

DDoSimu5G: A Simulator to Model D2D Botnet DDoS Traffic Loads on 5G Components

Karim Khalil*
EIT, LTH, Lund university
Lund, Sweden
karim.khalil@eit.lth.se

Sara Ramezani
Karlstad university
Karlstad, Sweden
sara.ramezani@kau.se

Christian Gehrmann
EIT, LTH, Lund university
Lund, Sweden
christian.gehrmann@eit.lth.se

Jakob Sternby
Ericsson Research, Ericsson
Lund, Sweden
jakob.sternby@ericsson.com

Abstract

5G networks are increasingly exposed to Distributed Denial of Service (DDoS) attacks launched by mobile botnets exploiting user equipment (UE). Existing studies have treated malware propagation and DDoS impact separately, with no prior simulation work having modeled how Device-to-Device (D2D) malware spreads and translates into network-wide DDoS stress. This paper introduces *DDoSimu5G*, an extension of *Simu5G* [33] integrated with the ONE simulator [24], which enables, for the first time, the combined modeling of D2D malware propagation, UE mobility, and botnet-driven traffic loads on 5G infrastructure. The framework is aligned with 3GPP Proximity based Services (ProSe) in the 5G System (5GS) TS 23.304 [1] specifications, supports configurable attack scenarios, and generates diverse datasets, including infection logs, mobility traces, and PCAP traffic. By linking propagation dynamics with DDoS effects, *DDoSimu5G* provides the research community with a reproducible open-source tool for studying and mitigating emerging D2D-driven threats in 5G networks.

CCS Concepts

• **Networks** → **Network performance evaluation**; • **Security and privacy** → **Mobile and wireless security**; **Denial-of-service attacks**.

Keywords

5G network simulation, malware propagation modeling, DDoS, traffic measurement, dataset generation.

ACM Reference Format:

Karim Khalil, Christian Gehrmann, Sara Ramezani, and Jakob Sternby. 2026. DDoSimu5G: A Simulator to Model D2D Botnet DDoS Traffic Loads on 5G Components. In *40th ACM SIGSIM Conference on Principles of Advanced Discrete Simulation (SIGSIM-PADS '26)*, June 24–26, 2026, Vienna, Austria. ACM, New York, NY, USA, 12 pages. <https://doi.org/10.1145/3806789.3810250>

*Corresponding author



This work is licensed under a Creative Commons Attribution 4.0 International License. *SIGSIM-PADS '26, Vienna, Austria*

© 2026 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-2648-4/26/06

<https://doi.org/10.1145/3806789.3810250>

1 Introduction

Cybersecurity threats targeting telecommunication networks have rapidly increased, with intrusions rising by 41% between 2023 and 2024¹. Malware-infected User Equipment (UE), particularly Cellular IoT devices (CIoTs), significantly contribute to this threat, with forecasts further indicate that cellular IoT connections will continue to rise sharply, from around 4 billion in 2024 to more than 7 billion by 2030, with a large share consisting of mobile devices such as connected cars, drones, and wearables²³. This allows attackers to exploit Device-to-Device (D2D) communication features and vulnerabilities in CIoTs, enabling rapid formation of large-scale botnets. These botnets leverage high device mobility and dense deployments, making resulting Distributed Denial-of-Service (DDoS) attacks both scalable and difficult to mitigate [17].

D2D is defined in 3GPP TS 23.304 [1] Proximity Services (ProSe), supporting three modes of communications: Direct Communication (i.e., UE-to-UE), UE-to-Network Relay, and UE-to-UE Relay. However, relatively few efforts have identified D2D as an attack vector on 5G networks [37], [38], and [30]. The authors recognized the lack of existing work focusing on the security aspects of real-world use cases created explicitly for a D2D communication environment. To the best of our knowledge, no previous work has examined malware propagation via D2D communication in 5G networks and its potential role in enabling large-scale DDoS attacks through the network infrastructure.

Therefore, this research addresses the key question: *How can researchers effectively model and analyze the combined dynamics of D2D malware propagation and resulting botnet-driven DDoS traffic loads on 5G networks?* Our solution, *DDoSimu5G*, a discrete-time simulation framework integrating malware propagation modeling, UE mobility, and 5G network traffic emulation. Our framework facilitates versatile scenario creation and dataset generation, empowering further research into robust detection and mitigation strategies for next-generation mobile networks.

All code and configuration files are made available in a public repository [6] for reproducibility.

¹<https://go.crowdstrike.com/2024-threat-hunting-report.html>

²<https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook>

³https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/gsma_resources/mobile-iot-in-a-5g-future-whitepaper/

Understanding how malware propagates and how resulting botnets affect network performance is essential yet challenging due to ethical and practical constraints on real-world experimentation. As a result, simulation frameworks play a critical role in enabling safe and controlled studies of adversarial behaviors. While prior works such as [9], [14], [18], and [42] have presented valuable theoretical and analytical models of D2D malware propagation, they often neglect the sequential steps of D2D communication as described in TS 23.304 [1]. In particular, the standard outlines the complete chain of ProSe operation, where communication delays are tied to transmission mode requests and Layer-2 procedures. This is central for realistically modeling malware propagation in D2D scenarios.

To overcome these limitations, we introduce a modular and generic Susceptible-Infected (SI) epidemic model tailored explicitly for Device-to-Device (D2D) communication in 5G networks. Unlike earlier abstract models, our design explicitly reflects the 3GPP TS 23.304 approximation of direct D2D dynamics, which approximates the communication delays and proximity constraints associated with 5G ProSe. The model supports configurable infection parameters and accommodates diverse mobility schemes, enabling more realistic simulations and systematic analysis of D2D malware-driven DDoS impacts on 5G infrastructure.

Furthermore, by basing propagation on direct D2D interactions, the framework ensures that the number of compromised devices increases dynamically, making attack severity a function of both mobility patterns and malware propagation rate rather than a pre-selected set of malicious nodes. In particular, the use of the ONE simulator [24] allows us to approximate realistic pedestrian routines and clustered mobility behaviors. We employ two representative movement models from the ONE simulator: a randomized baseline (RWP) and a structured, activity-driven model (GAM). The latter, adapted from the Working Day Movement model, which lends greater realism to the infection dynamics compared to purely synthetic models, as shown in prior work [7]. This design choice allows us to connect malware propagation with its impact on core components, and lays the foundation for generating 5G-specific, mobility-aware adversarial datasets.

A central motivation for our design is the need for datasets that capture how DDoS attacks evolve over time and how they affect 5G infrastructure. Existing benchmarks such as CIC-DDoS2019 [41], UNSW-NB15 [32], and more recent efforts such as IXP-Scrubber [44], LATAM-DDoS-IoT [4], and THU-DDoS2024 [15] provide valuable traffic traces for intrusion detection research. However, these datasets are agnostic to the specifics of 5G, as they do not capture encapsulation at the radio access network (RAN) or aggregation at the User Plane Function (UPF), nor do they reflect how infection dynamics influence adversarial load. Our framework addresses this gap by generating configurable 5G-specialized traces that link mobility-driven propagation and dataset generation with user-plane performance metrics. Our aim, rather than replacing existing benchmarks, is for DDoSimu5G to be viewed as a complement to the broader dataset landscape, offering researchers the ability to generate datasets tailored to 5G scenarios.

In this work, we scope the adversary to user-plane UDP volumetric flooding attacks. Such attacks are both prevalent and impactful. A recent report indicates that UDP floods accounted for approximately 61% of all DDoS incidents in H2 2023, significantly

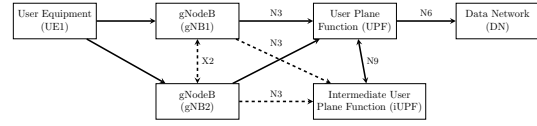


Figure 1: 5G user-plane topology with multiple gNodeBs and key interfaces.

outpacing TCP and SYN floods⁴. This makes them a practical and representative focus for our study. Moreover, these attacks are straightforward to execute, as they do not require sophisticated exploitation of C/IoT device firmware or SIM/USIM stacks; instead, lightweight application-layer malware can generate high-rate traffic streams that saturate 5G infrastructure while overwhelming backend services.

These challenges motivate our framework design. We summarize our contributions as follows:

- **An SI epidemic model tailored for D2D malware propagation in 5G networks**, supporting realistic simulation of botnet formation over time.
- **An integrated simulation framework capturing the full lifecycle** from malware propagation to UDP flooding DDoS attacks within 5G networks, and associated measuring network metrics.
- **Methodology for generating detailed datasets**, including mobility traces, D2D malware infection metrics, and realistic 5G traffic.

