Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Quantifying the Impact of Stealthy BLE Spam & Flooding Attacks on IoT Environments

Usman Rauf

urauf@mercy.edu

Mercy University

Adalynn Martinez

Mercy University

Fadi Mohsen

University of Groningen

Research Article

Keywords: Bluetooth Low Energy, Internet of Things, IoT security, wireless attacks, stealthy attacks, low energy protocols

Posted Date: June 22nd, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9728198/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Quantifying the Impact of Stealthy BLE Spam & Flooding Attacks on IoT Environments

Usman Rauf[1*], Adalynn Martinez[1] and Fadi Mohsen[2]

[1*]Department of Computer Science, Mercy University, Dobbs Ferry, NY, USA.

[2]Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence,University of Groningen, Groningen, The Netherlands.

*Corresponding author(s). E-mail(s): urauf@mercy.edu;
Contributing authors: amartinez@mercy.edu; f.f.m.mohsen@rug.nl;

Abstract

The energy-efficient design of the BLE protocol, emphasis on rapid, and user-friendly discovery, making it an ideal choice for IoMTs, specifically, military field medical systems, and battlefield wearable sensors. Especially in active conflict zones, when static medical facilities are vulnerable and often targeted, limiting their viability for sustained care delivery. This rapid deployment, and ease of management comes at the cost of expanded attack surface, i.e., BLE flooding attacks. During such attacks, adversaries flood advertisement channels with unauthorized connection or advertising requests to exhaust nearby device resources and disrupt legitimate communication, sometimes culminating in denial-of-service conditions. A first public proof-of-concept of such attacks, using a Raspberry Pi has since been adapted to commodity platforms (e.g., Flipper Zero, HackRF, Android), lowering the barrier to attack. In contested environments, such platforms are directly relevant to adversarial RF jamming and spoofing operations, where low-cost, portable devices can induce disproportionate disruption in dense wireless ecosystems. In this work, we develop a quantitative foundation for understanding the impact of such attacks and propose a practical deterrence strategy based on agility to raise the cost of such attacks. Our main contributions include: (1) formalization of this problem as a finite resource stochastic system with dynamic adversarial capabilities under diverse scenarios (e.g., single/multiple & static/agile attackers), identifying bounds where disruption becomes likely. (2) We also synthesize agility parameters for adaptive deterrence that can lead to the development of actionable guidance for implementers and standards bodies (Bluetooth Interest Group) seeking to harden BLE stacks and preserve the reliability of dense IoT ecosystems. (3) Our

third contribution is the cross-validation of our proposed stochastic model with a real-life test bed by implementing several attack scenarios. (4) Our last and main contribution includes the development of integrated agility based framework to neutralize BLE based threat.

Keywords: Bluetooth Low Energy, Internet of Things, IoT security, wireless attacks, stealthy attacks, low energy protocols

1 Introduction

The energy-efficient design of the BLE protocol, emphasis on rapid, and user-friendly discovery, making it an ideal choice for IoMTs, specifically, military field medical systems, and battlefield wearable sensors. Especially in active conflict zones, when static medical facilities are vulnerable and often targeted, limiting their viability for sustained care delivery. This rapid deployment, and ease of management comes at the cost of expanded attack surface, i.e., BLE flooding attacks. During such attacks, adversaries flood advertisement channels with unauthorized connection or advertising requests to exhaust nearby device resources and disrupt legitimate communication, sometimes culminating in denial-of-service conditions. A first public proof-of-concept of such attacks, using a Raspberry Pi has since been adapted to commodity platforms (e.g., Flipper Zero, HackRF, Android), lowering the barrier to attack. In contested environments, such platforms are directly relevant to adversarial RF jamming and spoofing operations, where low-cost, portable devices can induce disproportionate disruption in dense wireless ecosystems. In this work, we develop a quantitative foundation for understanding the impact of such attacks and propose a practical deterrence strategy based on agility to raise the cost of such attacks. Our main contributions include: (1) formalization of this problem as a finite resource stochastic system with dynamic adversarial capabilities under diverse scenarios (e.g., single/multiple & static/agile attackers), identifying bounds where disruption becomes likely. (2) We also synthesize agility parameters for adaptive deterrence that can lead to the development of actionable guidance for implementers and standards bodies (Bluetooth Interest Group) seeking to harden BLE stacks and preserve the reliability of dense IoT ecosystems. (3) Our third contribution is the cross-validation of our proposed stochastic model with a real-life test bed by implementing several attack scenarios. (4) Our last and main contribution includes the development of integrated agility based framework to neutralize BLE based threat.

Bluetooth Low Energy (BLE) protocol has become a cornerstone technology for modern wireless communication, enabling connectivity across a wide range of applications, including personal gadgets, smart home systems, industrial automation, and healthcare. Its widespread adoption is due to its energy efficiency, ease of use, quick deployment, and rapid device discovery. Though the emphasis on ease of use and quick deployment has inadvertently expanded the attack surface, exposing vulnerabilities that adversaries can exploit. For example, BLE's minimum energy consumption

and rapid device discovery are achieved via the reliance on lightweight advertising exchanges across three dedicated channels (37, 38, 39). This architecture proved effective for connecting wearables and peripherals, but has also left discovery and advertising as relatively unprotected operations [1]. Another example is the use of BLE-enabled sensors in healthcare. Remote monitoring systems rely on these sensors to deliver continuous and reliable updates, critical to relay vital signs and trigger timely responses[2]. Although these BLE-enabled sensors are vulnerable to adversarial manipulation, security surveys highlight that attacks such as energy drain and denial of service, targeting advertising or mesh communication, can greatly impair the reliability of these devices. This raises concerns regarding clinical safety and monitoring in dense IoMT environments[3].

In military and contested operational environments, the role of BLE-enabled IoMT systems becomes even more critical. Battlefield medical support increasingly relies on wearable sensors, portable monitoring systems, and ad hoc telemedicine platforms to provide real-time patient data in the absence of stable infrastructure. Unlike traditional healthcare settings, these systems operate in dynamic and adversarial RF environments where communication channels are inherently exposed. Static medical facilities and centralized infrastructure may be infeasible due to their susceptibility to targeting, necessitating decentralized and wireless-dependent solutions[4]. This reliance on BLE introduces a unique vulnerability: the same lightweight, unauthenticated advertising mechanisms that enable rapid deployment also expose these systems to disruption through low-cost RF interference, jamming, and spoofing. As a result, even resource-constrained adversaries equipped with commodity platforms can degrade or deny critical medical communication, amplifying the operational impact of BLE-based attacks beyond conventional IoT scenarios.

An emerging threat in this landscape is the BLE spam/flooding attack, which leverages BLE advertisement channels to flood nearby devices with unauthorized connection requests. These attacks can disrupt normal device operations, degrade user experience, and, in severe cases, lead to denial-of-service (DoS) conditions [5]. Furthermore, adversaries can manipulate BLE spams to interfere with legitimate communication, exploit device behavior, or facilitate other malicious activities. As the adoption of BLE-enabled devices continues to increase, understanding the feasibility, impact, and mitigation of such attacks is critical to securing the IoT ecosystem.

Despite ongoing research on BLE security, the study of BLE flooding attacks remains in its early stages, with limited assessments of their practical implications. The first proof-of-concept for this attack vector was demonstrated in 2023 using a Raspberry Pi equipped with a Bluetooth adapter and an external antenna [6]. Since then, it has been adapted for use on various platforms, including Flipper Zero, HackRF, and even Android applications, making it increasingly accessible to attackers[7–9]. BLE advertisements, as a fundamental component of device discovery and connectivity, inherently lack authentication or pairing requirements, rendering them particularly susceptible to exploitation.

To address these gaps, this paper presents a quantitative method to understand the repercussions of such attacks using a stochastic modeling approach. We examine the feasibility and impact of these attacks by evaluating key parameters such as device

duty cycles, spam transmission rates, and multiattacker scenarios. Furthermore, we investigate adversarial strategies to maximize disruption and assess mitigation techniques, including dynamic countermeasures where BLE devices adaptively adjust their behavior in response to spam attacks. Finally, we conduct an experimental analysis of real-world BLE spam traffic, providing insights on the characteristics of the attack and potential defense mechanisms. Demonstrating that sustained spam bursts can overwhelm BLE devices and degrade nearby IoT activity, underscoring the practical risks that motivate both our stochastic analysis and the evaluation of adaptive defenses.

