



Reliability analysis of anti-drone systems with image based detection and jamming techniques

Raina Raj¹ · Priyanka Kalita² · S. Dharmaraja³

Received: 15 February 2024 / Accepted: 20 January 2026

© The Author(s), under exclusive licence to Operational Research Society of India 2026

Abstract

A drone is an unmanned aircraft capable of remote operation. In recent years, drones have drawn increasing attention due to their potential misuse in security-sensitive environments, necessitating the development of reliable anti-drone technologies. This study presents a stochastic reliability model for an image-based anti-drone system that integrates detection and jamming mechanisms. The proposed framework employs Continuous-Time Markov Chain (CTMC) and Semi-Markov Process (SMP) models to represent system behavior under both exponential and non-exponential failure conditions. The steady-state probabilities for the SMP are obtained using a two-stage method, while both transient and steady-state analyses are conducted for the CTMC. Comparative numerical and simulation results demonstrate a close correspondence between the analytical and simulated values, confirming the accuracy and robustness of the proposed model. The findings highlight that reliability significantly decreases with increasing failure rates of detection and jamming units, emphasizing the importance of redundancy and component quality in anti-drone system design.

Keywords Anti-drone systems · Continuous time Markov chain · Reliability · Semi-Markov process · Simulation

✉ Raina Raj
rainaraj.curaj@gmail.com

Priyanka Kalita
priya.24723@gmail.com

S. Dharmaraja
dharmar@maths.iitd.ac.in

¹ Bharti School of Telecommunications Technology & Management, Indian Institute of Technology Delhi, New Delhi, India

² Department of Statistics, Bhattadev University, Bajali, Assam, India

³ Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, India

1 Introduction

Unmanned Aerial Vehicles (UAVs), or drones, are swiftly becoming indispensable in our modern lives, due to their extensive deployment across various applications [1]. Initially associated primarily with military applications drones have rapidly gained popularity in civilian sectors as well. The landscape of drone applications is remarkably diverse, spanning numerous verticals, including entertainment (aerial photography and videography), geology (mapping and surveying), transportation (traffic monitoring), security (search and rescue, crowd monitoring, emergency response, and disaster relief), shipping (parcel delivery), agriculture (crop monitoring, spraying, and bird control), and communication (emergency communication infrastructure). These groundbreaking applications and use cases of civilian drones hold the potential to revolutionize society by ushering in a more autonomous world.

Given the multitude of applications mentioned above, envisioning a future where swarms of drones fill the skies akin to flocks of birds is not far-fetched. While current regulations governing the use of drones in civil contexts impose some limitations on their proliferation, their adoption is projected to steadily increase over time. According to forecasts by the Federal Aviation Administration (FAA) in the United States, the number of model drones is expected to reach between 1.39 and 1.66 million, whereas non-model (commercial) drones are projected to reach a total of 835,000. However, the anticipated surge in the number of civilian drones operating in airspace raises significant concerns, particularly regarding public privacy and security. Given their “unmanned” nature, drones can be deployed anonymously for various illicit activities such as espionage, hacking, and targeted attacks. Specific scenarios highlighting these potential threats underscore the pressing need for robust drone detection systems to mitigate risks and ensure public safety and security.

1.1 Potential threat of commercial drone's

- *Cyber-security* The evolving landscape of cyber threats has underscored the imperative for robust drone detection and jamming measures, particularly in light of emerging drone-based cyber-attacks [2, 3]. Historically, enterprises have fortified their networks and computing systems through the deployment of localized private networks. However, with the widespread adoption of wireless broadband technologies like Wi-Fi and the proliferation of cloud-based storage and computing resources, the significance of physical proximity restrictions has intensified as a deterrent against cyber intrusions. As cyber criminals seek access to Wi-Fi and other short-range communication networks, drones offer an enticing avenue by enabling them to breach the boundaries of these networks with relative ease. Therefore, enhancing drone detection and jamming capabilities has become imperative for safeguarding against this evolving threat landscape and preserving the integrity of critical digital infrastructures.
- *Target attack* In recent years, drones have emerged as ominous instruments in the arsenal of terrorist organizations, facilitating targeted attacks on public figures across various regions worldwide. Beyond simply granting access to restricted

