH is found for relaying the data. In
contrast, only the presence of a direct link between the CH to the BS can ensure the successful communication of a CH member. Hence, with increased CHs, the extra benefit of using relay nodes decreases in the system as all CHs need to send their data directly to the BS. The lack of channel diversity due to the strict requirement of direct connection to the BS reduces the possibility of experiencing reliable channels by each CH member. As a result, the possibility of CH failure increases with an increasing number of CHs in the presence of a high connectivity threshold. In contrast, a low power threshold value requires much less received power to guarantee the network connectivity, which can be easily ensured by direct transmission between one node and the BS without requiring the support of any relay node. As a result, irrespective of the mode of operation (i.e., NCH/CH), a node can always ensure successful communication in the network. In addition, the random placements of NCH nodes over the prespecified grid position restrict the power-constrained NCH from reaching any CH in the presence of fewer CHs in the network. However, with an increase in the number of CHs, the possibility that one typical NCH will opt for an intermediate node to forward its data also increases. Thus, the higher possibility of direct communication and the added benefit of exploiting an intermediate node prevent the number of failing nodes from increasing further for a low power threshold, which explains the decreasing trend of the percentage of failing CHs as a function of the CH probability in the system. Hence, in the presence of a fixed number of nodes in the network, the percentage of failing nodes directly follows the trends of failing CHs percentage for all power threshold values.

In addition, from Fig. 5 we can observe a negligible increase in the network robustness with an increase in network size. A high robustness value for large networks indicates the strong potential of any network to continue its regular operation by combating any external disturbance and challenges. The observed parametric trend can be explained by following the similar argument stated above. In detail, an increase in the network size has a slightly more positive influence on the number of successful nodes after the disruption, than that on the number of successfully communicating nodes before the network is disrupted. More precisely, a comparatively higher increment in the post-disruption number of successful nodes (i.e., 204%) than that of the predisruption successful nodes (i.e., 200%) with increasing network size in Fig. 6 justifies the rising tendency of network robustness metric as a function of network size in Fig. 5. Hence, Figs. 6 and 7 combinedly justify both the increasing trend and the negligible variation in the network robustness in the presence of large network size and for different power thresholds values, respectively.

In Fig. 8, we evaluate the variation in temporal robustness as a function of CH failure probability for different NCH failure probability values, where we keep the CH probability fixed. A decreasing trend of network robustness as a function of CH failure probability is observed for a given NCH failure probability value. The observation is intuitive because, for a given number of failing NCHs in the network, an increase in failing CHs confirms more failing nodes in the network (as failing node number is equal to the sum of failing CHs and NCHs), which, in turn, reduces the temporal robustness of the network. A negligible variation in the temporal robustness for a wide range of CH probability values necessitates further study to investigate the effectiveness of CH members in maintaining the network robustness.

Therefore, to evaluate the significance of CH members, Fig. 9 investigates the influence of CHs in maintaining network connectivity in the disrupted network. In particular, this figure investigates the network connectivity reduction as a function of CH failure probability for different NCH failure probability values, where we observe an increasing trend of connectivity reduction as a function of the CH failure probability. Fig. 9 explains the parametric trend of the temporal robustness exhibited by Fig. 8. Therefore, the combined observations from Figs. 8 and 9 align with the fact reported in [32] that robustness is directly governed by the connectivity reduction in the disrupted network. Moreover, the overlapping lines corresponding to different node sizes confirm that our robustness metric is invariant of network size [32].

Next, we investigate the impact of the node removal on the temporal robustness factor. In particular, Figs. 10 and 11 exhibit the variation of temporal robustness as a function of node failure probability for different power threshold and CH probability values, respectively. The performed numerical investigation shows that the network robustness increases
for an increasing number of CHs and a higher power threshold value. From the fact stated above that network robustness is directly controlled by the connectivity reduction in the disrupted networks, Figs. 10 and 11 can be interpreted as follows: an increase in the CH probability and power threshold value is beneficial to maintaining the network connectivity in a disrupted network. The observation in Fig. 10 aligns with the results in [53] which show that more CHs provide better node coverage in the network.