The paper is organized as follows. First, we present the relevant background. Next, we discuss our threat model and review related work. We then describe the system model of our proposed simulation framework, followed by its evaluation and discussion. Finally, we conclude the paper and discuss future directions.

2 Background

This paper focuses on two key areas relevant to our integrated simulation framework: the 5G user-plane network components, and Direct-D2D communication in 5G networks.

2.0.1 5G User-Plane Network Topology. The 5G user plane is responsible for forwarding data packets between UEs and external data networks. As specified in 3GPP TS 23.501, this involves key components such as the gNodeB (gNB), which provides radio access and handles both control and user data, and the User Plane Function (UPF), which enforces traffic policies and manages QoS. In larger deployments, an Intermediate UPF (IUPF) may be used to aggregate traffic from multiple gNBs before forwarding to the core network. Figure 1 illustrates the main user-plane components and relevant interfaces, including:

- **X2 Interface:** Connects gNBs to facilitate coordination, load balancing, and seamless handovers between cells.
- **N3 Interface:** Connects the gNB to the UPF, enabling the transfer of user data packets.

⁴<https://www.securitymagazine.com/articles/101109-ddos-attacks-surge-in-h2-2023>

- **N9 Interface:** Connects two UPFs, such as an iUPF and a core UPF, allowing for flexible data routing within the core network.
- **N6 Interface:** Connects the UPF to the Data Network, facilitating the delivery of user data to external networks.

The user-plane handles data traffic transport and is configured by several control-plane functions. For analyzing DDoS behavior, our focus remains on the gNBs, UPFs, and their associated interfaces that directly handle data traffic.

2.0.2 Direct-D2D Communication in 5G. D2D communication is formalized in the 3GPP technical specification TS 23.304 under Proximity Services, as well as in the 5G ProSe security architecture principles defined in TS 33.503. Additionally, 3GPP TS 36.843 examines the radio aspects of D2D communication, including proximity-based discovery and resource management.

Unlike Delay-Tolerant Networks (DTNs), which use store-and-forward mechanisms, D2D communication typically relies on structured, direct transmissions using the cell radio resources (i.e., carrier frequency). Although D2D direct communications are often initiated and managed with assistance from the infrastructure for authorization and resource allocation, the actual data transmission on the ProSe-App occurs outside the core network.

While D2D has traditionally been examined for its positive impact on network performance, relatively few studies have focused on its vulnerabilities, particularly in the context of malware propagation or security threats. In this study, D2D communication is used to serve as a propagation vector for scalable, infrastructure-independent malware propagation in 5G networks.

3 Threat model

We assume an adversary whose objective is to transfer malware between UEs over the PC5 sidelink so that compromised UEs later generate coordinated DDoS traffic against network targets, in a similar fashion as the attacker goals presented in [36], and [45]. The adversary may operate as either (i) a compromised UE (insider) that legitimately participates in ProSe discovery and link establishment, or (ii) a local active radio-range adversary capable of injecting PC5 messages within radio range. We explicitly exclude operator-level compromises (i.e., the attacker cannot maliciously provision PC5 policies or keys via the PKMF/PCF [2]). We further assume cryptographic primitives remain strong: successful attacks therefore depend on compromised devices, protocol misuse, or permissive device installation policies rather than on breaking core crypto-measures. These capability is assumed in the simulations to evaluate worst-case scenarios.

3.1 Explicit assumptions

- (1) **Attacker primary goal:** Deliver and install malware on target UEs via PC5 unicast links so compromised UEs can later generate DDoS traffic. Secondary goals: persistence, remain undetected, and propagation of UDP flooding to saturate radio-access and transport resources.
- (2) **Attacker Method:** User-plane UDP flooding attacks. Such attacks are prevalent and impactful. The disproportionate strain on infrastructure stems from the stateless nature of

UDP, as UDP packets require no session management, making it easy to saturate both radio-access and transport-layer components with minimal attacker sophistication.

- (3) **Initial foothold:** Attacker controls a limited number legitimate UEs. Attacker can run PC5 message discovery, send Direct Communication Requests (DCRs), perform L2 establishment, and send user-plane payloads within radio range.
- (4) **Cryptographic model:** As per TS 33.503 [2] with attacker success depends on: (a) possession of valid keys/contexts, (b) exploitation of failures in authentication/integrity checks, or (c) disabled/absent protections.
- (5) **UE Device assumptions:** UE auto-accept or auto-install payloads. If devices require explicit user consent or strict app signing, infection success probability drops substantially.
- (6) **Link establishment and timing:** Attacker-triggered DCR and subsequent L2 establishment follow TS 23.304 procedures. Payload transfer latency is modeled in our D2D model Section 5.2.
- (7) **Radio model & proximity:** Payload transfer requires sustained contact within communication radius (r) therefore mobility of UEs are taken into consideration for successful malware propagation in our D2D Model, Section 5.2.
- (8) **Mobility exploitation:** The attacker exploits UE mobility to expand the botnet footprint across multiple gNodeB sectors and core network components.
- (9) **Detection & remediation:** The 5G network or endpoints detection and prevention mechanisms are absent.
- (10) **Scale of initial compromise:** Experiments percentage of initially compromised UEs is 5%, to measure epidemic growth.

4 Related Work

To establish the relevance and critical importance of our research, we review prior studies on (i) DDoS simulations in cellular networks, (ii) botnet propagation via D2D communication, (iii) simulation frameworks, and (iv) dataset gaps.

DDoS Simulations in Cellular Networks. Early studies such as [5] and [20] introduced conceptual mobile botnet architectures, showing the potential of malicious UEs impact on cellular network performance even with coordinated low-bandwidth attacks. Later works, including [27] and [21], relied on small-scale simulations with static UEs to examine throughput degradation. Other efforts, such as [31] and [10], employed malicious traffic generation tools like Bonesi to study DDoS attacks. Kitana et al. [25] uniquely explored mobility aspects within LTE botnet-driven DDoS, demonstrating the interplay between user movement and network vulnerability. These contributions, however, did not measure the impacts at the full 5G infrastructure level.

D2D Malware Propagation Models. D2D communication, while beneficial for network efficiency, introduces security risks due to its decentralized nature. The study presented in [28] models infection with random-walk mobility, showing that movement accelerates spread, but it does not incorporate malware packet transmission and propagation delays. While [14] has used Gauss–Markov mobility to show higher contact rates accelerate malware. To capture the spatial-temporal dynamics, the authors in [18] have used cellular

automata and truncated Lévy walks, although without considering infrastructure delays. Other studies such as [12], [42], and [3] relied on abstract topologies or unrealistic mobility. Benomar et al. [9] came closer to 5G by applying an agent-based SI model, but assumed fixed speeds and constrained propagation rules, limiting realism. Overall, these works highlighted the need for models that couple realistic mobility with explicit infection dynamics. Our framework advances this line of research by integrating configurable delays, diverse mobility schemes, and infrastructure-aware propagation into a unified 5G context.

5G Simulation Frameworks. Several simulators provide partial support for modeling dynamics in 5G. Simu5G [33], built on OM-NeT++, enables end-to-end user-plane simulations with traffic generation, mobility, and KPI monitoring. The ONE Simulator [24] is widely used for delay-tolerant and opportunistic message passing, making it suitable for modeling D2D propagation. NS-3 [40] remains a general-purpose wireless and IP simulator.

IoTSecSim [13] simulates malware propagation among IoT devices, enabling the evaluation of infection dynamics and defense strategies. However, it focuses primarily on device-level infections and does not model botnet-driven DDoS impacts on 5G infrastructures or core network KPIs. Similarly, Boeira et al. [11] extended Simu5G to generate KPI datasets supporting anomaly detection, focusing on RAN-level faults rather than malware-induced disruptions. However, none of the presented studies presented the temporal effect of malware spread on 5G infrastructure-level traffic, a gap our framework bridges.

Attack Datasets. Benchmark datasets such as CIC-DDoS2019 [41], Bot-IoT [26], and UNSW-NB15 [32] have been widely adopted for intrusion detection. However, these suffer from imbalance, limited diversity, and lack of 5G context, as shown in [23], [19], and [35]. Recent efforts have addressed some shortcomings: LATAM-DDoS-IoT [4] focuses on IoT-specific attacks, THU-DDoS2024 [15] mixes flood types for traffic complexity, UNSW-NB15-Bot-IoT [46] combines datasets to mitigate imbalance, and IXP-Scrubber [44] extracts balanced traffic from backbone vantage points. While valuable, these remain static and do not capture dynamic propagation-driven growth. Our framework is therefore best viewed as a *complement*: it generates 5G-specific traces at gNBs and UPFs, embedding infection dynamics that link botnet growth with infrastructure stress.