areas for the execution of nefarious plots, drones empower terrorists with the capability to surveil and track their targets remotely, particularly while they are in transit. Regrettably, drones have become increasingly alluring tools for orchestrating targeted assaults [4]. A series of alarming incidents underscores the gravity of this threat. For instance, the brazen drone attack on a Saudi airport in Jazan, along with another assault on Russian airbases and naval facilities orchestrated by a swarm of miniature drones armed with explosives, exemplify the escalating employment of drones in terrorist endeavors. These incidents serve as poignant reminders of the urgent need for heightened vigilance and the development of innovative countermeasures to mitigate the evolving risks posed by drone-enabled terrorism.

As drones increasingly infiltrate military operations, their potential to pose safety and security threats have become more apparent. This realization has spurred the development of anti-drone technologies. These systems are meticulously engineered to mitigate the risks associated with drone-related accidents and potential acts of terrorism, necessitating continuous advancements to keep pace with evolving drone flight systems. The origins of anti-drone and counter-drone systems trace back to seminal works such as [5]. This foundational research delved into the survivability analysis conducted for initiatives like the U.S. Army's Aquila drone program and the Joint Short Range drone program. Their findings not only shed light on the capabilities and requirements of anti-drone measures but also set the stage for subsequent advancements in this field.

1.2 Drone detection method

The drone detection system utilizes various features inherent to drones to detect their presence, ascertain their location, and identify other pertinent attributes. Drones typically emit distinct signals, including but not limited to radio frequency (RF) signals, acoustic waves, thermal signatures, and induce Doppler effects within the surrounding environment. These signals can be effectively captured by specialized sensor systems and subsequently processed to discern the presence of a drone within a designated area of interest.

This detection process encompasses a range of sensing methodologies, leading to the categorization of drone detection systems into four primary classes: acoustic detection, RF detection, radar detection, and visual detection. Each category employs distinct technologies and approaches tailored to the unique characteristics of the signals emitted by drones.

- 1 *Acoustic detection* This method relies on the detection and analysis of sound waves produced by drones. Specialized microphones and acoustic sensors are deployed to capture and analyze the unique acoustic signatures generated by drone propulsion systems and rotors. By discerning these acoustic patterns, the system can identify the presence and approximate location of drones [6].
- 2 *RF detection* RF detection involves the utilization of radio frequency sensors to intercept and analyze the RF signals transmitted by drones. These signals

are emitted by the drone's communication systems, control mechanisms, and onboard electronics. RF detection systems employ antennas and receivers to capture and analyze these signals, allowing for the detection and tracking of drones within the system's range [7].

- 3 *Radar detection* Radar-based detection systems utilize radar technology to detect and track drones by analyzing the radar cross-section of these UAVs. Radar systems emit electromagnetic waves and analyze the echoes reflected by objects within their field of view. By detecting the unique radar signatures of drones, these systems can accurately determine their presence, location, and trajectory of drones within the monitored airspace [8].
- 4 *Visual detection* Visual detection systems rely on optical sensors, such as cameras and image processing algorithms, to visually detect and identify drones. These systems analyze visual data to recognize the distinctive shapes, movements, and features associated with drones against the background environment. Visual detection is particularly effective in environments where drones are visually observable, such as in urban areas or open airspace [9].

The article is organized as follows. Section 2 describes the state of the art for the underlying study and the contribution of the proposed model. To summarize this article, the proposed stochastic model is described in Sect. 3, followed by its analysis in Sect. 4. The suggested model's reliability indicators are presented in Sect. 5, while Sect. 6 provides an in-depth graphical representation of reliability measures. Finally, Sect. 7 concludes with suggestions for further research.

2 Review of literature

Drones, having proven their worth in battlefield scenarios, rely heavily on GPS for precise navigation and maintaining flight integrity. To ensure the ongoing success of drone missions, one pivotal technique extensively studied, as discussed in [10], is GPS anti-jamming. In response to GPS anti-jamming threats, most anti-drone systems opt for military-grade components to effectively neutralize potentially malicious drones [11, 12]. However, deploying military-grade anti-drone systems in civilian areas poses numerous challenges. Military counter-drone measures often involve the use of jamming systems to disrupt the control channels of target drones [13]. These jamming devices emit exceptionally high-strength RF signals within the drone's operating frequency band, causing communication disruptions. In the military settings, deployment sites are tightly controlled, and operators are equipped with field manuals to manage jamming conditions, enabling them to address or mitigate the side effects of jamming, as discussed in [14, 15]. Conversely, in non-military applications, employing RF jamming to counter high-speed drones risks temporarily incapacitating existing wireless network systems, including mobile access and wireless sensor networks [16].