Finally, the significance of the work in [32] and the invariant nature of our proposed network robustness as a function of CH probability and power threshold value for the node density of $10^6$ nodes/km$^2$ in Fig. 5 motivate us to perform a comparative study with the work in [32] and address the query of whether the invariance of temporal robustness is valid for all sets of simulation parameters. In this context, we would like to highlight the fact that multiple works in [46] and [56] confirm numerous benefits of cluster-based mMTC network architecture, such as efficient group paging, minimizing radio access network congestion, and maximizing energy efficiency, which are crucial aspects for beyond 5G networks. In Figs. 12 and 13, our proposed robustness metric follows similar parametric trends of network robustness for system parameters, such as the number of CHs and power threshold values, as compared to the work in [32]. However, it ensures a comparatively higher temporal robustness value than the one presented in [32]. This is because, unlike [32], where the authors express the temporal efficiency as the average reciprocal distance over all pairs of network nodes, our work describes the temporal efficiency in terms of the number of successfully communicating nodes in the network. Therefore, the different definition of temporal efficiency followed in our robustness measure makes it distinguishable from the one presented in [32], as shown in Figs. 12 and 13.

A. Computational Complexity

The below section compares the computational complexities of a few well-established network robustness metrics with the
one we propose. In this context, all prior robustness metrics, i.e., super connectivity, toughness, scattering number, tenacity, expansion parameter, isoperimetric number, min-cut, and the $k$-connectivity evaluate the network robustness in an NP-time, hence, are unsuitable for large networks. Therefore, to clearly define the advantage of our proposed robustness metric, we now provide a step-by-step time complexity calculation. As mentioned earlier, we perform a stochastic analysis of the temporal robustness metric over all possible node positions in grid, the number of CHs in the network, all numbers of removed nodes, and corresponding feasible range of removed CHs caused by network disruption. Note that the NCH failure probability expecting over all the node positions can be expressed by (9), shown at the bottom of p. 6920, which has constant time complexity. However, the dependency on the number of CHs in the network, the number of nodes removal, and the feasible range of the removed CHs can be characterized by the nested for loops with the maximum number of iterations of $(N + 1)$, $N$, and $(K + 1)$, respectively. Note that the maximum number of CHs that can be removed from the network, $K$, is equal to $N$. The above fact confirms that the time complexity of the temporal robustness metric evaluation is $(N + 1) \times N \times (N + 1) = N^3 + 2N^2 + N$. Hence, the worst-case time complexity of our proposed scheme is $O(N^3)$, which is the same as the algebraic connectivity described in [30]. In addition, as shown in Approximation 2, the two-level approximated form stated in (8) excludes the requirement of the for loop associated with the number of CHs in the network, thereby experiencing the time complexity of $O(N^2)$. The low complexity of our proposed metric makes it a particularly promising candidate for temporal robustness measurement, especially for large networks.

V. Conclusion

Robust connectivity is one of the essential requirements of communication networks. The demand for a reliable connection in the latest 5G deployment scenarios led to recent investigations to revisit the topic of robustness analysis. Unlike fixed networks, wireless communication networks experience both the random fluctuation and uncertainty of the links and nodes present in the network, limiting the application of existing works, and motivating the necessity for further investigations in this domain. The lack of complete analysis in terms of temporal robustness inspired us to perform a stochastic analysis of temporal robustness in mMTC networks in this article. The comparative study with the numerical investigation confirms the exactness of our proposed analytical framework. Furthermore, the encapsulation of the communication range effect and the network’s temporal variation enables the proposed metric to quantify the temporal robustness in a realistic communication network. Besides, the low complexity and minimal gap with respect to the exact analytical expression confirm the suitability of the introduced two-level approximated form as a candidate low-complexity temporal robustness metric, proving particularly useful for large-scale deployments.