In summary, while prior works have advanced DDoS attacks analysis, D2D propagation models, simulators, and datasets, they typically overlook the integration of these elements into a single, end-to-end framework. Our work addresses this gap by combining realistic D2D propagation with 5G infrastructure modeling, enabling both dataset generation and evaluation of detection mechanisms under adversarial stress.

5 Proposed System Model

This section describes the architecture of the simulation framework, the components, and the proposed D2D malware propagation model.

5.1 Simulation Framework

The framework integrates two components: the ONE simulator [24] and Simu5G [33], see Figure 2. This separation allows D2D mobility and infection propagation to be modeled independently from 5G infrastructure-level data traffic simulation, while maintaining discrete-event synchronization.

The ONE simulator is tailored for Delay-Tolerant Networks (DTNs), supporting ad-hoc, opportunistic, and D2D communication. It excels in mobility modeling and contact event generation, making it well-suited for simulating the spread of malware through proximity-based D2D interactions. Its modular and extensible architecture allowed us to implement a customizable D2D propagation model, as described in Section 5.2. Additionally, its computational efficiency made it preferable for rapidly iterating over large-scale mobility scenarios and extracting temporal contact metrics.

5.1.1 ONE simulator adaptation. We created a custom routing class, *D2DRouter*, extending *ActiveRouter*, to model direct transmission of malware between infected and susceptible nodes, see Section 5.2. Malware infections occur after a handshake and configurable transfer delay; nodes become infectious after an installation time.

Accurately capturing the effects of D2D-based malware propagation requires realistic modeling of user mobility. However, public access to real-world movement traces remains limited in scope and resolution [29]. To address this challenge, we leverage mobility models available in the ONE simulator that can approximate both generic and structured human movement. In particular, previous evaluations have shown that the ONE simulator mobility models can approximate realistic node movements and clustering behavior during daily activities, lending credibility to its use in adversarial simulation scenarios [7].

To simulate realistic movement, we use two mobility models:

- **Random Waypoint (RWP):** A synthetic baseline.
- **Generic Activity Model (GAM):** A map-based model for simulating structured lunch-hour pedestrian mobility, featuring fixed destinations and timed stops.

To assess the spread of D2D malware, RWP provides randomized movement to model generic propagation dynamics, while GAM simulates structured pedestrian routines that lead to temporary clustering of users, creating high-contact opportunities for malware transmission. Together, these models combine baseline dynamics with activity-driven realism, offering a richer perspective on how D2D propagation unfolds in 5G scenarios. The source code and mobility configurations are openly available in our repository at [6].

Movement traces and infection positions are extracted and visualized in Figure 3. Nodes are defined as any cellular UE capable of D2D communication. The ONE simulator logs node movement and infection metrics in JSON format for later use in Simu5G.

5.1.2 Simu5G adaptation. The JSON logs are imported into Simu5G using BonnMotion-compatible trace files [8]. A custom module, *DataTrafficController*, dynamically modifies traffic behavior of infected nodes based on their infection timestamp and position. This enables runtime switching from benign to DDoS traffic profiles based on infection events, allowing accurate modeling of adversarial traffic loads.

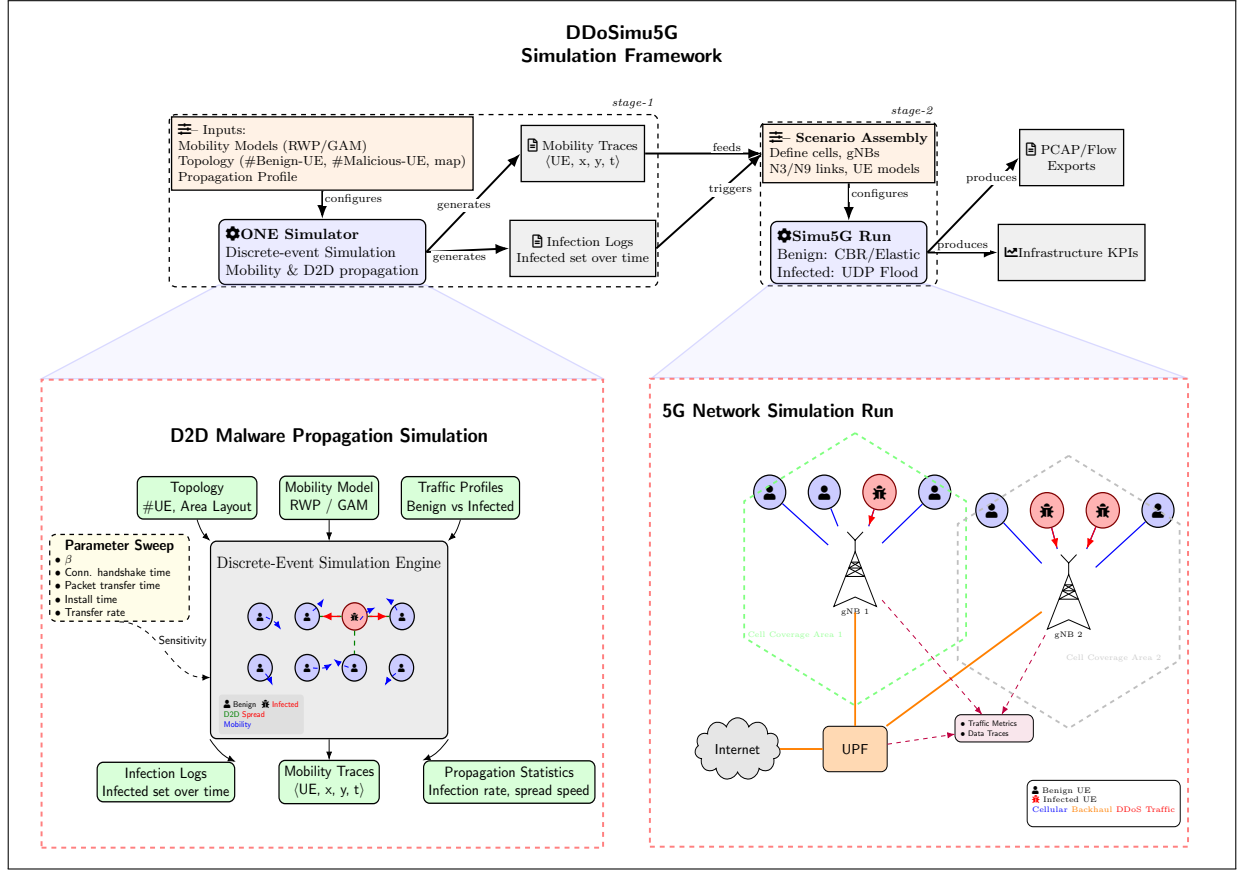


Figure 2: DDoSimu5G framework architecture

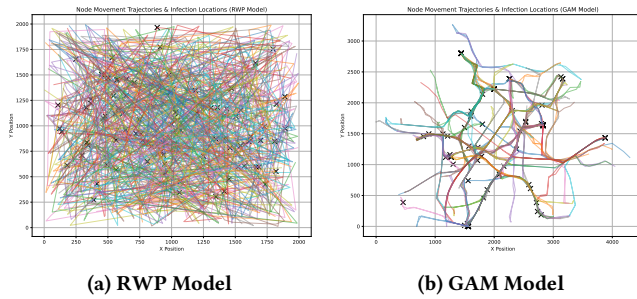


Figure 3: ONE simulator traces for node movement trajectories and infection positions represented as "X" for RWP and GAM mobility models during 1 hour of simulation.

5.1.3 Metrics and Trace Extraction. Table 1 summarizes the extracted metrics. The extracted logs enable the generation of realistic traffic patterns and support detailed analysis of malware behavior and its impact on data traffic loads on 5G network components.

5.1.4 Dataset Generation. A major limitation in the domain of studying DDoS attacks in 5G networks is the scarcity of realistic datasets reflecting malware propagation and DDoS activity in 5G

Table 1: Metrics extracted from Infection and Movement Simulation JSON Logs

Mobility Metrics	
Metric Name	Description
Node Position	(x, y) coordinates of the node at 60-sec intervals
Trajectory Path	Sequence of positions showing node movement over time, including node velocity per step
D2D Malware Infection Metrics	
Node IDs	ID of the infecting and infected nodes
Contact Duration	Time interval between connection and disconnection
Distance Between Nodes	Distance between nodes during initial contact, and at infection success
Node Positions at Contact	(x, y) positions of both nodes at contact start
Malware Infection Details	Timestamps for message creation, request, handshake, start/end transfer, and successful infections. Node (x, y) coordinates at infection. Infection status (active or inactive infection).

networks. Existing datasets, such as CIC-DDoS2019 [41], often lack mobility realism, D2D behavior, and infrastructure-level detail. While tools like DDoSIM [34] offer botnet simulation, they fall short in modeling large-scale, time-evolving 5G deployments.