Road-map:

The remainder of this paper is structured as follows: Section 2 reviews related work. Section 3 outlines our formalization and modeling methodology. Section 4 presents our feasibility and impact analysis of the attack. Section 5 shows the empirical analysis. Section 6 presents agility and formal methods based defense framework the neutralize persistent threats. Finally, we conclude the paper in Section 7.

2 Related Work

The research landscape relevant to traffic degradation in Internet of Medical Things (IoMT) networks under adversarial BLE activity can be grouped into three streams: (i) modeling efforts that quantify network-quality deterioration, (ii) public BLE datasets, and (iii) attack-analysis and detection frameworks.While each category contributes distinct insights, we emphasize modeling efforts as the most aligned with our goals of capturing adversarial behavior under dynamic conditions. The other two streams offer useful support material but do not engage directly with attacker–defender modeling.

To structure this review, we organize prior work according to nine modeling capabilities that help distinguish their relevance to attacker–defender dynamics in BLE environments. *Protocol* specifies the communication layer or network context in which the model operates. *Attack Type* identifies whether adversarial behavior is captured and specifies the forms represented (e.g., DoS, MITM). *Attacker Profiling* denotes the degree to which adversaries are behaviorally characterized, such as by aggression level or operational strategy. *Behavioral Dynamics* considers how interdependent behaviors evolve, for example, the relationship between spam rate and scanning duty cycles. *Agent Agility* evaluates whether agents (attacker or defender) can adapt strategies in response to environmental conditions. *Impact Estimation* assesses whether the consequences of attacks on system performance or communication quality are explicitly quantified. *Model Validation* denotes the degree to which predicted behavioral patterns are cross-validated through experimental setups or controlled testbeds, thereby linking theoretical models to observed evidence. *Engagement Dynamics* examines the diversity of modeled interaction scenarios, including static–static, agile–static, and agile–agile matchups. Finally, *Focus* indicates the primary analytical or operational goal, such as device localization, threshold-based detection, or behavior-based threat modeling.

Capability	Halloush & Liu [10]	Zhang et al. [11]	Shanbhag et al. [12]	Kavousi Ghafi et al. [13]	Bhunia et al. [14]	Allouzi & Khan [15]	Our Behavioral Model
Protocol	Smart Grid / Generic Wireless	UAV	Cognitive Radio / WSN	BLE Coexistence (WLAN/BLE)	Cognitive Radio Networks	IoMT Edge Networks	BLE
Attack Type	Jamming (DoS)	Stealthy Jamming	Adaptive Jamming	✗	Jamming (DoS)	DoS, Spoofing, Malware, etc.	DoS, Adaptive Spam
Attacker Profiling	Partial (2 operational types)	Partial (Hidden jammed/unjammed states)	✓	✗	✗ (Beyond paper scope)	✗	✓
Behavioral Dynamics	✓	✓ (Timing States)	✓	✗	✗ (Beyond paper scope)	✗	✓
Agent Agility	Partial (Defender)	✗ (Detection Only)	Partial (adaptive attacker)	✗	Partial (honeypot defense dynamics)	✗	✓
Impact Estimation	✓	✗	Partial (total error probability)	✓ (BER/PER under interference)	✓	Partial (threat likelihood distribution)	✓
Model Validation	Testbed cross-validation	Simulation-based	Simulation-based	IQ & spectrum traces	Simulation-based	Simulation-based with CVSS probabilities	Testbed cross-validation
Engagement Dynamics	Limited (single jammer)	Limited (single link/jammer)	Limited (single attacker; adaptive attacker vs static victim)	✗	Limited (attacker static)	✗	✓
Focus	QoS under Jamming	Detection of Stealthy Jamming	Adaptive Adversary Strategy	Co-Channel Intelligent Interference	Anti-jamming with Honeypot	Threat Likelihood Estimation	Behavior-based Threat Modeling

Table 1: Summary of prior modeling efforts across wireless domains versus our BLE spam model, emphasizing outcome granularity and validation approach.

Modeling efforts for network-quality deterioration: Prior work across wireless domains has explored stochastic and queueing-theoretic models to quantify degradation caused by interference or malicious behavior. Table 1 presents our analysis of these efforts with respect to the nine modeling capabilities introduced.

As shown in Table 1, most prior models focus on jamming in various wireless networking contexts. Yet comparable work for BLE remains sparse. While many identify denial-of-service (DoS) as an attack type, few attempt *attacker profiling* or capture fine-grained *behavioral dynamics*. In particular, attributes such as *agent agility* and *engagement dynamics* are largely missing. Such treatments overlook adaptive adversaries and do not link attacker send rates or duty-cycle exploitation to system-level degradation.

Stochastic abstractions have been employed to model the impact of interference on quality-of-service (QoS) in wireless communication environments. One example, introduced by Halloush and Liu is a semi-Markov process (SMP) to model jamming-resilient systems, enabling derivation of availability metrics and packet loss probabilities under varying levels of adversarial intensity[10]. Similarly, Bhunia et al. introduced a queuing-theoretic model for cognitive radio networks incorporating honeypot-based defenses to analyze the effects of jamming on packet delays and loss[14]. While both models illustrate the feasibility of quantifying long-term service degradation, their analyses remain confined to coarse-grained QoS metrics. They do

not directly link interference conditions to outcomes in device discovery or session outcomes.

To capture stealth and adaptivity, learning-based and state-driven approaches extend this line of work. Zhang et al. apply a hidden Markov model (HMM) to detect low-rate jamming in UAV-assisted wireless networks, inferring adversarial behavior from received energy traces[11]. Shanbhag et al. adopt a Markov decision process (MDP) framework to capture adaptive jamming strategies that evolve through environmental feedback[12]. Although these approaches highlight the agility of the attacker and his behavioral dynamics, they primarily report performance in terms of detection accuracy or the efficiency of the attacker's policy, rather than the impact on system-level services.

Efforts more closely aligned with BLE include the work of Kavousi Ghafi et al., who developed measurement-driven interference models using IQ-domain and spectral traces. Their study characterizes packet error rates under co-channel interference from BLE and WLAN sources, demonstrating that interference effects can be captured with high statistical fidelity [13]. However, the scope remains centered on coexistence challenges rather than deliberate adversarial behavior.

Allouzi and Khan contributed a Markov-chain-based modeling framework for IoMT edge networks, estimating attack transition probabilities based on device vulnerabilities and CVSS scores[15]. This work illustrates how stochastic state transitions can effectively represent diverse attack vectors in medical environments. Yet the analysis is broad, covering spoofing, DoS, and malware, without attention to BLE-specific broadcast channels. Specifically, it focuses on the probability of various threat occurrences rather than assessing the capabilities of the attacker.

Public BLE datasets: BLE datasets offer valuable empirical support for tasks such as device classification and anomaly detection. However, they offer limited support for adversarial modeling. BLEBeacon [16], SDR4IoT [17], Bouaru et al. university exam captures [18], and CICIoMT2024 [19] consist primarily of benign traffic. Only minimal adversarial content is observed in CICIoMT2024. Crucial features, such as *attacker profiling*, *agent agility*, and *engagement dynamics*, are either absent or heavily abstracted. BlueTack [20] (see also [21]) is a partial exception, compared to the previous datasets, for IDS evaluation in IoMT. The dataset centers on DoS and MITM scenarios, but the attack traces are aggregated into fixed time windows, limiting analysis of fine-grained behavioral dynamics. As a result, the data cannot directly capture agent agility or reveal engagement dynamics.

Attack-analysis and detection frameworks: Protocol and system analyses advance state-aware checking, robustness testing, and target-side safeguards. This includes tools and studies such as BlueSWAT [22], BLESS [23], BLEdiff [24], formal-model–driven discovery [25], and security testing frameworks [26]. These resources document or emulate *attack types* (e.g., misconfiguration abuse, DoS, or state disruption) and provide *model validation* via testbeds/case studies. However, *attacker profiling* remains limited (focus is device/app/implementation rather than adversary identity/rate control), *behavioral dynamics* are only partially captured, *agent agility* is rarely parameterized (attackers/defenders typically static), and *engagement dynamics* (coordination among multiple attackers, or closed-loop A↔D coupling) are generally

out of scope. Domain-specific IoMT defenses (e.g., MITM detection for eHealthcare BLE [27]) further motivate adversary-aware modeling but similarly treat the attacker as largely static. Complementary attack studies such as demonstrations of BLE DoS feasibility [28, 29], protocol-level manipulations [30], and the SweynTooth family of implementation faults [31], clearly establish *attack type* coverage. Although they offer empirical validation, they typically omit *attacker profiling*, do not model *behavioral dynamics* beyond simple floods, and do not consider *agent agility* or *engagement dynamics*.