REFERENCES

[1] “Minimum requirements related to technical performance for IMT-2020 radio interface(s); ITU-R,” Rep. M.2410-0, ITU, Geneva, Switzerland, Nov. 2017.
[2] D. Goswami and S. S. Das, “Iterative sub-band and power allocation in downlink multiband NOMA,” IEEE Syst. J., vol. 14, no. 4, pp. 5199–5209, Dec. 2020.
[3] W. Luo and K. Sycara, “Minimum k-connectivity maintenance for robust multi-robot systems,” in Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS), 2019, pp. 7370–7377.
[4] K. Hazra, V. K. Shah, S. Roy, S. Deep, S. Saha, and S. Nandi, “Exploring biological robustness for reliable multi-UV/RF networks,” IEEE Trans. Netw. Service Manag., vol. 18, no. 3, pp. 2776–2788, Sep. 2021.
[5] F. Lei, S. Guo, J. Sun, Y. Peng, and W. Li, “A fault tolerance mechanism for on-road sensor networks,” Sensors, vol. 16, p. 2059, Dec. 2016.
[6] L. Ma et al., “Enhancing robustness and resilience of multiplex networks against node-community cascading failures,” IEEE Trans. Syst., Man, Cybern., Syst., vol. 52, no. 6, pp. 3808–3821, Jun. 2022.
[7] “Universal mobile telecommunications system (UMTS); LTE; 5G; NR; multi-connectivity; overall description; stage-2; study on architectural enhancements for 5G multicast-broadcast services,” Rep. TS 37.340 V15.3.0, 3GPP, Sophia Antipolis, France, 2018.
[8] S. Pokhrel, J. Ding, J. Park, O.-S. Park, and J. Choi, “Towards enabling critical mMTC: A review of URLLC within mMTC,” IEEE Access, vol. 8, pp. 131796–131813, Jul. 2020.
[9] N. H. Mahmood et al. (Univ. Oulu, Oulu, Finland), White Paper on Critical and Massive Machine Type Communication Towards 6G, 6G Research Visions. (Jun. 2020). [Online]. Available: http://urn.fi/urn:nbn:fi-feki-20200727818.
[10] R. Trivisonno, R. Guerzoni, I. Vaishnavi, and D. Soldani, “Towards zero latency software defined 5G networks,” in Proc. IEEE Int. Conf. Commun. Workshop (ICCW), Sep. 2015, pp. 2566–2571.
[11] D. Feng et al., “Toward Ultra-Reliable low-latency communications: Typical scenarios, possible solutions, and open issues,” IEEE Veh. Technol. Mag., vol. 14, no. 2, pp. 94–102, Jun. 2019.
[12] V. Gezerlis, T. Doukoglou, M. Iordache, U. Herzog, and T. Chen, “5G European validation platform for extensive trials deliverable D1.2 requirements definition and analysis from vertical industries and core applications,” 5G Public-Private-Partnership, Heidelberg, Germany, Oct. 2018.
[13] “Machine-to-Machine communications (M2M); M2M service requirements,” ETSI, Sophia Antipolis, France, Rep. ETSI TS 102 689 V1.1.1, Aug. 2010.
[14] “LTE; evolved universal terrestrial radio access network (E-UTRAN); self-configuring and self-optimizing network (SON) use cases and solutions,” Rep. 3GPP TR 36.902 version 9.3.1 release 9, 3GPP, Sophia Antipolis, France, Jan. 2016.
[15] D. Goswami, N. Marchetti, and S. S. Das, “Distributed time synchronization in ultradense networks,” IEEE Syst. J., vol. 16, no. 2, pp. 2136–2147, Jun. 2022.
[16] A. H. Dekker and B. Colbert, “Network robustness and graph topology,” in Proc. Aust. Comput. Sci. Conf., vol. 26, Feb. 2004, pp. 359–368.
[17] A. Sydney, C. Scoglio, M. Youssef, and P. Schumm, “Characterizing the robustness of complex networks,” Int. J. Internet Technol. Secured Trans., vol. 2, pp. 291–320, Nov. 2008.
[18] M. Newman, “The structure and function of complex networks,” Comput. Phys. Commun., vol. 147, pp. 40–45, Mar. 2003.
[19] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, “Attack robustness and centrality of complex networks,” PloS one, vol. 8, Apr. 2013. Art. no. e59613.
[20] H. Tangmunarunkit, R. Govindan, S. Jamin, S. Shenker, and W. Willinger, “Network topology generators: Degree-based vs. structural,” Comput. Commun. Rev., vol. 32, pp. 147–159, Oct. 2002.
[21] A. Jamakovic and S. Uhlig, “Influence of the network structure on robustness,” in Proc. 15th IEEE Int. Conf. Netw., Adelaide, SA, Australia, Nov. 2007, pp. 278–283.
[22] A. Tsigadham and A. Lee-Garcia, “Autonomic traffic engineering for network robustness,” IEEE J. Sel. Areas Commun., vol. 28, no. 1, pp. 39–50, Jan. 2010.
[23] W. Ellens, F. Spieksma, P. Mieghem, A. Jamakovic, and R. Kooij, “Effective graph resistance,” Linear Algebra Appl., vol. 435, pp. 2491–2506, Nov. 2011.
[24] A. Moinet, B. Darties, N. Gastineau, J.-L. Baril, and O. Togni, “Completely independent spanning trees for enhancing the robustness in ad-hoc networks,” in Proc. IEEE 13th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob), Rome, Italy, Oct. 2017, pp. 63–70.
[25] S. Wandelt and X. Sun, “Robustness estimation of infrastructure networks: On the usage of degree centrality,” in Proc. 13th Int. Conf. Availabil. Rel. Secur., New York, NY, USA, Aug. 2018, p. 45.