To address this, **DDoSimu5G**[6] supports integrated logging of infection dynamics, node mobility, and per-UE traffic using the ONE simulator and Simu5G. Packet-level traces can be exported in .pcap

or .pcapng using OMNeT++'s PcapRecorder [43], enabling flow inspection, anomaly detection, and ML dataset generation. Combined, these features allow for reproducible, trace-driven experimentation across multiple layers of the 5G stack.

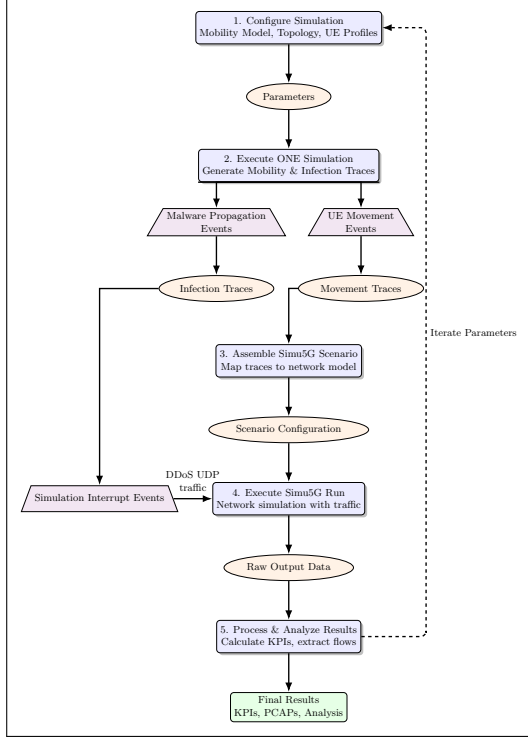


Figure 4: DDoSimu5G process flow diagram

5.1.5 Process Workflow. The process workflow of DDoSimu5G is presented in 4. The workflow begins with configuring simulation parameters, including mobility models, map topology, and UE profiles (Benign/Malicious) patterns. The ONE simulator then executes to generate both mobility traces and malware infection events. These traces are processed separately, movement traces maps to UE mobility and network/handover behavior, while infection data triggers DDoS attack simulations. The Simu5G platform executes the network simulation, incorporating both normal traffic and attack events. Finally, results are analyzed to extract key performance indicators, packet captures, and comprehensive network behavior analysis, with an optional feedback loop for parameter optimization.

5.1.6 Integration Challenges and Outcomes.

- **Semantic mismatch:** ONE is message-centric with epidemic propagation, while Simu5G is packet-centric with 5G protocols; we defined conversion layers to map infection events into traffic flows.
- **Time alignment:** ONE operates on discrete events with contact-based malware propagation timing, while Simu5G simulates slot-level scheduling; we introduced a synchronization

mechanism to map infection logs into attack traffic injection events.

- **UE behavior adaptation:** Simu5G's UEs had to be extended with role switching logic (benign $\leftrightarrow$ infected) driven by infection logs.
- **Reproducibility:** Common data formats (JSON traces) allow decoupled runs, enabling repeatable experiments and parameter sweeps.
- **Scalability:** Our framework supports scenarios from a handful of UEs up to $\sim 1,000$ UEs per run in both ONE and Simu5G. Larger experiments are realized by parallelizing runs in blocks of 1,000 UEs, allowing exploration of botnets with tens of thousands of devices. While each run yields KPIs for its block, stacking metrics and propagation delays provides an approximate view of large-scale network effects.

5.2 D2D Malware Propagation Model

Following the classical SI epidemic model used in prior D2D propagation studies [9], we adapt our design to approximate the PC5 sidelink and the sequential ProSe transmission procedures defined in 3GPP TS 23.304 [1], including the Direct Communication Request (DSR) and the UE-oriented and ProSe-service-oriented Layer-2 link establishment that precede ProSe data transfer. Modeling these stages is necessary to capture timing and proximity constraints that critically influence infection dynamics in realistic 5G D2D scenarios. Our model offers a 3GPP-grounded foundation for simulating and analyzing malware propagation in 5G-enabled D2D networks.

The model is implemented as a modular framework that supports integration with varied mobility schemes and configurable infection parameters. The theoretical model below considers only the subset of susceptible nodes ($S_{I_s} \subseteq U$) within the total UE population U . The complementary non-susceptible set ($S_{I_{ns}} = U \setminus S_{I_s}$) is not modeled here but introduced later to analyze the indirect impacts of malware-driven DDoS traffic activation on 5G network components.

5.2.1 Theoretical Model. In the proposed model, each node can exist in one of the following three states: **Susceptible** (I_s) nodes that are benign but vulnerable to infection, **Infected Inactive** (I_{inact}) nodes that have been infected but are not yet propagating malware, and **Infected Active** (I_{act}) nodes that have been infected and are actively propagating malware to other nodes. I_{inact} nodes transition to the infected active state after a fixed period of time t_{act}^c . In the proposed model, the status of all nodes is updated at regular intervals of $len(t)$ seconds. The total population of nodes (N) at any given time step t is constant and $N = N_{I_s}(t) + N_{I_{inact}}(t) + N_{I_{act}}(t)$, where $N_{I_s}(t)$, $N_{I_{inact}}(t)$, and $N_{I_{act}}(t)$ denote the number of I_s , I_{inact} , and I_{act} nodes at t , respectively.

Malware Propagation Algorithm. Algorithm 1 describes the malware propagation model. In this model, nodes successfully maintain the communication as long as nodes as they remain within the communication radius r . The Euclidean distance of two nodes x and y is denoted by $\text{dist}(x, y)$.

Contact Rate. We assume that the nodes are distributed randomly in the entire area A , the node density (ρ) is $\frac{N}{A}$, v_i , v_j , and ϕ denote the speed of i , j , and angle between the velocity vectors,

Algorithm 1 Malware propagation

Require: Sets S_{Is} , $S_{I_{inact}}$, and $S_{I_{act}}$ where the elements of these sets are the following nodes respectively: I_s , I_{inact} , and I_{act} .

```

 $S_{I_{inact}} \leftarrow \emptyset, t \leftarrow 0$ 
while  $N \neq N_{I_{act}}(t)$  do
  for  $x \in S_{I_{act}}$  do
    for  $y \in S_{Is}$  do
      if  $\text{dist}(x, y) \leq r$  for duration  $T_{infection}$  then
        add  $y$  to  $S_{I_{inact}}$ 
        remove  $y$  from  $S_{Is}$ 
    for  $z \in S_{I_{inact}}$  do
      if  $z$  has been in set  $S_{I_{inact}}$  for time  $t_{act}^c$  then
        add  $z$  to  $S_{I_{act}}$ 
        remove  $z$  from  $S_{I_{inact}}$ 
   $t \leftarrow t + \text{len}(t)$ 

```

respectively. Equation (2) in [39] gives the contact rate (C_R), which is the number of nodes j entering the area around node i that is bounded by r :

$$C_R = \frac{\rho r}{\pi} \int_0^{2\pi} (v_i^2 + v_j^2 - 2v_i v_j \cos \phi)^{1/2} d\phi. \quad (1)$$

Infection Spread Approximation. To approximate the total time of infection, we first compute the number of newly infected nodes at a given time step t . *Central Limit Theorem* is a probability theory that is stating that, if certain conditions are met, the distribution of the sample mean—after being standardized—tends toward a *normal distribution* as the sample size increases. Thus, the probability of newly infected nodes at a given time step t is estimated as follows:

$$f(t) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(t-\mu)^2}{2\sigma^2}}, \quad (2)$$

where μ is the mean and σ^2 is the variance of the distribution. Eq. 2 evaluates the probability density function at discrete time steps t . Therefore, to approximate the number of newly infected nodes at a given t , we calculate $f(t) \times N \times \text{len}(t)$, where $\text{len}(t)$ is the time step's interval width. To approximate the total infection spread at time t_n , we need to compute:

$$\sum_{i=1}^n f(t_i) \times N \times \text{len}(t_i). \quad (3)$$

Table 2 provides a summary of the notations.