Gap and our contribution Across these streams, existing work rarely (a) profiles the *attacker* with per-attacker timing/rate parameters, (b) models *behavioral dynamics* at the advertisement timescale, (c) exposes *agent agility* on both sides, or (d) explicitly models *engagement dynamics* (e.g distinguishing between independent and coordinated attackers, as well as non-adaptive (open-loop) and adaptive (closed-loop) attacker–defender interactions) and links these dynamics to measurable traffic degradation in IoMT environments.. Our probabilistic approach addresses this gap by (1) defining per-attacker success over BLE duty cycle and send-rate, (2) extending to the multi-attacker case via the complement-of-no-success formulation, (3) allowing attacker/defender agility as scenario parameters, and (4) validating alignment with a controlled testbed to link model predictions to observed packet distributions and drop rates.

3 Problem Description & Formalization

Calculating the probability of a successful attack on a device operating on low-energy protocol in this scenario involves considering the timing and the probability that the device will be active and able to receive flood/spam messages during its active listening periods. Assuming that a BLE device actively listens for a random amount of time (***Active Listening Time***) before backing-off, or going to sleep mode (***Sleep-Time***), and cannot receive messages in sleep mode, the success probability of an attacker is highly dependent on the availability of the channel opening, and its capability to Spam/flood it. Hence, using these parameters, the problem of estimating attack impact or success probability of flooding/spamming a victim can be modeled as follows:

- **Active Listening Time (ALT):** We represent the window of average time the BLE device actively listens before going to sleep mode as active listening time (ALT). Whereas, $\boldsymbol{ALT} \in \mathbb{R}^+$ (measured in milliseconds or seconds).

- **Sleep Time (ST):** This variable represents the window of time in which a device chooses not to actively participate in receiving certain types of traffic, in this case, unauthorised advertisements. This notion is very similar to the back-off mechanism in Carrier Sense Multiple Access (CSMA CA/CD), but instead of activating/assigning a back-off window after sensing the channel, this sleep time is determined solely by the device's preference and risk tolerance, without scanning any channels. Whereas, $\boldsymbol{ST} \in \mathbb{R}^+$ (measured in milliseconds or seconds).

- **Duty Cycle (DC):** The duty cycle is the ratio of the active listening time to the total cycle time (sum of active listening time and sleep time).

$$DC = \frac{ALT}{ALT + ST}, \quad \text{where } DC \in [0, 1] \subset \mathbb{R}$$

- **Spam Rate (SR):** The spam rate represents the frequency at which an attacker sends spam messages over time. It is inversely proportional to the interval between consecutive spam attempts, meaning the shorter the interval between messages, the higher the spam rate. Mathematically, this relationship can be expressed as:

$$SR = \frac{1}{T_{SA}}, \quad \text{where } SR \in \mathbb{R}^+,\ T_{SA} \in \mathbb{R}^+$$

  Here, T_{SA} denotes the ***time between spam attempts***, measured in seconds or milliseconds, and **SR** denotes the ***spam rate***, measured in messages per unit time (e.g., per second). This relationship reflects the standard rate–period dependency, where both variables are strictly positive real numbers. For example, if an attacker sends one spam message every 20 milliseconds ($T_{SA} = 0.02\,s$), the corresponding spam rate would be $SR = \frac{1}{0.02} = 50$ messages per second.
- **Probability of Spam Success (PS):**
  Let Δt (in milliseconds) denote the ***observation window*** during which a single spam packet is transmitted.
  Then given ***DC***, and ***SR***, the probability of successfully delivering a spam can be formally defined as a product of independently transmitting a spam at a rate (***SR***), while listener is active with a specific duty cycle (***DC***), within the same observational window ($\Delta(t)$). Therefore, the formal expression becomes:

$$P_{Spam} = DC \times SR \times \Delta t, \quad \text{where } P_{Spam} \in [0, 1] \subset \mathbb{R}$$

  For example, if the attacker sends spam every 20 milliseconds ($SR = \frac{1}{20\text{ ms}}$) and the duty cycle is 10% (*DC=0.1*), then the probability of success would be $P_{Spam} = 0.1 \times \frac{1}{20\text{ ms}} \times 20\ ms$. Thus there is a 10% chance that this particular packet will be received. The same framework generalises to many packets or many attackers by the complement–probability expressions introduced later.

It's important to note that these calculations provide an estimate, and the actual success probability may vary based on the specific behavior of the BLE device and the attacker's strategy. Therefore, to understand the impact of such attacks and their likelihood, a more robust model needs to be formalized, which can take into account multiple attackers with static and dynamic attack parameters. With this objective in hand, our next objective is to develop a formalization to measure the impact of multiple attackers.

The probability of successfully spamming a target in a scenario where there are multiple attackers can be calculated using the complement probability theorem. For this the base case becomes the scenario in which at least one attacker is successful in conducting the spam attack. The probability that at least one of the attackers

succeeds can be calculated as follows:

$$P_{\text{Spam}}(\text{AOS}) = 1 - P_{\text{Spam}}(\text{NS}) \tag{1}$$

Where: Term $P_{Spam}(AOS)$ refers to the probability of at least one attacker succeeding, and term $P_{Spam}(NS)$ refers to the probability of no one (attacker) succeeding.

If there are N attackers, and P^i_{Spam} represents the probability of success for i_{th} attacker, then the probability of no success for any attacker can be calculated as the product of probabilities of no success for each attacker:

$$P_{\text{Spam}}(\text{NS}) = \prod_{i=1}^{N}(1 - P^i_{\text{Spam}}) \tag{2}$$

Therefore, the final expression for the probability of at least one attacker succeeding in a spam attack becomes:

$$P_{\text{Spam}}(\text{AOS}) = 1 - \prod_{i=1}^{N}(1 - P^i_{\text{Spam}}) \tag{3}$$

We use the above-mentioned formalization (for $P_{Spam}(Atleast-One-Succeeds)$) as our new base model to analyze the attack parameters in details, and build two different variations on it under attack models in the forthcoming section.

4 Feasibility of Attack & Impact Analysis

As our main objective is to design a deterrence strategy for flooding/spam attacks, the very first step towards this direction is the understanding of "*how deadly this attack can be*", and whether it is even possible to design a deterrence against such attacks by altering underlying parameters, i.e., duty cycle, and back-of-window.

Understanding the feasibility of such attacks on low-energy protocols requires a structured analysis of how different attack models influence the probability of a successful spam/flooding attempt. In this section, we mathematically formalize attack models and analyze these models under different attack scenarios that vary in terms of attacker and defender capabilities and strategies. The goal is to quantify the likelihood of success under different assumptions and to highlight the impact of attacker adaptability on infrastructure security, and eventually devise a strategy to counter these attacks.

4.1 Attack Models

Towards this direction, we abstract the adversary's behavior into two canonical cases that describe the threat landscape. ***The Static Model***, that embodies a memoryless attacker with a fixed transmission pattern, energy budget, and consistency; this permits closed-form insight into how a victim's duty-cycle parameters alone govern vulnerability. In contrast, the ***Agile Model*** represents an adaptive adversary that continuously changes its emission schedule in response to observed channel opportunities,

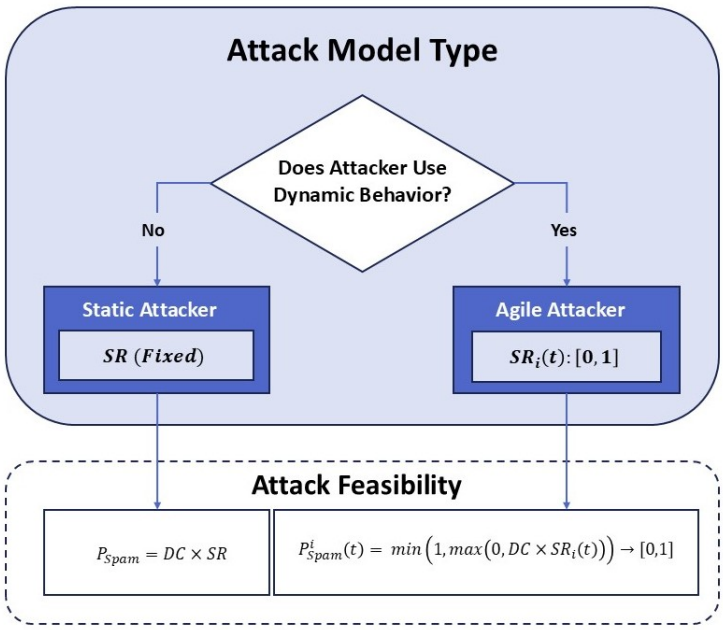


Fig. 1: Conceptual overview of the two attack model types considered in this work. A static attacker uses a fixed spam rate, whereas an agile attacker varies its transmission behavior over time. In both cases, the feasibility of a successful flooding attempt is determined by the interaction between the attacker's spam rate and the victim's duty cycle.