[26] V. Chvátal, “Tough graphs and hamiltonian circuits,” Discr. Math., vol. 306, nos. 10–11, pp. 910–917, 2006.

[27] H. Jung, “On a class of posets and the corresponding comparability graphs,” J. Comb. Theory B, vol. 24, no. 2, pp. 125–133, 1978.

[28] D. Mouzannar, “Tenacity of a graph with maximum connectivity,” Discr. Appl. Math., vol. 159, no. 5, pp. 367–380, Mar. 2011.

[29] J. Yu, M. Barahona, Y. Tan, and H.-Z. Deng, “Spectral measure of structural robustness in complex networks,” IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 41, no. 6, pp. 1244–1252, Nov. 2011.

[30] G. Deng, “The robustness analysis of wireless sensor networks under uncertain interference,” Sci. World J., vol. 2013, Nov. 2013, Art. no. 185970.

[31] S. Scellatto, I. Leontiadis, C. Mascolo, P. Basu, and M. Safer, “Evaluating temporal robustness of mobile networks,” IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 105–117, Jan. 2013.

[32] S. Trajanovski, S. Scellatto, and I. Leontiadis, “Error and attack vulnerability of temporal networks,” Phys. Rev. E, vol. 85, Jun. 2012, Art. no. 066105. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevE.85.066105

[33] M. Abdel-Basset, H. Hawash, R. K. Chakraborty, and M. J. Ryan, “Semi-supervised spatiotemporal deep learning for intrusions detection in IoT,” Internet Things J., vol. 8, no. 15, pp. 12251–12265, Aug. 2021.

[34] H. H. Sano and L. Berton, “Topoloy and robustness analysis of temporal air transport network,” in Proc. 35th Annu. ACM Symp. Appl. Comput., New York, NY, USA, 2020, pp. 1881–1884.

[35] S. Scellatto, I. Leontiadis, C. Mascolo, P. Basu, and M. Safer, “Understanding robustness of mobile networks through temporal network measures,” in Proc. IEEE INFOCOM, Shanghai, China, Apr. 2011, pp. 1–5.

[36] V. Batagelj and S. Praprotnik, “An algebraic approach to temporal network analysis based on temporal quantities,” Soc. Netw. Anal. Mining, vol. 6, p. 28, May 2016.

[37] X. Feng, S-W. He, and Y-B. Li, “Temporal characteristics and reliability analysis of railway transportation networks,” Transportmetrica A Transp. Sci., vol. 15, no. 2, pp. 1825–1847, 2019. [Online]. Available: https://doi.org/10.1080/23249935.2019.1647308

[38] N. Wang, N. Wu, L-L. Dong, H-K. Yan, and D. Wu, “A study of the temporal robustness of the growing global container-shipping network,” Sci. Rep., vol. 6, Oct. 2016, Art. no. 34217.

[39] S. Dhuli, S. Kouachi, A. Chhabra, and Y-N. Singh, “Network robustness analysis for IoT networks using regular graphs,” IEEE Internet Things J., vol. 9, no. 11, pp. 8809–8819, Jun. 2022.

[40] O. Dagdeviren and V. K. Akram, “The effect of random node distribution and transmission ranges on connectivity robustness in wireless sensor networks,” in Proc. Int. Symp. Netw. Comput. Commun. (ISNCC), Istanbul, Turkey, Jun. 2019, pp. 1–5.

[41] M. Williams and M. Musolesi, “Spatio-temporal complex networks: Reachability, centrality, and robustness,” Roy. Soc. Open Sci., vol. 3, p. 160196, Jun. 2015.

[42] Q. Liang and E. Modiano, “Survivability in time-varying networks,” in Proc. IEEE INFOCOM 35th Annu. Int. Conf. Comput., Shanghai, China, Apr. 2016, pp. 1–9.

[43] M. Paik and H. Ko, “Distributed group location update algorithm for massive machine type communication,” Sensors, vol. 24, no. 24, p. 7336, Nov. 2020. [Online]. Available: https://www.mdpi.com/1424-8208/20/24/7336

[44] K. Lee, J. Shin, Y. Cho, K. S. Ko, D. K. Sung, and H. Shin, “A group-based communication scheme based on the location information of MTC devices in cellular networks,” in Proc. IEEE Int. Conf. Commun. (ICC), Ottawa, ON, Canada, Jun. 2012, pp. 4899–4903.