5.2.2 Empirical Validation. To examine variability in D2D malware propagation, we conducted 10 simulation runs each for RWP and GAM mobility models, using different random seeds to vary node positions and trajectories. From each set, we selected the fastest, slowest, and median runs based on final infection time. Simulations included 100 mobile UEs, over 3,600s, moving at 1–5m/s, reflecting pedestrian and cyclist speeds. RWP was used in a 2000×2000m² open space, while GAM used the Helsinki map with configurable stop behavior. Key parameters are shown in Table 3.

Contact Rate Validation. If we assume that the nodes move with the average speed, i.e., $v_i = v_j = 3\text{m/s}$, then from Eq. 1 we obtain $C_R = \frac{100(150)}{2000(2000)\pi} \int_0^{2\pi} (3^2 + 3^2 - 18 \cos \phi)^{1/2} d\phi = 0.029$. Therefore, according to the theoretical formula in Equation 1, we expect approximately 3% of nodes to be in contact at any given time. For each mobility model, the simulation was repeated ten times,

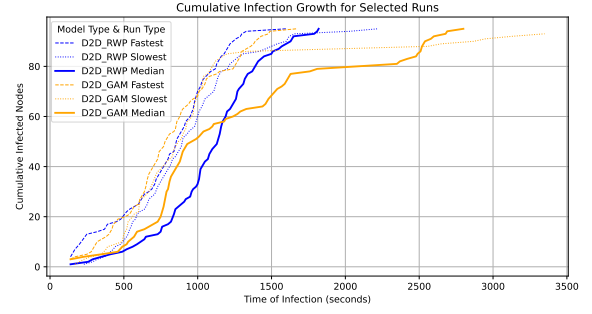


Figure 5: Cumulative Infection Growth for fastest, slowest, and median runs

and the median run was selected for analysis. We then sampled five random time snapshots: $t = 47.02, 88.97, 361.41, 592.21, 1178.24$ seconds. At each snapshot, we measured the number of active node-to-node connections, defined as connections that were previously established and still active at that time. The median number of active connections per node across these snapshots for **D2D GAM** and **D2D RWP** is 4.0 and 3.0 connections, respectively.

Infection Spread Approximation Validation. We present a baseline metric that highlights the overall infection behavior across the selected runs, Figure 5. The figure shows the cumulative infection growth over time for the fastest, slowest, and median runs. Now, let us, as an example, assume that we want to count the total number of newly infected nodes after 2000 seconds in the RWP model. If $\text{len}(t) = 50\text{sec}$, the mean infection time is $\mu = \frac{t_1+t_2+\dots+t_n}{n} = (50 + 100 + 150 + \dots + 2000)/40 = 1025$ and the variance is $\sigma^2 = 1/n \sum_{i=1}^n (t_i - \mu)^2 = 1/40 \sum_{i=1}^{40} (t_i - 1025)^2 = 333125$. Thus, from Formula 3, the number of total newly infected after 2000 seconds is $\sum_{i=1}^{40} f(t_i) \times 100 \times 50 = 91.7$. Since the simulation starts with 5 initially infected nodes, the total number of infected nodes is approximately 96.7, which closely aligns with the values observed in Figure 5 (92 infected UEs in 1800 sec in the RWP median run).

6 System Model Evaluation

This section presents the simulation scenario, experiment setup, and results used to evaluate the impact of D2D-based malware propagation and botnet-driven DDoS traffic on 5G network components. It details the simulated environment, including UE count and simulation duration, followed by the baseline configuration and test cases. The section concludes with key findings.

6.1 Simulation Scenario

All test cases use RWP mobility with a fixed random seed to isolate traffic load effects. This ensures consistency across experiments and allows observed variations in performance to be attributed solely to traffic-related factors. The network topology is based on a 2km × 2km urban area of Lund University's technical campus. This environment complements the RWP mobility model, reflecting the low-speed, unstructured movement typical of students and staff. The spatial scale allows unrestricted UE movement throughout the simulation, supporting realistic malware propagation dynamics.

Table 2: Summary of notations.

Notation	Description	Notation	Description
I_s	Susceptible	ϕ	The angle between the velocity vectors $\vec{V}_i$ and $\vec{V}_j$
I_{inact}	Infected Inactive	t_{act}^c	Time required for an inactive node to become active
I_{act}	Infected Active	N	The number of total population
$len(t)$	The duration of time step t	$T_{infection}$	The total infection delay
r	The communication radius	$dist(x, y)$	The Euclidean distance of two nodes x and y
S_{I_s}	The elements of this set are the nodes I_s	v_i and v_j	Speed of nodes i and j respectively
$S_{I_{inact}}$	The elements of this set are the nodes I_{inact}	C_R	The contact rate for a given node i
$S_{I_{act}}$	The elements of this set are the nodes I_{act}	ρ	The node density

Table 3: D2D malware propagation simulation parameters.

Parameter	Value
Number of UEs (N)	100
Initial Infected Nodes ($S_{I_{act}}$)	5
Susceptible Nodes (I_s)	95
Movement Speed Range (v_i)	1.0 – 5.0 m/s
Possible Movement Angle (ϕ)	[0, 360]
Sidelink Interface PC5 Communication Range (r)	150 meters
Malware Installation Delay (t_{act}^c)	20 seconds
Handshake Delay (DCR, TS 23.304 §6.4)	1 second
Malware Preparation Delay (UE/ProSe Layer-2 Link Establishment, TS 23.304 §6.4)	3 seconds
Malware Size	500 KB
Message TTL	300 seconds

The 5G setup includes 5 gNodeBs interconnected via X2 interfaces for handovers and coordination, with an intermediate UPF aggregating traffic before routing it through a core UPF to backend servers.

For analysis, we use UDP-based status update traffic modeled via a Constant Bit Rate (CBR) application. DDoS traffic reflects typical IoT botnet behavior, generating high-rate, low-overhead UDP packets that stress transport and core components. Although limited to a single service type, this controlled setup enables the repeatable and interpretable evaluation of infrastructure under load. All traffic operates at the IP layer, simulating the 5G user-plane in a typical enhanced Mobile Broadband (eMBB) scenario. A unified slice is used to reflect urban deployments where heterogeneous services share network resources.

While the framework does not impose a strict limit on the number of UEs, we selected configurations that balance computational efficiency during the simulation runs with realistic mobility and traffic patterns. Our baseline scenario includes 100 stationary UEs, while additional test cases evaluate up-to 500 UEs under varied mobility and traffic conditions. All UEs move at pedestrian or cyclist speeds. High-speed (vehicle speed) UEs are excluded due to their minimal network impact in this topology. Each simulation runs for 3,600 seconds (1 hour) to capture meaningful patterns in malware propagation and traffic behavior.

6.2 Experiment Setup

This section presents the experimental setup, including the base network configuration (Section 6.2.1) and the test scenarios (Section 6.2.2). Baseline performance is first evaluated under benign conditions. Then, mobility traces and infection metrics from the ONE simulator are used to control traffic behavior in each scenario, enabling evaluation of the impact on 5G core performance.

6.2.1 Baseline configuration. The baseline simulation is configured to reflect realistic 5G deployments under benign traffic conditions. As shown in Table 4, the network uses 10Gbps Ethernet (Eth10G) links and a large MTU. Each gNB and UE operates on a single 2GHz carrier with 2 RBs, using parameters consistent with 3GPP TS 38.214. Best-effort UDP traffic is generated at a low rate—100-byte packets every 5 seconds, emulating low-rate periodic traffic common in IoT telemetry applications (V2X), sensors, and wearables [22].

Although the current setup reflects a typical low-load scenario, the simulation framework is modular and configurable, allowing researchers to modify radio, transport, and traffic parameters to evaluate more demanding or adversarial configurations. For example, malicious UEs can be simulated to generate traffic at rates approaching 5Gbps, consistent with load patterns observed in real-world DDoS incidents [16].

Table 4: Base configuration parameters used in the Simu5G simulation environment.

Parameter	Value
Channel Rate / Delay	10 Gbps / 0.1 μ s
MTU (Maximum Transmission Unit)	10,000 bytes
Carrier Aggregation / Frequency / Bandwidth	1 component carrier per gnb and UE / 2 GHz / 2 Resource Blocks (RBs)
UE / gNB Transmit Power	26 dBm / 46 dBm (macrocell)
Target BLER	0.01 (shift: 5)
CQI Feedback Period	40 ms
Handover and Dynamic Cell Association	Enabled
CBR Application Type	CbrSender/CbrReceiver
CBR Packet Size / Interval	100 bytes (UE $\rightarrow$ Server), 100 bytes (Server $\rightarrow$ UE) / 1 second

6.2.2 Test Cases. We evaluate one baseline and three test cases, summarized in Table 5. The baseline scenario models static UEs with periodic benign traffic to establish reference traffic load and loss levels. TC001–TC002 increase mobility and load to observe benign stress behavior. TC003 simulate a DDoS scenario where infected UEs send 1000-byte packets every 10ms, mimicking high-rate UDP flooding attacks that strain L3/L4 layers⁵.