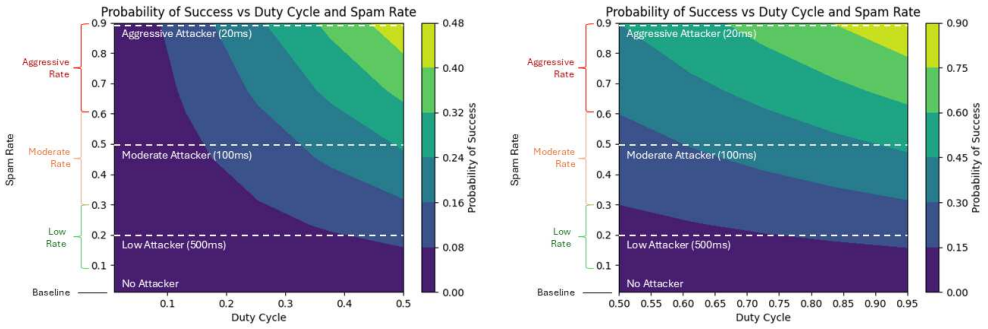
thereby exploiting any temporal slack in the protocol. The side-by-side development and Study of these models (c.f. Fig. 1) clarifies the security margin lost once an attacker gains even limited situational awareness and sets the foundation for defence strategies that remain effective across both extremes.

4.1.1 Static Model: Single Static Attacker Vs. Static Victims

The static model represents the simplest case of spam attacks, where a single attacker uses a fixed strategy against victims whose duty cycles remain constant. To establish a baseline, we first analyze the one-to-one scenario (a single attacker against a single victim). This allows us to observe how the victim's duty cycle could potentially influences the probability of a successful spam attempt.

Using the base model, we vary the victim's duty cycle across two ranges: a low range ($DC \in [0.01, 0.5]$) and a high range ($DC \in [0.5, 0.9]$). Figures 2a and 2b show that higher duty cycles correlate strongly with higher spam success probability, confirming that victims with longer active listening periods are more vulnerable to static attackers.

While this experiment considers a one-to-one case, the insights generalize to scenarios with multiple static victims, as each victim's probability of being successfully



(a) Spam success probability across $DC \in [0.01, 0.5]$.

(b) Spam success probability across $DC \in [0.5, 0.9]$.

Fig. 2: Duty cycle vs. spam success probability (P_{Spam}).

spammed depends primarily on its own duty cycle and the attacker's fixed spam rate. This baseline result will serve as a reference for more complex models in the following subsections. This baseline case highlights how static assumptions simplify the analysis but also limit the attacker's effectiveness. In the next subsection, we extend the model to consider *agile attackers*, who adapt their strategies dynamically, significantly increasing the impact on victims.

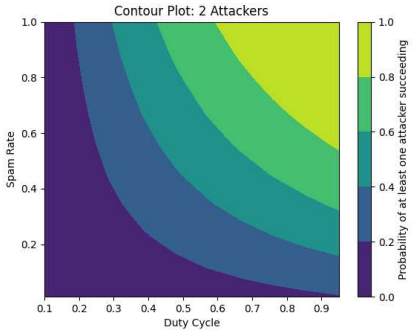
To systematically evaluate attacker behavior across varying transmission intensities, we define three attacker profiles based on advertisement interval selection. Under normal conditions, fast BLE advertising typically operates in the range of 100 to 500 ms [32]. This serves as a reference baseline for attacker profile classification.

We define an aggressive attacker transmitting at intervals below 100 ms, exceeding conventional fast-advertising rates and increasing channel saturation. A moderate attacker operates within the 100–500 ms range, aligning disruptive transmissions with normal traffic patterns to improve stealth. A low-rate attacker transmits at intervals above 500 ms, reducing observable deviation from baseline behavior while sacrificing immediate spam impact. While the static model assumes a fixed spam rate, this classification enables systematic evaluation of how varying transmission intervals influence detectability and victim success probability.

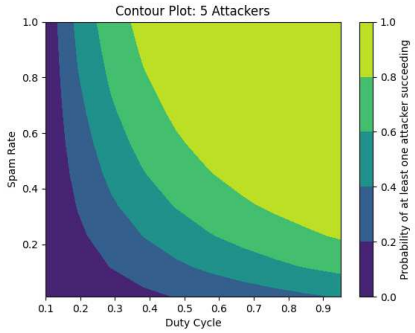
4.1.2 Agile Attack Model: Multiple Agile Attacker Vs. Static Victim

Unlike the static case, agile attackers adapt their behavior dynamically to maximize impact. They can adjust their spam rate (stochastic) over time, making their attacks more effective and harder to defend against.

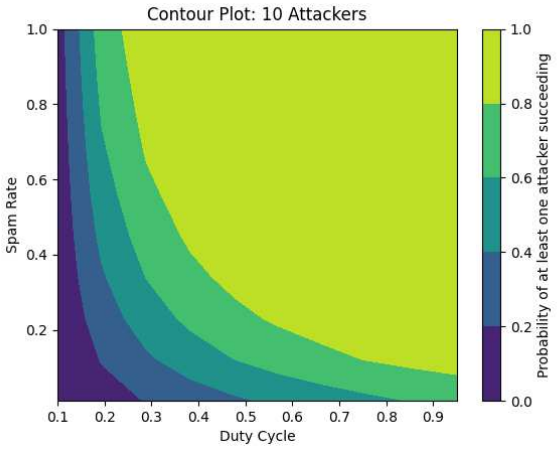
To understand and model the impact of an agile attacker, we must revisit our base model for multiple attackers. The terms $P_{Spam}(AOS)$ and $P_{Spam}(NS)$ in the base model, will no longer be static, and deterministic now due to the involvement of a random variate $SR_i(t) :\mapsto [0, 1]$, which represents spam rate of i^{th} attacker at an arbitrary time/iteration (t). Therefore, the final expression in the base scenario (P^{AOS}_{Spam}) updates



(a) 2 agile attackers



(b) 5 agile attackers



(c) 10 agile attackers

Fig. 3: Impact of agile attackers on attack success rate ($SP^{\text{AOS}}_{\text{Spam}}(t)$) over time.

to $P^{AOS}_{Spam}(t)$, and the resultant model, which encapsulates the attacker's agility, can be formally written as follows:

$$P_{\text{Spam}}\text{NS}(t) = \prod_{i=1}^{N} \left(1 - P^{i}_{\text{Spam}}(t)\right) \tag{4}$$

Whereas:

$$P^{i}_{\text{Spam}}(t) = \min\left(1, \max\left(0, DC \times SR_i(t)\right)\right) \mapsto [0,1] \tag{5}$$

$$P^{\text{AOS}}_{\text{Spam}}(t) = 1 - P^{\text{NS}}_{\text{Spam}}(t) = 1 - \prod_{i=1}^{N} \left(1 - P^{i}_{\text{Spam}}(t)\right) \mapsto [0,1] \tag{6}$$

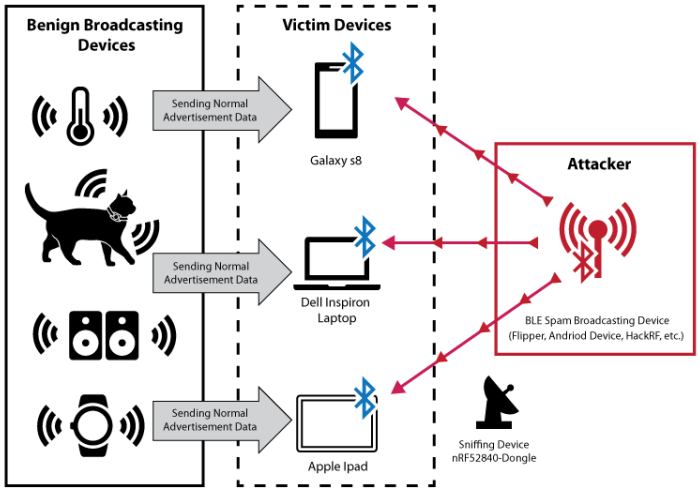


Fig. 4: The testbed emulates realistic BLE communication with benign broadcasting devices (thermometer, smartwatch, AirTags) and three victim hosts, including a Galaxy S8 (Android), Dell Inspiron (Windows), and iPad (iOS). A BLE spam transmitter (e.g., Flipper Zero) generates adversarial traffic, while an nRF52840 dongle captures packets for analysis.