Numerous incidents have brought to light the concerning utilization of drones for various activities, ranging from espionage and planned attacks on critical installations to unintentional damage inflicted upon both defense and civilian assets [17].

Addressing these threats, a paper outlined in [18] proposes the implementation of a cost-effective Software Defined Radio (SDR)-based system to safeguard vital areas against unauthorized drone incursions. Consequently, many national regulations strictly prohibit the non-military use of jamming systems, as highlighted in [19]. This compels civilian anti-drone systems to explore alternative methods to counter illegal or unauthorized drone activities. Despite the increasing adoption of anti-drone systems by numerous countries as part of their military arsenal, there exists a notable gap in the literature concerning the reliability analysis of such systems. Conducting reliability analyses on anti-drone systems poses several challenges, including the dynamic nature of drone threats, the complexity of integrating diverse technologies, and the need for comprehensive testing methodologies. Additionally, the lack of standardized evaluation criteria and the evolving tactics employed by malicious actors further contribute to the complexity of reliability assessment in this domain.

Abunada and Osman [20] introduced a novel design for anti-drone jamming and detection technology aimed at countering the increasing threat posed by unmanned aerial vehicles. Their innovative approach combines jamming capabilities with sophisticated detection mechanisms to effectively neutralize unauthorized drone activities. In a related effort, Shin et al. [21] proposed a drone position tracking system utilizing multiple Bluetooth Low Energy (BLE) receivers. This system offers enhanced accuracy and reliability in tracking drone movements, thereby enabling efficient monitoring and control of drone operations in various environments. In a broader exploration of future radar applications, Wang et al. [22] delved into advanced strategies, including deep intelligent learning and multi-dimensional information processing technologies. Their research emphasizes the importance of adapting radar systems to operate effectively in complex environments, enhancing combat capabilities, and developing modular, versatile, and software-based signal processing platforms to meet the evolving defense needs. Meanwhile, Khan et al. [23] conducted a comprehensive review of existing drone detection techniques, critically evaluating the state-of-the-art in this rapidly evolving field. Their work provides valuable insights into the strengths and limitations of current detection methods, paving the way for further advancements in drone detection technology.

Drone detection algorithms heavily rely on hyper-spectral images to achieve accurate and reliable identification of UAVs. Liu et al. [24] presented pioneering work in this domain in their study, where they developed a system capable of autonomously detecting and tracking drones using only a single camera. This innovative approach addresses a significant challenge in image-based drone detection: the accurate identification of small airborne objects, such as drones, amidst complex visual backgrounds. Expanding on this research, Zheng et al. [25] investigated the specific problem of air-to-air visual detection of micro drones using monocular cameras. Their research aims to enhance the capabilities of drone detection systems by focusing on the detection of smaller UAVs, which are often more challenging to detect due to their size and agility. The use of image-based techniques in their work demonstrates promising results in achieving more accurate detection and classification of micro objects as drones, surpassing the performance of alternative detection methods [26]. Furthermore, ongoing advancements in image processing and machine learning techniques continue to improve the effectiveness of image-based drone detection sys-

tems. These techniques enable the extraction of detailed features from hyper-spectral images, allowing for enhanced drone identification and classification accuracy even in complex and dynamic environments. As research in this field progresses, image-based methods are expected to play a pivotal role in the development of robust and reliable drone detection systems for various applications, including security, surveillance, and airspace management.

The literature currently lacks a comprehensive stochastic models for anti-drone systems, particularly those considering both detection and jamming technologies. Understanding the reliability and availability of these systems is paramount for their effective deployment. Despite its importance, only a handful of researchers have delved into developing mathematical models for anti-drone systems. Notably, Garcia et al. [27] proposed a simulation model for a visually based anti-drone system focused on drone detection, achieving an impressive accuracy rate of 93.40%. Similarly, Zheng et al. [25] introduced a simulation model to evaluate the accuracy of a visual detection anti-drone system. Additionally, Chen et al. [28] concentrated on dynamic modeling and simulation for an anti-drone system based on capture technology.