[45] S. K. Sharma and X. Wang, “Toward massive machine type communications in ultra-dense cellular IoT networks: Current issues and machine learning-assisted solutions,” IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 426–471, 1st Quart., 2020.

[46] Z. Li, J. Chen, R. Ni, S. Chen, X. Li, and Q. Zhao, “Enabling heterogeneous mMTC by energy-efficient and connectivity-aware clustering and routing,” in Proc. IEEE Globecom Workshops (GC Wkshps), Singapore, Dec. 2017, pp. 1–6.

[47] H. Shariatmadari et al., “Machine-type communications: Current status and future perspectives toward 5G systems,” IEEE Commun. Mag., vol. 53, no. 9, pp. 10–17, Sep. 2015.

[48] A. Nessa, M. Kadoch, and B. Rong, “Fountain coded cooperative communications for LTE-a connected heterogeneous M2M network,” IEEE Access, vol. 4, pp. 5280–5292, 2016.

[49] P. Pujol, R. Statnica, and F. Vahid, “LTE user association for self-deployable networks in disaster management scenarios,” in Proc. Int. Conf. Inf. Commun. Technol. Disast. Manage. (ICT-DM), Dec. 2019, pp. 1–4.

[50] B. Yang, M. Ding, G. Mao, and X. Ge, “Performance analysis of dense small cell networks with generalized fading,” in Proc. IEEE Int. Conf. Commun. (ICC), May 2017, pp. 1–7.

[51] S. Tabbane, “IoT standards part II: 3GPP standards GPP standards,” Internet of Things (IoTs) networks, 3GPP, Sophia Antipolis, France, Sep. 2018.

[52] M. Youssef, A. Youssef, and M. Younis, “Overlapping Multihop clustering for wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 12, pp. 1844–1856, Dec. 2009.

[53] H. Yang and B. Sikdar, “Optimal cluster head selection in the LEACH architecture,” in Proc. IEEE Int. Perform. Comput. Commun. Conf., May 2007, pp. 93–100.

[54] “3rd generation partnership project; technical specification group radio access network; universal mobile telecommunications system (UMTS); 5G; service requirements for the 5G system,” Rep. TS 22.261 version 16.14.0, 3GPP, Sophia Antipolis, France, Apr. 2021.

[55] J. Huang, W. Zhan, X. Sun, P. Liu, and D. Kong, “Cluster-based group paging scheme with preamble reuse for mMTC in 5G networks,” in Proc. IEEE Global Commun. Conf., Dec. 2020, pp. 1–6.
Harun Siljak (Senior Member, IEEE) received the bachelor’s and master’s degrees in electronics and control engineering from the University of Sarajevo, Sarajevo, Bosnia and Herzegovina, in 2010 and 2012, respectively, and the Ph.D. degree in electronics and electrical engineering from International Burch University, Sarajevo, in 2015. He is currently an Assistant Professor of Embedded Systems, Control, and Optimization with Trinity College Dublin, Dublin, Ireland. He has published more than 40 peer-reviewed articles in communications, computation, control, and mathematics, and more than 15 media articles on science, technology, and society. His research interests include complex networks and cyber-physical systems and unconventional methods of computation, communication, and control.

Suvra Sekhar Das received the B.Eng. degree in electronics and communication engineering from the Birla Institute of Technology, Ranchi, India, in 2000, and the Ph.D. degree in wireless communication from Aalborg University, Aalborg, Denmark, in 2007. He was a Senior Scientist with the Innovation Laboratory, Tata Consultancy Services, Kolkata, India, from 2000 to 2008. He is currently an Associate Professor with the G. S. Sanyal School of Telecommunications, Indian Institute of Technology Kharagpur, Kharagpur, India. His research interests include the field of radio access technology.

Nicola Marchetti (Senior Member, IEEE) received the first M.Sc. degree in electronic engineering from the University of Ferrara, Ferrara, Italy, in 2003, and the second M.Sc. degree in mathematics and the Ph.D. degree in wireless communications from Aalborg University, Aalborg, Denmark, in 2010 and 2007, respectively. He is an Associate Professor of Wireless Communications with Trinity College Dublin, Dublin, Ireland, where he is also a Fellow. He performs his research under the Irish Research Centre for Future Networks and Communications (CONNECT). He has authored in excess of 170 journals and conference papers, two books and nine book chapters, and holds four patents. His research interests include: autonomous and self-organizing networks, communications for biology, PHY algorithms and MAC Protocols, and quantum communications and networks. Dr. Marchetti received four Best Paper Awards.