5 Empirical Analysis and Comparison

5.1 Testbed Setup

Testbeds are designed to mimic various real-world environments where BLE devices operate, such as indoor, outdoor, and different interference scenarios. This includes setting up barriers, varying distances between devices, and introducing controlled interference to simulate a wide range of conditions. For this test, we will initially use low-cost market equipments, as described in Figure 4. Specifically, we construct the testbed around four types of cheap or readily available equipments: BLE sensors, BLE host devices, an attacker device responsible for generating adversarial behavior, and a BLE sniffer for monitoring.

As shown in Figure 4, benign BLE devices continuously broadcast advertisement traffic toward nearby host platforms while sharing the same wireless space with the attacker device. The attacker operates as an external broadcaster capable of injecting adversarial advertisement packets without requiring prior pairing or authentication, reflecting the opportunistic nature of BLE spam attacks.

5.1.1 Required Hardware

BLE Sensors: These could be any BLE sensor, which tends to broadcast readings/measurements taken from its surroundings. Our experimental testbed incorporates a diverse range of BLE–enabled sensors and user devices to emulate the heterogeneity found in real-world environments. The setup includes a Govee Smart Thermo-Hygrometer H5075 for environmental monitoring, a Samsung Galaxy Watch 4 representing wearable systems, and two mobile Apple AirTags attached to pet collars to simulate dynamic movement within the test area. Operating in an open environment within a small office, the testbed continuously captures ambient Bluetooth activity from surrounding devices entering and exiting the vicinity. This background activity introduces realistic environmental noise from various Bluetooth and BLE peripherals such as headsets, speakers, and other transient consumer devices. This provides a more authentic representation of wireless interference in a given environment.

Victim Devices: BLE sensors are not self-sufficient, which means we need a host to control or extract data from them, in IoMT it could be any client-tailored/custom upgraded smart tablet, whereas outside of IoMT settings, the monitoring equipment is usually smartphones, tablets, and/or computers. For broad coverage, our testbed includes one representative host from each category, each selected to reflect a different commercial BLE host ecosystem and common user platform. The chosen hosts act as victim devices that communicate with nearby BLE sensors: a Samsung Galaxy S8 smartphone running Android (representing mainstream Android phones), a ninth-generation Apple iPad (representing iOS/tablet clients), and a Dell Inspiron 14 5425 laptop running Windows 11 Pro (64-bit), equipped with an AMD Ryzen 7 5825U processor, 16 GB DDR4 memory, and a 512 GB NVMe SSD storage device (representing Windows-based computer hosts). Together, these devices provide heterogeneous endpoints for evaluating cross-platform BLE interactions and monitoring behavior across typical real-world host environments.

Attacker Device: To mimic a persistent attacker, we used a Flipper Zero device with BLE spam installed. Flippers have a tendency to broadcast traffic on multiple frequency channels, by channel and frequency hopping. Users can also randomize the MAC address for each packet sent or change the DoS/spamming speed from 20ms to 500ms based on the victim's device OS. For analysis purposes we will only utilize changing the spam interval rate, as MAC address randomization complicates the identification process.

Sniffing Devices: For capturing packets on the data link layer and network layer (layer 2), we aim to employ Wireshark with the integration of a nRF52840 dongle flashed with Nordic's nRF Sniffer for Bluetooth LE will be attached to a host machine running Wireshark to complete the setup of our testbed. To ensure that packets between the attacker device and the victim devices are captured properly the dongle will be placed between these devices. For the initial test we aim to have the main victim, sensor and attacker devices stationary to collect baseline data. Victim and attacker devices would be kept within a meter radius of the dongle to reduce the risk of lost packets at increase distances.

While this configuration provides an affordable and accessible BLE sniffing solution, it introduces certain operational limitations. The nRF52840 dongle can monitor

Table 2: Distribution of BLE packets across scenarios with varying spam rates

Scenario	Spam Rate	Attacker Packets	Normal Packets	Total Packets	% Spam
Baseline	n/a	0	210,107	210,107	0.00
Moderate Attacker	100 ms	99,644	234,275	333,919	29.84
Aggressive Attacker	20 ms	450,153	211,720	661,873	68.01

only one BLE advertisement channel at a time and does not support true simultaneous multi-channel capture. As a result, packet loss may occur, particularly in environments with elevated channel congestion or high advertisement density. In noisier settings, rapid channel hopping and overlapping transmissions can further increase the likelihood of missed packets. Which must be considered when interpreting captured traffic distributions.

5.2 Evaluation

To validate the behavioral trends predicted by our probability estimation model in section 4 (Figure 2), we conducted controlled data collection of BLE packet transmissions under varying attacker conditions. The resulting comparison, summarized in Table 2, presents the distribution of BLE packets across three scenarios: Baseline (no attacker), Moderate Attacker (100 ms spam interval), and Aggressive Attacker (20 ms spam interval). Each capture session lasted one hour, with random MAC address rotation disabled to ensure consistent filtering of attacker-generated traffic. The primary objective was to assess how varying spam rates influence real-world packet dominance and to evaluate the extent to which these measurements align with the model's simulated probability estimates.

In the Baseline condition, no attacker activity was present. The capture contained 210,107 normal BLE transmissions, corresponding to a measured spam rate of 0%. As predicted, the model estimated a success probability of zero across all scanning duty cycles, consistent with expectations in an uncompromised environment.

In the Moderate Attacker condition (100 ms spam interval), the attacker introduced 99,644 additional packets, increasing the total observed traffic to 333,919. This represents an approximate 30% increase in captured packets from the baseline. Given that the maximum delay setting available on the Flipper device is 500 ms, the 100 ms injection rate corresponds to the middle region of our simulation's probability curve. For moderate scanning duty cycles, the model predicts a success probability of approximately 15–45%, which closely matches the empirical results. At this rate, attacker traffic coexists with legitimate BLE communication but begins to noticeably reduce available channel capacity for normal transmissions.

In the Aggressive Attacker condition (20 ms spam interval), the attacker injected 450,153 and comprising approximately 68% of the total captured traffic. Operating at five times the rate of the 100 ms condition, this configuration aligns with the upper bound of the simulated probability estimates. Even moderately active receivers (duty cycle: 60%) experienced modeled success probabilities above 50%, with higher duty cycles approaching near-total disruption. In practice, an attacker operating at a 20

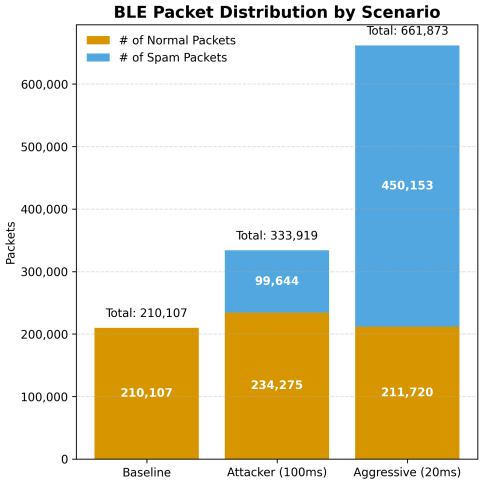


Fig. 5: Absolute BLE packet counts across scenarios.

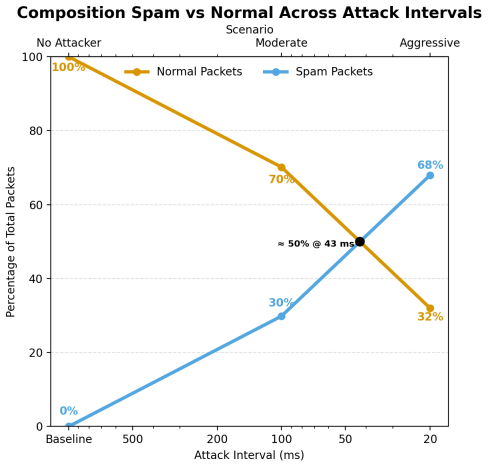


Fig. 6: Relative packet composition across attack intervals.

ms interval can inject sufficient traffic to substantially degrade or even suppress BLE communications for devices that rely on opportunistic scanning.