Reliability assessment is pivotal for the efficient and robust design of anti-drone systems incorporating both detection and jamming techniques. An efficient design necessitates an exceptionally low likelihood of component failure. Establishing the reliability of such systems involves creating a stochastic model. However, determining the most suitable stochastic model that accurately approximates the real-time system behavior poses a significant challenge. This paper addresses several challenges associated with assessing the reliability of anti-drone detection and jamming systems by introducing a comprehensive stochastic model. By doing so, it aims to provide insights into the performance and reliability of these critical security systems in diverse operational scenarios. Figure 1 illustrates the architecture of an anti-drone system.

2.1 Contribution

The significance of our research stems from the scarcity of studies addressing the reliability of intricate anti-drone systems. A comprehensive review of the existing literature reveals that no prior research has examined the reliability analysis of anti-drone architectures integrating both detection and jamming technologies. This nota-

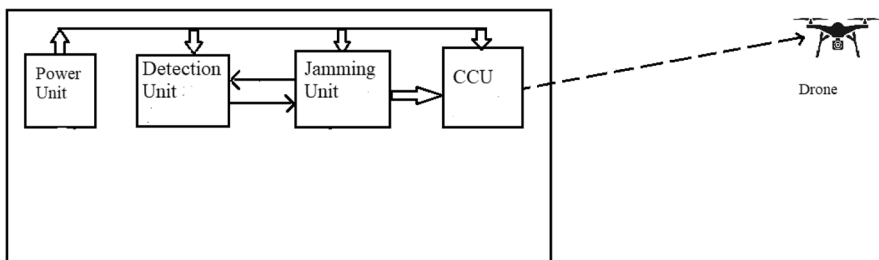


Fig. 1 Architecture of an anti-drone system

ble gap in knowledge serves as the primary motivation for our investigation into the reliability assessment of an image-based anti-drone system.

The novelty of the proposed model is twofold.

- 1 In this study, we introduce a detailed architectural framework for an anti-drone system. The existing literature lacks a work which provides an extensive state of the art on the anti-drone systems. The proposed architecture comprehensively integrates the essential functional units of an image-based anti-drone system—namely, the detection, jamming, power, and control subsystems—into a unified operational framework. Each subsystem is characterized by its distinct role and interaction within the overall system workflow.
- 2 The proposed architecture serves as the foundation for stochastic reliability modeling of the anti-drone systems. We propose a stochastic model for its reliability evaluation. The bottom level is modeled using a Reliability Block Diagram (RBD) to capture the interdependence and redundancy structure of hardware components such as detection and jamming units. The top level employs both Continuous-Time Markov Chain (CTMC) and Semi-Markov Process (SMP) formulations to represent the stochastic transitions among system operational states, incorporating component-level reliability information from the RBD model.

The selection of the CTMC and SMP frameworks is grounded in the operational behavior and time-to-failure characteristics of real-world anti-drone systems. In such systems, certain components—such as power supplies, signal processors, and communication modules—typically exhibit constant failure and repair rates during their useful life. These behaviors align well with the memoryless property of exponential distributions, making the CTMC model suitable for representing the overall operational dynamics under steady environmental and load conditions. However, other critical subsystems, particularly laser emitters, image sensors, and source modules, experience multi-phase degradation caused by thermal stress, optical fatigue, and component aging. Their time-to-failure patterns are non-exponential and better captured by phase-type or hypo-exponential distributions. For such cases, the SMP framework offers the flexibility to model arbitrary sojourn-time distributions, thereby providing a more realistic description of degradation and restoration processes that deviate from the Markovian assumption. While alternative hybrid or non-Markovian approaches (e.g., Petri nets, stochastic Petri-Markov models, or simulation-only methods) could be applied, they typically require more extensive parameter estimation and offer limited analytical tractability for steady-state reliability evaluation. This approach is particularly practical for anti-drone systems deployed in defense and surveillance applications, where some subsystems follow predictable exponential lifetimes while others demonstrate variable degradation patterns due to environmental exposure and mission duration.