We monitor: (1) primary metrics: uplink data rate at the UPF and gNB, and (2) complementary metrics: uplink Radio Link Control (RLC) layer packet loss per UE. All simulation data and configurations are available at [6].

⁵<https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/>

Table 5: Overview of the evaluated test cases in DDoSimu5G.

Test Case	Scenario Description	Purpose	Parameter Choices Per TC	Expected Behavior
Baseline-TC: 100 UEs Stationary	100 UEs generate periodic CBR traffic while stationary.	Establish baseline for UPF/gNB throughput and reliability under static conditions.	UE mobility = stationary; UE count = 100	Stable and smooth traffic data rate with minimal packet loss.
TC001: 100 UEs Mobile	Same as TC001 with UE mobility as per traces from ONE simulator (RWP model).	Assess mobility impact on throughput and loss compared to TC001.	mobility = enabled; all other settings identical to TC001	Increased variability in data rate; slight RLC packet loss during handovers.
TC002: 100 UEs Mobile + 400 stationary UEs	100 UEs generate benign traffic from sim-start; additional stationary 400 UEs with same traffic load.	Observe the network under a higher benign traffic load.	UE count = 500; staggered traffic start; mobility = enabled	Network load peaks over time; UPF/gNB congestion may increase; packet loss localized to peak intervals.
TC003: D2D-Based UDP DDoS Flooding	100 UEs send 1000-byte packets every 10ms after being malicious as per D2D propagation model. With + 400 stationary benign UEs	Emulate DDoS behavior using realistic infection-driven activation; test impact on infrastructure.	Traffic rate and packet size increased after infection; activation controlled by infection traces; mobility = enabled	Significant increase in traffic rate at UPF/gNB; packet loss rises across UEs; signs of overload appear after infection propagation.

6.3 Simulation Results

In this section, the 5G network infrastructure is evaluated under benign and adversary traffic loads, based on Table 5. Our analysis considers infrastructure components namely, gNBs, UPF, and the connectivity between them via N3/N9 interfaces. This allows us to quantify how D2D-driven botnets manifest at the 5G user plane. To observe the observable degradation of service quality under adversarial stress, our evaluation focuses on throughput, delay, and packet loss.

Baseline-TC: In the baseline scenario, 100 stationary UEs generate periodic CBR traffic. Data rates at the UPF (266 kbps) and gNBs (max 130 kbps) remain stable throughout the simulation, with no packet loss. This confirms optimal link conditions and establishes a reference for data rate and service delivery reliability without mobility or congestion.

TC001: Enabling UE mobility on the 100 UEs in the test case introduces uplink rate variability and packet loss. Although data rates remain close to the baseline (UPF: 220–250 kbps (Figure 6a); gNBs: 90–130 kbps), short-term drops occur during handovers and weak signal periods. Due to the use of RLC Unacknowledged Mode (UM), packet loss increases moderately, as no retransmissions occur during transitions or signal degradation.

TC002: Scaling to 500 UEs increases network load but without significant packet loss on the added UEs. UPF data rate rises to 700–800 kbps (Figure 6b) and gNBs reach up to 300 kbps. While the added 400 UEs contribute to higher data rate, packet loss remains minimal (Figure 6d), indicating that the infrastructure absorbs larger benign loads without congestion under current capacity limits.

TC003: UDP flooding DDoS scenario causes a sharp increase in network traffic. UPF data rates rise nearly linearly with botnet size, peaking at 8–10 Mbps (Figure 6c), while benign UEs experience a 7× increase in packet loss (Figure 6d). A per-layer trace of a single benign UE (499), shown in Table 6, illustrates how retransmissions within the encapsulated GTP-U lower layers contribute to the observed packet loss. These retransmissions arise not from degraded radio conditions, as the average SINR remains stable, but from delayed scheduling grants at the gNB, where infected UEs monopolize uplink time slots. The gNB’s allocation of wireless resources via Physical Resource Blocks (PRBs) exhibits clear congestion, with the uplink queue bit length increasing sharply from 1,300 bits in TC002 to over 8,000 bits and peaking around 12,000 bits in TC003, thereby

Table 6: Per-layer transmission statistics for UE-499 under benign (TC002) and DDoS (TC003) scenarios.

Layer	TC002	TC003	Observation
PDCCP (UDP packets)	3,599	3,599	Same offered load
RLC → MAC	8,077	32,839	4× more retransmissions
MAC → PHY	14,043	174,880	12× more PDUs
HARQ Attempts	8,077	32,834	4× increased retries

Table 7: ONE Simulator - D2D Malware Propagation. Performance vs. number of UEs.

UEs	Wall (s)	CPU time (s)	%CPU	Peak RSS (MB)
100	2.5–2.7	6.5–7.0	257–260%	409–439
500	45–61	52–68	111–116%	452–457
1000	201–242	212–253	104–105%	512–523

limiting scheduling capacity for benign users. Consequently, benign UEs experience longer waiting times in the RLC buffer due to expired HARQ timers and missed scheduling windows.

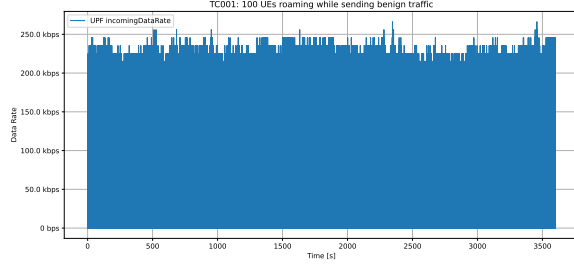
6.4 Framework Performance and Scalability

All experiments were executed on a Z370 AORUS Ultra system (Intel i7-8700K with 6 cores, 32GB DDR4 RAM, GTX 1060 6GB).

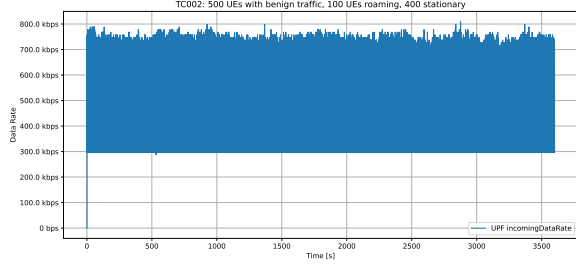
Performance. We measured the execution cost of both simulators under increasing UE counts. Table 7 reports the ONE Simulator, where runtime grows superlinearly (multi-threaded) with N while peak memory increases only modestly.

Table 8 reports the Simu5G scenarios, where simulations are consistently CPU-bound ($\approx 99\%$ CPU). For Simu5G, mobility adds a moderate overhead (A→B: +58% wall time, +40% memory), additional stationary UEs significantly extend runtime (B→C: 6.2× wall time, 0.63 GB memory), and higher traffic load nearly doubles runtime (C→D: 1.7× wall time, 2.1 GB memory).

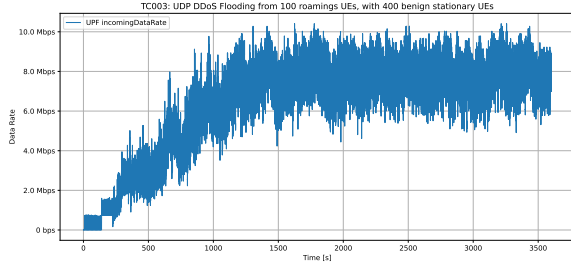
Scalability. Across both ONE and Simu5G, the results show that memory usage scales gently and approximately linearly with the number of UEs in both simulators, remaining within workstation limits even at 1000 UEs (1–3 GB depending on traffic intensity). While simulation runtime does not scale linearly, in ONE, it grows almost quadratically as the number of UEs increases, whereas in



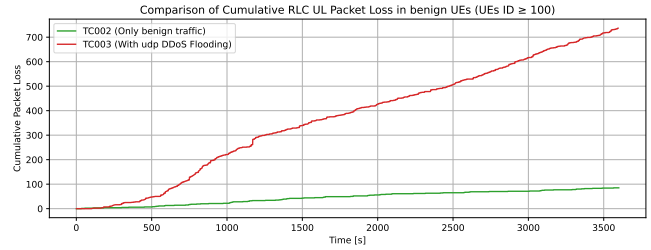
(a) UPF uplink data rate with 100 mobile UEs. Data rate fluctuating between 220–250 kbps with minor due to mobility-induced handovers.