The absolute distribution of BLE traffic across each attack condition is illustrated in Figure 5. Although the volume of legitimate BLE transmissions remains relatively stable across all scenarios, attacker-generated traffic increases substantially as advertisement intervals decrease. In the aggressive 20 ms condition, adversarial packets exceed legitimate traffic by more than a two-to-one ratio. Demonstrating the ability of high-rate spam transmissions to dominate the observable BLE channel. The corresponding packet composition across attack intervals is depicted in Figure 6. Although the volume of legitimate transmissions remains largely stable across all scenarios, the overall traffic increases substantially under attack conditions, reducing the proportional presence of normal packets within the dataset. The two distributions converge near the 50% threshold at approximately 43 *ms*, signifying the point at which adversarial activity begins to dominate the communication channel. Below this threshold, injected spam remains relatively stealthy, blending with benign BLE exchanges. Above it, spam traffic saturates the channel and becomes far easier to detect due to its overwhelming contribution to total packet volume.

From a defensive perspective, this crossover highlights the importance of adopting an adaptive duty-cycle strategy. Receivers equipped with the capability to dynamically regulate their scanning intervals can mitigate transient or low-frequency spam activity while maintaining efficient communication throughput. This agility allows for early-stage mitigation of low-impact interference while still ensuring timely detection and response once attacker behavior surpasses the observable threshold.

While these experiments employed a single attacker at fixed delay intervals, the underlying model has broader implications. An agile adversary, capable of dynamically adjusting spam rates or transmitting in short bursts synchronized to observed scanning

intervals, could achieve disproportionately high disruption with lower total packet volumes. In multi-attacker scenarios, even low-rate devices can collectively elevate the spam rate to disruptive levels without any single attacker drawing significant attention. For example, a single attacker at a moderate 100 ms rate achieves an estimated success probability of 30% for a moderate-duty-cycle receiver. Two such attackers operating independently elevate the success probability to roughly 40–60%, while three attackers at the same rate reach 60–80%, approaching the impact of a single aggressive 20 ms spammer.

Overall, these empirical results reinforce the predictive value of the simulation, confirming that it accurately characterizes both brute-force disruption and more subtle, coordinated attacks. Moreover, the findings underscore that even moderately distributed adversaries can degrade BLE communication quality over time, posing significant challenges for systems that rely on duty-cycled or energy-constrained scanning strategies.

6 Defense Against Persistent Spam Threats

6.1 Feasibility of Agility Based Defense: Multiple Agile Attackers Vs. Agile Victim

In this agility-based defensive model, we introduce a dynamic and adaptive defense strategy to counteract the actions of multiple agile attackers. This model acknowledges the ever-changing nature of cyber threats and aims to create a resilient environment through agility. This approach assumes both attackers and victims to be agile. This defensive mechanism represents a more complex and dynamic environment compared to the previous models.

By using the same concept of agility (as in the attack model), if the defender can also dynamically and randomly change their parameters (spam rate (SR) for the attacker and the ratio duty cycle (DC) for the defender) over time, the resulting probability calculation becomes more intricate. The dynamics of this defensive scenario and the interactions between the attacker and defender would need to be considered. We aim to study the feasibility of such a defensive posture by measuring the probability of a successful attack.

A more general formulation will now involve time-dependent functions for both the attacker's spam rate $SR(t)$ and the defender's duty cycle $DC(t)$. The probability of a successful attack for an individual attacker i^{th} at time t could be represented as:

$$P^{i}_{\text{Spam}}(t) = \min\left(1, \max(0, DC(t) \times SR_i(t))\right), \quad \mapsto [0,1] \tag{7}$$

Therefore, the probability that no attacker succeeds at time t, updates to:

$$P^{\text{NS}}_{\text{Spam}}(t) = \prod_{i=1}^{N} \left(1 - P^{i}_{\text{Spam}}(t)\right) \tag{8}$$

$$P^{\text{AOS}}_{\text{Spam}}(t) := 1 - P^{\text{NS}}_{\text{Spam}}(t) \equiv 1 - \prod_{i=1}^{N} \left(1 - P^{i}_{\text{Spam}}(t)\right), \quad \mapsto [0,1] \tag{9}$$

Although, the final expressions for $P^{NS}_{Spam}(t)$ and $P^{AOS}_{Spam}(t)$ remain same (as in scenario 2), the impact of random variate $DC(t) :\mapsto [0, 1]$, over multiple BLE frequency channels, changes the outcome of the probability distribution.

Figure 7 illustrates the simulated probability distributions of $P^{\text{AOS}}_{\text{Spam}}(t)$ across 100,000 trials for 2, 5, and 10-agile attackers facing an agile defender. With only two attackers, the distribution remains narrow and concentrated near low success probabilities, suggesting that an agile defender can reliably suppress the threat. As the number of attackers grows to five and then ten, the distribution progressively shifts toward higher success probabilities and exhibits greater spread, converging towards 22% success rate for ten-attackers.

A direct comparison between Figure 3c and Figure 7 (bottom panel) reveals the measurable advantage conferred by defender-side agility. In Figure 3c, a static defender facing 10 agile attackers experiences near-certain disruption across virtually all combinations of spam rate and duty cycle, with $P^{\text{AOS}}_{\text{Spam}}(t)$ approaching 1.0 across the majority of the parameter space. The contour plot leaves almost no safe operating region for the defender, even for lower duty cycles, confirming that a fixed duty cycle offers negligible resistance against a coordinated, adaptive multi-attacker threat.

In contrast, Figure 7 (bottom panel) shows that when the defender also adopts agility by dynamically randomizing its duty cycle $DC(t)$, the maximum observed attack success probability converges to only 22%. This represents a substantial reduction compared to the near-certain disruption depicted in Figure 3c, effectively multiplying the cost an attacker must bear to achieve the same level of disruption. The spread in the probability distribution further indicates that defender-side agility introduces genuine uncertainty into the attacker's ability to time spam transmissions successfully, even under sustained ten-attacker pressure, rendering coordinated flooding attempts considerably less predictable and harder to sustain.

6.2 Design of Agility-based Defense Using First-Order Logic

Since our main objective is to minimize the value of the probability of at least one successful attack, our objective function becomes:

$$Minimize(P^{AOS}_{Spam}(t)) \mapsto [0, 1]$$

Although this can be solved by using optimization techniques (to find global minima), it is almost impossible to solve it in linear time, given the non-linear nature of the objective function. To tackle an agile attacker, this problem must be solved in near real-time, so that the defender can adjust its strategy on the go. Therefore, optimization might not be the ideal choice, hence opening the door for methods that may be able to find a counter-example in a certain scenario. For example, the optimization problem can be converted into a satisfiability problem, where we can add a threshold, and impose a constraint that the probability of attack must not exceed a certain acceptable threshold, instead of finding a global minimum value.

In this case, we can formalize the problem using uninterpreted functions and variables in First-Order Logic as follows:

- Duty cycle of the defender: $DC(t) \mapsto \{\, DC \in \mathbb{R} \mid 0 \leq DC(t) \leq 1 \,\}$.