To validate the analytical findings and assess the model's accuracy, a simulation-based approach is implemented. The close agreement between analytical and simulated results demonstrates the reliability and practical applicability of the proposed stochastic modeling framework.

3 Model specification

In this work, the proposed model is considered for the anti-drone system studied in [20]. The proposed model represents a hierarchical stochastic model for the anti-drone system. The main components of the anti-drone system are provided as follows:

- *Power unit (P)* It is used to supply the power to all the components of the anti-drone system. The failure of the power unit causes the complete shutdown of the system.
- *Detection unit (D)* The Detection Module (DM) is a critical component of an anti-drone system designed to identify and detect unauthorized drones flying in a specific area. Its primary function is to monitor the airspace, analyze data from various sensors, and provide early warning or alert signals when it detects potential drone threats. Here are some key aspects and components typically associated with the detection unit:
 - *Detection sensors (DS)* The module often includes various sensors to detect drones using different technologies. Common detection sensors include radar, RF detectors, acoustic sensors, electro-optical cameras, and lidar. These sensors work together to provide comprehensive coverage and multiple layers of detection. If the main detection sensor fails, the redundant detection sensor takes over its operation.
 - *Signal processing unit (SPU)* The detection data collected from sensors are processed and analyzed in real-time by a signal processing unit. This unit is responsible for filtering out false positives and distinguishing between authorized and unauthorized drones based on their characteristics and behavior.
- *Jamming unit* The Jamming Module is a crucial component of an anti-drone system designed to counteract and neutralize unauthorized drones that pose a threat. Its primary function is to disrupt or interfere with the communication and control signals of the detected drones, rendering them inoperable or causing them to return to their point of origin. Here are some key aspects and components typically associated with jamming unit :
 - *Jamming devices (JD)* The module is equipped with jamming devices that jam the downlink signals such as electromagnetic signals, RF or microwave signals, targeted at the frequency bands commonly used by drones for communication and control. If the main jamming device stops working, the redundant device takes over its operations.
 - *Jamming control unit (JCU)* A control unit manages the operation of the jamming devices. It can adjust the frequency, power level, and direction of the jamming signals based on the characteristics of the detected drones.
- *Communication and control unit (CCU)* In an anti-drone system, the CCU serves as the central component responsible for managing and coordinating the various aspects of the system. The CCU collects data from different sensors and detec-

tion systems within the anti-drone system, such as radar, lidar, cameras, acoustic sensors, and RF detectors. It then processes and fuses this data to create a comprehensive situational awareness picture.

The model contains two levels namely the top-level and bottom-level. The failure of these components are provided as follows.

Top Level At the system level, a failure is defined as the condition in which the anti-drone system becomes incapable of performing its intended detection and neutralization functions. This state is reached when:

- *Power unit (P)* The power unit supplies continuous electrical energy to all other modules. Failures typically arise due to battery exhaustion, voltage regulator malfunction, or overheating of power converters. Since this unit directly sustains all system components, its failure causes an immediate system shutdown. The preventive measures may include implementation of dual-redundant power sources, real-time voltage and temperature monitoring, and automatic switching circuits to alternate between primary and backup supplies.
- *Detection unit (D)* The detection module is responsible for identifying and classifying unauthorized drones through sensor data acquisition and signal processing. Failures may result from sensor degradation, communication interference, or processing overloads. When both the detection and jamming units fail simultaneously, rendering the system unable to either detect or respond to drone threats. The preventive measures may incorporate redundant components operating in diverse modalities (RF, radar, acoustic, and visual), periodic sensor calibration, and noise-filtering algorithms to reduce false alarms.
- *Communication and control unit (C)* The CCU acts as the system's command hub, coordinating information exchange among detection, jamming, and power units. Failures in this module can arise from communication link loss, data fusion errors, or software synchronization faults. The preventive measures may incorporate fault-tolerant communication protocols, secure wireless links, and multi-channel data fusion architectures to ensure operational continuity.

The top-level stochastic model (Fig. 2) captures these transitions between fully operational, partially degraded, and failed states. The preventive measures at this level may include the use of redundant critical components, automated fault detection, and dynamic reconfiguration protocols that isolate faulty subsystems while maintaining partial functionality. Although, the underlying model does not consider the redundancy at the top level system.