(b) UPF uplink data rate with 500 UEs. Aggregate data rate increases to 700–800 kbps with slight fluctuations, showing resilience under scaled benign traffic.



(c) UPF uplink data rate under D2D-based udp DDoS flooding. Botnet-driven traffic causes sharp increases peaking near 9–10 Mbps, indicating network strain.



(d) Comparison of total packet loss across benign UEs (IDs 100–499) in TC002 vs. TC003. DDoS scenario shows a 7× increase in packet loss due to infrastructure congestion.

Figure 6: UPF data rate and packet loss under varying mobility, user density, and DDoS conditions.

Table 8: Simu5G – per-scenario performance.

Scenario	UEs	Wall & CPU (s)	%CPU	RSS (MB)
A) Baseline-TC	100	868	99%	213
B) TC001	100	1373	99%	305
C) TC002	500	8554	99%	634
D) TC003	500	14845	99%	2085

Simu5G it escalates rapidly with both UE population and traffic intensity. While CPU utilization saturates near 100%, meaning execution is compute-bound rather than memory-bound. Extrapolating to 1000 UEs suggests runtimes of several hours in Simu5G (4–7 h depending on load) and hundreds of seconds in ONE, highlighting CPU execution time as the limiting factor. Thus, large experiments are best managed by parallel batch execution, which scales throughput linearly with available cores so long as sufficient memory is available.

7 Discussion

This study, though conducted in a controlled simulation environment, provides transferable insights into 5G network behavior under adversarial conditions. Results show that even power-constrained CIoT devices can still generate short, intense traffic bursts capable of stressing critical infrastructure components such as the UPF and gNB.

The results show that benign traffic scaled predictably with mobility and user density, whereas botnet-driven traffic introduced nonlinear stress patterns, causing a 30× increase in UPF data rate and a 7× rise in benign UE packet loss. The increase in packet loss is partly attributed to the simulated cells being configured with only two PRBs and a simplified fair-sharing scheduler, a reduction imposed by runtime constraints. Nevertheless, the qualitative behavior of 5G networks under DDoS load remains unchanged, as increasing the number of PRBs would raise capacity, but with proportionally larger benign and adversarial traffic, similar congestion patterns would still emerge, reflecting how D2D-propagated DDoS traffic strains network infrastructure and degrades service quality for users.

DDoSImu5G contributes a modular and extensible framework that integrates a 3GPP-aligned D2D malware propagation and traffic generation 5G simulation environment. Its flexible configuration supports diverse mobility models, infection dynamics, and traffic profiles, enabling reproducible testing of emerging adversarial behaviors and defensive strategies.

We acknowledge that real 5G deployments vary widely by operator configuration, infrastructure topology, and user density. The presented simulations aim to capture general trends rather than emulate a specific network. Variability across deployments implies that these findings should inform trend-based understanding and resilience assessment rather than exact performance prediction. Ethical constraints also preclude experimentation with live 5G

infrastructure, highlighting the value of simulation-based methodologies, such as DDoSimu5G, for the safe evaluation of high-impact attack scenarios.

8 Conclusions and Future Work

We introduced DDoSimu5G, a simulation framework that combines D2D malware propagation with end-to-end 5G traffic load measurements. The framework enables analysis of how DDoS malware-driven traffic impacts core network components. Test cases show predictable scaling under benign loads and nonlinear degradation under attack. DDoSimu5G supports reproducible analysis of 5G attacks and invites extension by the research community.

In future work, we aim to expand the framework's traffic profiles to generate richer datasets for studying detection, mitigation, and 5G resilience under mixed benign and malicious conditions.