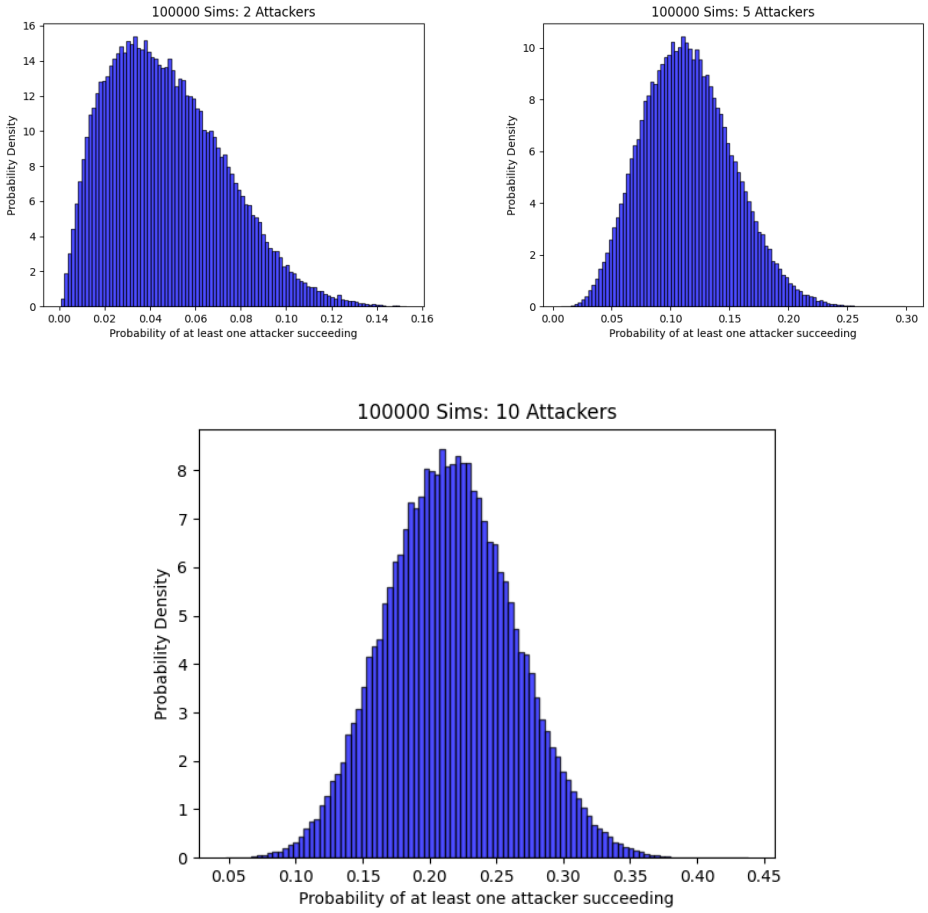


Fig. 7: Probability of at least one successful attack ($P^{\text{AOS}}_{\text{Spam}}(t)$) over time for varying numbers of agile attackers against an agile defender. Top-left: 2 attackers. Top-right: 5 attackers. Bottom: 10 attackers.

- Spam rate of attacker i: $SR_i(t) \mapsto \{\, SR_i \in \mathbb{R} \mid 0 \leq SR_i(t) \leq 1,\ 1 \leq i \leq M \,\}$, where M denotes the maximum number of attackers.
- Individual probability that attacker i succeeds: $P^i_{\text{Spam}}(DC, SR) \mapsto \{\, P^i_{\text{Spam}} \in \mathbb{R} \mid 0 \leq P^i_{\text{Spam}}(t) \leq 1 \,\}$.

Combined success probability. Let $M \in \mathbb{N}_{\geq 1}$ be the maximum number of attackers defined above. Assuming independent attempts, the probability that *at least one*

attacker succeeds at time t is

$$\boxed{P^{\text{AOS}}_{\text{Spam}}(t) = 1 - \prod_{i=1}^{M} \Big(1 - P^{i}_{\text{Spam}}\big(DC(t), SR_i(t)\big)\Big)}$$

When the separable model $P^{i}_{Spam}(d, s) = d \times s$ is instantiated, this reduces to $P^{AOS}_{Spam}(t) = 1 - \big(1 - DC(t)\, SR_1(t)\big) \cdots \big(1 - DC(t)\, SR_M(t)\big)$, which is the expression implemented in the prototype SMT script.

Threshold formulation. Rather than minimising $P^{AOS}_{Spam}(t)$ outright, we select an acceptable upper bound $T \in [0, 1]$ (e.g. $T = 0.35$) and restrict the *search space* of duty–cycle and spam-rate parameters to a defender-defined operating window

$$\boxed{\begin{array}{c} \underline{D} < DC(t) < \overline{D}, \\ \underline{S} < SR_i(t) < \overline{S}, \quad 1 \le i \le M \end{array}}$$

where $\underline{D}, \overline{D}, \underline{S}, \overline{S}$ are constant bounds supplied by policy.

Existential counter-example query (SMT). The optimization problem is recast as the following satisfiability question:

$$\boxed{\begin{array}{c} \exists\, (DC, SR) :\ \underline{D} < DC(t) < \overline{D} \\ \wedge \bigwedge_{i=1}^{M} \big(\underline{S} < SR_i(t) < \overline{S}\big) \\ \wedge\ P^{\text{AOS}}_{\text{Spam}}(t) > T \end{array}}$$

If the SMT solver returns SAT, it provides concrete values $DC(t)$ and $SR_i(t)$ that violate the threshold, signaling the defender to adapt its parameters (and avoid unsafe configuration). A result of UNSAT certifies that no admissible configuration exceeds T for the current M.

Figure 8 presents the conceptual architecture of the proposed agility-based defense framework. The adversarial side of the model accommodates both static and agile attackers: a static attacker operates with a fixed spam rate SR, while an agile attacker varies its transmission behavior over time, represented by the time-dependent function $SR_i(t)$. The defense module, relies on the stochastic model to calculate the probabilities, and correspondingly utilizes our above mentioned formalization and Satisfiability Modulo Theories (SMT) solver, to verify, whether a safe state exists for certain parameters. This safety information is then relayed to the defender to synthesize strategy, such that the corresponding parameters can be tuned to avoid any further jamming, spam, or DoS attacks.

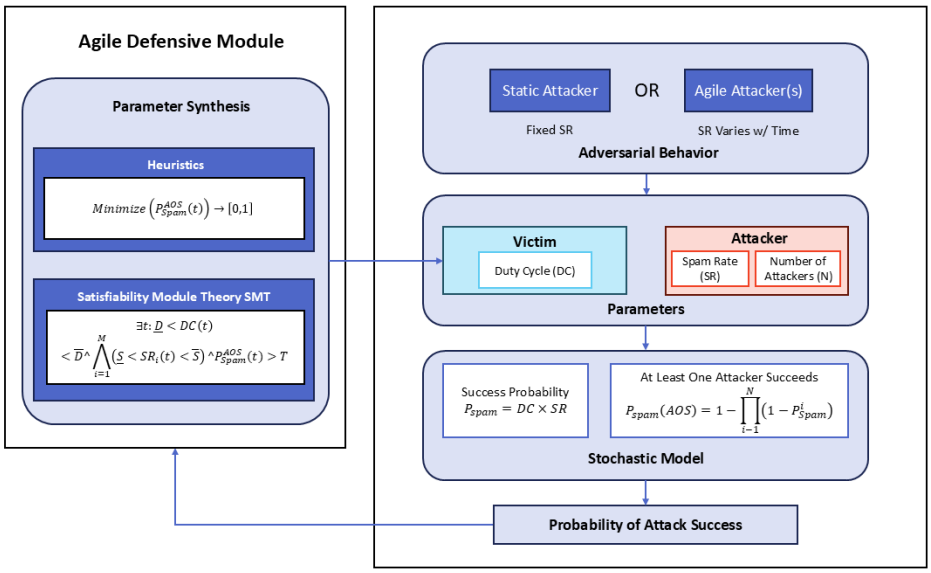


Fig. 8: Conceptual structure of the agility-based defense framework. The defender employs heuristic optimization and SMT-based constraint reasoning to synthesize adaptive duty-cycle parameters, while the adversary may operate as a static or agile attacker with time-varying spam rates.

7 Conclusion & FutureWork

This work demonstrate the measurable impact of BLE spam and flooding attacks on IoT environments and establishes a foundation for understanding their disruptive capacity. We formalized the the problem as a stochastic process and presented: (i) precise threat models of both static and adaptive adversaries and their interaction with IoT environment; (ii) empirical validation through a controlled testbed that captured real-world BLE traffic across varying levels of attacker aggression; and (iii) integration of defender-side agility into the same stochastic framework to evaluate response strategies under dynamic conditions. To the best of our knowledge, this is the first effort to model adversarial behavior in IoT environments, combining empirical validation with formal analytical tools to characterize attacker capabilities and inform actionable defense strategies.

The findings underscore two key insights. First, even moderately aggressive attackers, when distributed across multiple devices, can achieve levels of disruption comparable to a single, high-intensity adversary. Second, defender-side agility can reduce the probability of attack success below critical/desired thresholds. However, translating this potential into practice remains a significant challenge. By jointly modeling attacker adaptability and system responsiveness, our study offers BLE implementers a quantitative basis to anticipate degradation risks and reason about adaptive mitigation strategies.

Through this adversarial behavioral modeling, our study contributed both validated empirical evidence and actionable insight. The combination of probabilistic modeling and testbed validation not only quantified the impact of stealthy BLE flooding attacks but also produced design-level recommendations for strengthening IoT deployments. While our defense-side modeling provides a promising foundation, future work should extend these results into deployable countermeasures and policy-level guidance for standardization bodies such as the Bluetooth SIG.

In particular, future work will explore the impact and practical viability of channel hopping as a defensive strategy, including the extent to which BLE stack updates or modifications can support more agile channel-selection behavior. We also aim to extend the proposed stochastic model to explicitly study multi-channel effects, enabling a more realistic analysis of adversarial flooding and resilience emerging from defender's adaptation across multiple BLE advertising channels. Finally, we plan to collect a more rigorous and diverse dataset to further validate the defensive capabilities of the proposed model under realistic Internet of Medical Things (IoMT) deployment conditions.