Bottom Level Figure 3 shows the block diagram of the bottom level system. Each subsystem at the bottom level is associated with specific failure mechanisms influenced by operational load, environmental stress, and hardware limitations. Their individual failure conditions and mitigation measures are detailed as follows:

- *Detection sensors (DS)* The detection sensor is responsible for identifying and classifying unauthorized drones through sensor data acquisition and signal processing. Failures may result from sensor degradation, communication interfer-

Fig. 2 Stochastic model for the top level system

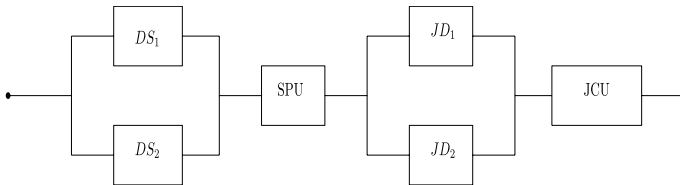
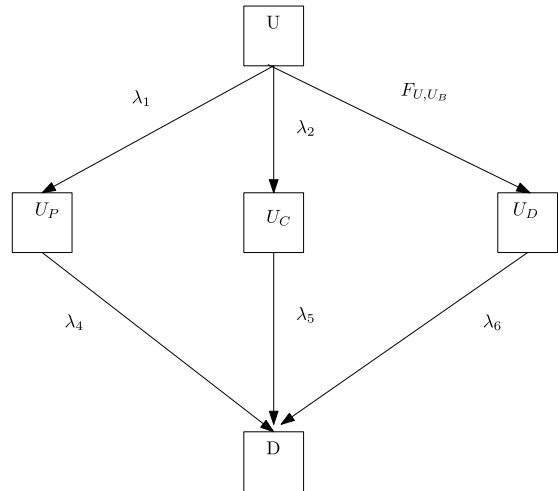


Fig. 3 RBD of bottom level system

ence, or processing overloads. For the preventive measures, we have introduced redundant sensors (DS_1 , DS_2) operating in diverse modalities (RF, radar, acoustic, and visual), periodic sensor calibration, and noise-filtering algorithms to reduce false alarms. The SPU processes raw data to distinguish legitimate drones from background noise. The failures stem from software glitches, memory corruption, or thermal overloads during intensive data handling.

- Jamming unit** The jamming module neutralizes detected drones by emitting electromagnetic interference signals. The failure of jamming devices (JD) may occur due to transmitter burnout, frequency mismatch, or antenna damage. We have considered redundant jamming transmitters (JD_1 , JD_2) to sustain continuous operation. The jamming control Unit (JCU) controls signal parameters such as power, direction, and modulation. Failures are often due to software errors or signal feedback instability.

4 Reliability analysis

This section presents a comprehensive reliability analysis of the proposed anti-drone system, which is structured into two levels: a bottom-level RBD model and a top-level stochastic model. The bottom-level model focuses on the key hardware components of the system and evaluates their combined reliability using series–parallel

configurations. The resulting reliability of this subsystem is then incorporated as an input parameter for the top-level analysis, which characterizes the overall system behaviour through stochastic modeling. Depending on the assumed failure-time distributions of the components, the stochastic formulation is developed using both CTMC and SMP frameworks. Time-dependent analyses are performed for each model to derive the corresponding reliability measures and to capture the dynamic performance of the anti-drone system under varying operational conditions.

The SMP framework has been adopted in this study because it provides a more realistic representation of the stochastic behaviour of the anti-drone system compared to a CTMC. In a CTMC model, the sojourn time in each state is assumed to follow an exponential distribution, implying a constant transition rate and the memoryless property. However, in practical engineering systems, particularly those involving electromechanical and optical subsystems, such assumptions are often restrictive. The SMP formulation relaxes this constraint by allowing the sojourn time distributions to be non-exponential, thereby capturing state-dependent and time-varying failure mechanisms more accurately. This flexibility makes the SMP model suitable for representing the mixed operational dynamics of the anti-drone system, which includes both instantaneous and delayed transition behaviours.