References

- [1] 2025. *3GPP TS 23.304 V19.5.0: Proximity-based services (ProSe); Stage 2*. Technical Report TS 23.304 V19.5.0. 3rd Generation Partnership Project (3GPP). https://www.3gpp.org/ftp/Specs/archive/23_series/23.304/ Section 6.4: 5G ProSe Direct Communication.
- [2] 2025. *3GPP TS 33.503 V19.2.0: Security for 5G System; Proximity Services (ProSe)*. Technical Report TS 33.503 V19.2.0. 3rd Generation Partnership Project (3GPP). https://www.3gpp.org/ftp/Specs/archive/33_series/33.503/ Version 19.2.0, September 2025.
- [3] Asma Al Kindi, Dawood Al Abri, Ahmed Al Maashri, and Fahad Bait-Shiginah. 2019. Analysis of malware propagation behavior in Social Internet of Things. *International Journal of Communication Systems* 32, 15 (2019), e4102.
- [4] Josue Genaro Almaraz-Rivera, Jesus Arturo Perez-Diaz, Jose Antonio Cantoral-Ceballos, Juan Felipe Botero, and Luis A. Trejo. 2022. Toward the Protection of IoT Networks: Introducing the LATAM-DDoS-IoT Dataset. *IEEE Access* 10 (2022), 106909–106920. doi:10.1109/ACCESS.2022.3211513
- [5] Marios Anagnostopoulos, Georgios Kambourakis, and Stefanos Gritzalis. 2016. New facets of mobile botnet: architecture and evaluation. *International Journal of Information Security* 15 (2016), 455–473.
- [6] Anonymous. 2025. DDoSimu5G: Simulation Framework for Malware Propagation and DDoS Attacks in 5G Networks. Code and configurations available at an anonymized repository link during review.
- [7] Anonymous. 2025. Resilient Automatic Model Selection for Mobility Prediction. (2025). Accepted in Cluster Computing, 2025. Under double-blind review.
- [8] Nils Aschenbruck, Raphael Ernst, Elmar Gerhards-Padilla, and Matthias Schwamborn. 2010. BonnMotion: a mobility scenario generation and analysis tool. In *Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques* (Torremolinos, Malaga, Spain) (SIMUTools '10). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, Article 55, 10 pages. doi:10.4108/ICST.SIMUTOOLS2010.8684
- [9] Ziyad Benomar, Chaima Ghribi, Elie Cali, Alexander Hinsén, and Benedikt Jahnel. 2022. Agent-based Modeling and Simulation for Malware Spreading in D2D Networks. In *Proceedings of the 21st International Conference on Autonomous Agents and Multiagent Systems* (Virtual Event, New Zealand) (AAMAS '22). International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 91–99.
- [10] Sulabh Bhattarai, Stephen Rook, Linqiang Ge, Sixiao Wei, Wei Yu, and Xinwen Fu. 2014. On simulation studies of cyber attacks against LTE networks. In *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*. IEEE, Piscataway, NJ, 1–8. doi:10.1109/ICCCN.2014.6911737
- [11] Conrado Boeira, Antor Hasan, Khaleda Papry, Yue Ju, Zhongwen Zhu, and Israat Haque. 2024. A Calibrated and Automated Simulator for Innovations in 5G. *arXiv e-prints* (2024), arXiv–2404.
- [12] Elie Cali, Alexander Hinsén, Benedikt Jahnel, and Jean-Philippe Wary. 2024. Chase–escape in dynamic device-to-device networks. *Journal of Applied Probability* 61, 1 (2024), 311–339.
- [13] Kok Onn Chee, Mengmeng Ge, Guangdong Bai, and Dan Dongseong Kim. 2024. IoTSecSim: A framework for modelling and simulation of security in Internet of things. *Computers & Security* 136 (2024), 103534.
- [14] Bo-Rui Chen, Shin-Ming Cheng, and Maina Bernard Mwangi. 2022. A mobility-based epidemic model for IoT malware spread. *IEEE Access* 10 (2022), 107929–107941.
- [15] Kaiwen Chi, Xiaohui Xie, Yanning Hu, Dongyang Zhao, Yuming Xie, Liang Zhang, and Yong Cui. 2024. E-DDoS: An Evaluation System for DDoS Attack Detection. In *2024 IEEE 32nd International Conference on Network Protocols (ICNP)*. 1–6. doi:10.1109/ICNP61940.2024.10858578
- [16] Cisco Systems. 2021. UPF Reporting of Load Control over N4 Interface. https://www.cisco.com/c/en/us/td/docs/wireless/ucc/upf/2021-01/b_ucc-5g-upf-config-and-admin-guide_2021-01/m_upf-reporting-of-load-control-over-n4-interface.pdf. Accessed: 2024-05-22.
- [17] Andrei Costin and Jonas Zaddach. 2018. Iot malware: Comprehensive survey, analysis framework and case studies. *BlackHat USA* 1, 1 (2018), 1–9.
- [18] Jie Dou, Gang Xie, Zhiyi Tian, Lei Cui, and Shui Yu. 2024. Modeling and Analyzing the Spatial–Temporal Propagation of Malware in Mobile Wearable IoT Networks. *IEEE Internet of Things Journal* 11, 2 (2024), 2438–2452. doi:10.1109/JIOT.2023.3295016
- [19] Gints Engelen, Vera Rimmer, and Wouter Joosen. 2021. Troubleshooting an intrusion detection dataset: the CICIDS2017 case study. In *2021 IEEE Security and Privacy Workshops (SPW)*. IEEE, 7–12.
- [20] Paolo Farina, Enrico Cambiaso, Gianluca Papaleo, and Maurizio Aiello. 2016. Are mobile botnets a possible threat? The case of SlowBot Net. *Computers & Security* 58 (2016), 268–283.
- [21] Jan Feng, Bing-Kai Hong, and Shin-Ming Cheng. 2020. DDoS Attacks in Experimental LTE Networks. In *Web, Artificial Intelligence and Network Applications*, Leonard Barolli, Flora Amato, Francesco Moscato, Tomoya Enokido, and Makoto Takizawa (Eds.), Springer International Publishing, Cham, 545–553.
- [22] GSMA. 2022. *Improving Energy Efficiency for Mobile IoT*. White paper. GSM Association. <https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2022/02/2022.03-GSMA-Energy-Efficiency-for-Mobile-IoT-1.pdf>
- [23] Hanan Hindy, David Brosset, Ethan Bayne, Amar Kumar Seeam, Christos Tachatzis, Robert Atkinson, and Xavier Bellekens. 2020. A taxonomy of network threats and the effect of current datasets on intrusion detection systems. *IEEE Access* 8 (2020), 104650–104675.
- [24] Ari Keränen, Jörg Ott, and Teemu Kärkkäinen. 2009. The ONE simulator for DTN protocol evaluation. In *Proceedings of the 2nd International Conference on Simulation Tools and Techniques* (Rome, Italy) (SimuTools '09). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, Article 55, 10 pages. doi:10.4108/ICST.SIMUTOOLS2009.5674
- [25] Asem Kitana, Issa Traore, and Isaac Woungang. 2016. Impact Study of a Mobile Botnet over LTE Networks. *Journal of Internet Services and Information Security (JISIS)* 6, 2 (2016), 1–22.
- [26] Nickolaos Koroniotis, Nour Moustafa, Elena Sitnikova, and Benjamin Turnbull. 2019. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems* 100 (2019), 779–796. doi:10.1016/j.future.2019.05.041
- [27] Katina Kravlevska, Michele Garau, Mathias Førlund, and Danilo Gligoroski. 2019. Towards 5g intrusion detection scenarios with omnet++. *Proceedings of 6th International OM* 66 (2019), 44–51.
- [28] Bo Liu, Wanlei Zhou, Longxiang Gao, HaiBo Zhou, Tom H Luan, and Sheng Wen. 2016. Malware propagations in wireless ad hoc networks. *IEEE Transactions on Dependable and Secure Computing* 15, 6 (2016), 1016–1026.
- [29] Massimiliano Luca, Gianni Barlacchi, Bruno Lepri, and Luca Pappalardo. 2021. A survey on deep learning for human mobility. *ACM Computing Surveys (CSUR)* 55, 1 (2021), 1–44.
- [30] Ola Malkawi, Nadim Obaid, and Wesam Almobaideen. 2024. Intrusion Detection System for 5G Device-to-Device Communication Technology in Internet of Things. *Informatica* 48, 15 (2024).
- [31] Ana Serrano Mamolar, Zeeshan Pervez, Qi Wang, and Jose M. Alcaraz-Calero. 2019. Towards the Detection of Mobile DDoS Attacks in 5G Multi-Tenant Networks. In *2019 European Conference on Networks and Communications (EuCNC)*. IEEE, Piscataway, NJ, 273–277. doi:10.1109/EuCNC.2019.8801975
- [32] Nour Moustafa and Jill Slay. 2015. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 Military Communications and Information Systems Conference (MilCIS)*. 1–6. doi:10.1109/MilCIS.2015.7348942
- [33] Giovanni Nardini, Dario Sabella, Giovanni Stea, Purvi Thakkar, and Antonio Virdis. 2020. Simu5g—an omnet++ library for end-to-end performance evaluation of 5g networks. *IEEE Access* 8 (2020), 181176–181191.
- [34] Islam Obaidat, Zachary Palko, and Meera Sridhar. 2023. From DDoSim to DDoSimQ: Enhancing DDoS Attack Simulations Through Full System Emulation. In *Proceedings of the 5th Workshop on CPS&IoT Security and Privacy*. Association for Computing Machinery, New York, NY, USA, 37–37. doi:10.1145/3605758.3623501
- [35] Jared M. Peterson, Joffrey L. Leevy, and Taghi M. Khoshgoftaar. 2021. A Review and Analysis of the Bot-IoT Dataset. In *2021 IEEE International Conference on Service-Oriented System Engineering (SOSE)*. 20–27. doi:10.1109/SOSE52839.2021.00007
- [36] Suranga Prasad, Pramod Munaweera, Tharaka Hewa, Yushan Siriwardhana, and Mika Yliniittä. 2025. Simulation of IIoT-Driven Attack Vectors on 5G Core Networks: Dataset Generation and Machine Learning Based Detection (IoT '24). Association for Computing Machinery, New York, NY, USA, 184–187.

- doi:10.1145/3703790.3703815
- [37] S.V. Jansi Rani, Iacovos Ioannou, Prabagarane Nagaradjane, Christophoros Christophorou, Vasos Vassiliou, Sai Charan, Sai Prakash, Niel Parekh, and Andreas Pitsillides. 2023. Detection of DDoS attacks in D2D communications using machine learning approach. *Computer Communications* 198 (2023), 32–51. doi:10.1016/j.comcom.2022.11.013
 - [38] S. V. Jansi Rani, Iacovos I. Ioannou, Prabagarane Nagaradjane, Christophoros Christophorou, Vasos Vassiliou, Harshita Yarramsetti, Sai Shridhar, L. Mukund Balaji, and Andreas Pitsillides. 2023. A Novel Deep Hierarchical Machine Learning Approach for Identification of Known and Unknown Multiple Security Attacks in a D2D Communications Network. *IEEE Access* 11 (2023), 95161–95194. doi:10.1109/ACCESS.2023.3308036
 - [39] CJ Rhodes and RM Anderson. 2008. Contact rate calculation for a basic epidemic model. *Mathematical biosciences* 216, 1 (2008), 56–62.
 - [40] George F Riley and Thomas R Henderson. 2010. The ns-3 network simulator. In *Modeling and tools for network simulation*. Springer, 15–34.
 - [41] Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani. 2019. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In *2019 International Carnahan Conference on Security Technology (ICCST)*. IEEE, Piscataway, NJ, 1–8. doi:10.1109/CCST.2019.8888419
 - [42] Shigen Shen, Haiping Zhou, Sheng Feng, Jianhua Liu, and Qiyang Cao. 2019. SNIRD: Disclosing rules of malware spread in heterogeneous wireless sensor networks. *IEEE Access* 7 (2019), 92881–92892.
 - [43] Antonio Virdis and Michael Kirsche. 2019. Recent advances in network simulation. *EAI/Springer Innovations in Communication and Computing* (2019).
 - [44] Matthias Wichtlhuber, Eric Strehle, Daniel Kopp, Lars Prepens, Stefan Stegmüller, Alina Rubina, Christoph Dietzel, and Oliver Hohlfeld. 2022. IXP scrubber: learning from blackholing traffic for ML-driven DDoS detection at scale. In *Proceedings of the ACM SIGCOMM 2022 Conference* (Amsterdam, Netherlands) (SIGCOMM '22). Association for Computing Machinery, New York, NY, USA, 707–722. doi:10.1145/3544216.3544268
 - [45] Wenhao Wu, Zhenyu Li, Xilai Liu, Zhaohua Wang, Heng Pan, Guangxing Zhang, and Gaogang Xie. 2025. Lemon: Network-Wide DDoS Detection with Routing-Oblivious Per-Flow Measurement. In *Proceedings of the 34th USENIX Security Symposium (USENIX Security 25)*. USENIX Association, Seattle, WA, USA. <https://www.usenix.org/conference/usenixsecurity25/presentation/wu-wenhao>
 - [46] Muhammad Zeeshan, Qaiser Riaz, Muhammad Ahmad Bilal, Muhammad K. Shahzad, Hajira Jabeen, Syed Ali Haider, and Azizur Rahim. 2022. Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets. *IEEE Access* 10 (2022), 2269–2283. doi:10.1109/ACCESS.2021.3137201