Funding

This work is not supported by any Funding Agency.

Datasets

All the data used in this paper can be made available upon request.

References

[1] Cho, K., Park, G., Cho, W., Seo, J., Han, K.: Performance analysis of device discovery of bluetooth low energy (ble) networks. Computer Communications **81**, 72–85 (2016) https://doi.org/10.1016/j.comcom.2015.10.008

[2] Fourati, L.C., Said, S.: Remote health monitoring systems based on bluetooth low energy (ble) communication systems. In: The Impact of Digital Technologies on Public Health in Developed and Developing Countries, ICOST 2020. Lecture Notes in Computer Science, vol. 12157, pp. 41–54. Springer, ??? (2020). https://doi.org/10.1007/978-3-030-51517-1_4

[3] Lacava, A., Zottola, V., Bonaldo, A., Cuomo, F., Basagni, S.: Securing bluetooth low energy networking: An overview of security procedures and threats. Computer Networks **211**, 108953 (2022) https://doi.org/10.1016/j.comnet.2022.108953

[4] World Health Organization: Strategic Situational Analysis (SSA) (n.d.). https://extranet.who.int/ssa/Index.aspx

[5] Malwarebytes Labs: Meet the Entirely Legal, iPhone-crashing Device, the Flipper Zero: Lock and Code S04E25. Malwarebytes. https://www.malwarebytes.com/b

log/podcast/2023/12/meet-the-entirely-legal-iphone-crashing-device-the-flipper-zero-lock-and-code-s04e25 Accessed 2025-10-01

[6] Winder, D.: iPhone iOS 17 Hack Attack Reported in the Wild—How To Stop It. Forbes (online) (2023). https://www.forbes.com/sites/daveywinder/2023/11/06/iphone-ios-17-hack-attack-reported-in-the-wild-how-to-stop-it/

[7] Bluetooth LE Spam | F-Droid. Binary distribution listing for the Android BLE Spam app. https://f-droid.org/packages/de.simon.dankelmann.bluetoothlespam/ Accessed 2025-08-16

[8] BLESpam — PortaPack Mayhem Firmware Wiki. HackRF/PortaPack Mayhem app for spamming various BLE packets (Android Fast Pair, iOS, etc.). https://github.com/portapack-mayhem/mayhem-firmware/wiki/BLESpam/Bluetooth-Low-Energy-Receiver Accessed 2025-08-16

[9] Dankelmann, S.: Bluetooth LE Spam. Open-source Android app that generates spoofed BLE advertisements (Apple/Google/Samsung/Microsoft protocols). https://github.com/simondankelmann/Bluetooth-LE-Spam Accessed 2025-08-16

[10] Halloush, R., Liu, H.: Modeling and performance evaluation of jamming-tolerant wireless systems. Journal of Ambient Intelligence and Humanized Computing **10**, 4361–4375 (2019) https://doi.org/10.1007/s12652-018-1113-8

[11] Jianliang Wu, Wei Li: Detection of stealthy jamming using hidden markov models in uav-assisted networks. In: Proc. IEEE GLOBECOM (2023)

[12] Shanbhag, A., Huang, W.: Learning attack mechanisms in wireless sensor networks using markov decision processes. Expert Systems with Applications **127**, 30–43 (2019) https://doi.org/10.1016/j.eswa.2019.01.001

[13] Ghafi, H.K., Spindelberger, C., Arthaber, H.: Modeling of co-channel interference in bluetooth low energy based on measurement data. EURASIP Journal on Wireless Communications and Networking **2021**(1), 143 (2021) https://doi.org/10.1186/s13638-021-02005-2

[14] Bhunia, S., Su, X., Sengupta, S., Vázquez-Abad, F.: Stochastic model for cognitive radio networks under jamming attacks and honeypot-based prevention. In: Chatterjee, M., Cao, J.-n., Kothapalli, K., Rajsbaum, S. (eds.) Distributed Computing and Networking, pp. 438–452. Springer, Berlin, Heidelberg (2014)

[15] Allouzi, M.A., Khan, J.I.: Identifying and modeling security threats for iomt edge network using markov chain and common vulnerability scoring system (CVSS). CoRR **abs/2104.11580** (2021) 2104.11580

[16] Sikeridis, D., Papapanagiotou, I., Devetsikiotis, M.: Blebeacon: A real-subject trial dataset from mobile bluetooth low energy beacons. CoRR **abs/1802.08782**

(2018) 1802.08782

[17] Duque, A., Finet, M., Vial, T., Humbert, M.: SDR4IoT BLE & Zigbee RF dataset. Zenodo (2021). https://doi.org/10.5281/zenodo.4639390 . https://doi.org/10.5281/zenodo.4639390

[18] Bouaru, R., Peculea, A., Iancu, B., Buzura, S., Cebuc, E., Dadarlat, V.: Analysis of a bluetooth traffic dataset obtained during university examination sessions. Data **9**(4) (2024) https://doi.org/10.3390/data9040049

[19] Dadkhah, S., Neto, E.C.P., Ferreira, R., Molokwu, R.C., Sadeghi, S., Ghorbani, A.A.: Ciciomt2024: A benchmark dataset for multi-protocol security assessment in iomt. Internet of Things **28**, 101351 (2024) https://doi.org/10.1016/j.iot.2024.101351

[20] Unal, D.: BlueTack. IEEE Dataport (2021). https://doi.org/10.21227/skhs-0b39 . https://dx.doi.org/10.21227/skhs-0b39

[21] Abad, A.E., *et al.*: Secure bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system. Sensors **22**(21), 8280 (2022) https://doi.org/10.3390/s22218280

[22] Che, X., He, Y., Feng, X., Sun, K., Xu, K., Li, Q.: Blueswat: A lightweight state-aware security framework for bluetooth low energy. In: Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. CCS '24, pp. 2087–2101. Association for Computing Machinery, New York, NY, USA (2024). https://doi.org/10.1145/3658644.3670397 . https://doi.org/10.1145/3658644.3670397

[23] Zhang, Y., Weng, J., Ling, Z., Pearson, B., Fu, X.: Bless: A ble application security scanning framework. In: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, pp. 636–645 (2020). https://doi.org/10.1109/INFOCOM41043.2020.9155473

[24] Karim, I., Ishtiaq, A., Hussain, S., Bertino, E.: Blediff: Scalable and property-agnostic noncompliance checking for ble implementations, pp. 3209–3227 (2023). https://doi.org/10.1109/SP46215.2023.10179330

[25] Wu, J., Wu, R., Xu, D., Tian, D.J., Bianchi, A.: Formal model-driven discovery of bluetooth protocol design vulnerabilities. In: 2022 IEEE Symposium on Security and Privacy (SP), pp. 2285–2303 (2022). https://doi.org/10.1109/SP46214.2022.9833777

[26] Ray, A., Raj, V., Oriol, M., Monot, A., Obermeier, S.: Bluetooth low energy devices security testing framework. In: 2018 IEEE 11th International Conference on Software Testing, Verification and Validation (ICST), pp. 384–393 (2018). https://doi.org/10.1109/ICST.2018.00045

[27] Yaseen, M., Iqbal, W., Rashid, I., Abbas, H., Mohsin, M., Saleem, K., Bangash, Y.A.: Marc: A novel framework for detecting mitm attacks in ehealthcare ble systems. J. Med. Syst. **43**(11), 1–18 (2019) https://doi.org/10.1007/s10916-019-1440-0

[28] Peter Gullberg: Denial of service attack on bluetooth low energy. Technical report, Karlstad University (2017). https://www.researchgate.net/publication/317063884

[29] James Ditton, Jad Moubarak: A proof-of-concept denial-of-service attack against bluetooth iot devices. In: IEEE PerCom Workshops, pp. 94–99 (2020)

[30] Juan Castro, Javier Nigam: Ble injection-free attack: Forcing key renegotiation without packet injection. In: Proc. Int. Conf. on Autonomous and Intelligent Systems (2019). https://nigam.info/docs/jaihc19.pdf

[31] Matheus E. Garbelini, Chundong Wang, Sudipta Chattopadhyay: Sweyntooth: Unleashing mayhem over bluetooth low energy. In: USENIX ATC (2020). https://asset-group.github.io/disclosures/sweyntooth/sweyntooth.pdf

[32] Argenox Technologies: BLE Advertising Primer. https://argenox.com/library/bluetooth-low-energy/ble-advertising-primer