The lifetime distributions of individual components have been chosen based on their physical failure characteristics. The source and laser components are modelled using a hypo-exponential distribution because their degradation process typically occurs in multiple sequential stages, such as gradual optical decay followed by complete failure. The hypo-exponential distribution, being a generalization of the exponential distribution with two or more distinct rate parameters, effectively represents such multi-phase failure phenomena where the total lifetime is the sum of multiple exponential phases with different mean rates.

In contrast, other components—such as sensors, control units, and power electronics—are assumed to have exponentially distributed failure times. This assumption is justified because these components are considered to operate within their *useful life period*, during which the failure rate remains approximately constant. The exponential model thus provides a reasonable and mathematically tractable representation of their random failures under steady operating conditions. Moreover, empirical studies and reliability handbooks for electronic systems indicate that the exponential assumption is valid for components that are not subject to significant aging, burn-in, or wear-out effects. Consequently, the combined use of exponential and hypo-exponential distributions under the SMP framework ensures that both simple and complex failure mechanisms are accurately captured, providing a balanced trade-off between model realism and analytical tractability.

4.1 Reliability analysis of bottom level system

The reliability of the bottom-level RBD model is evaluated by considering the time-to-failure behavior of each component. The reliability function for an individual component, $R(t)$, is defined as the probability that the component operates without failure up to time t :

$$R(t) = P(T > t),$$

where T is a random variable representing the time to failure. The failure of components of the anti-drone system are more realistically modeled using the *Weibull distribution*. The *Weibull distribution* is a versatile and widely adopted model in reliability engineering because it can accurately represent different failure behaviors observed in complex electromechanical systems. Unlike the exponential distribution, which assumes a constant failure rate, the Weibull model allows the failure rate to vary with time, making it suitable for components that undergo wear-out, degradation, or early-life failures. In the context of anti-drone systems, components such as sensors, signal processors, and jamming modules are exposed to thermal stress, environmental fluctuations, and operational fatigue, leading to non-constant failure patterns. Therefore, adopting the Weibull distribution provides a more realistic and flexible representation of component reliability, allowing for improved accuracy in system-level reliability estimation.

For a component following a Weibull distribution with shape parameter β and scale parameter η , the reliability function is given by

$$R(t) = e^{-(t/\eta)^\beta}.$$

After determining the reliability of each component, the overall reliability of the bottom-level RBD, which includes redundancy in the detection and jamming units, can be expressed as:

$$R_b(t) = \left[1 - \left(1 - e^{-(t/\eta_d)^{\beta_d}} \right)^2 \right] \times \left[1 - \left(1 - e^{-(t/\eta_j)^{\beta_j}} \right)^2 \right] \times e^{-((t/\eta_{spu})^{\beta_{spu}} + (t/\eta_{jcu})^{\beta_{jcu}})}. \quad (1)$$

Here, $\eta_d, \eta_j, \eta_{spu}, \eta_{jcu}$ denote the scale parameters (characteristic lifetimes), and $\beta_d, \beta_j, \beta_{spu}, \beta_{jcu}$ denote the shape parameters for the detection sensor, jamming device, signal processing unit, and jamming control unit, respectively.

4.2 Reliability analysis of top level system

This section presents the stochastic modeling of the top-level system, which comprises three major subsystems: the power unit, detection unit, and communication unit. In this framework, it is assumed that while some components exhibit exponentially distributed failure times, others may follow non-exponential lifetime distributions due to their complex degradation behaviour. Consequently, the overall stochastic process can be formulated using either a CTMC or a SMP, depending on the specific failure-time characteristics of the components under consideration.

4.2.1 Semi-markov process model

The suggested model allows for the assumption that the component failure times would follow exponential distributions. However, a hypo-exponential distribution is used to simulate the lifetime of the detection component. Table 1 describes the distributions of sojourn times associated with each state for the proposed model.

The analysis of the proposed model is described in this section. Let $\{X(t), t \geq 0\}$ be the stochastic process for the underlying system, where $X(t)$ denotes the state of the system at any time t . Due to the hypo-exponential distribution for the mean sojourn time of some states, and Markov attributes of the time epochs, the underlying stochastic process can be appropriately modeled by a SMP [29]. The state space of the proposed stochastic model is given as follows:

$$\Omega = \{U, U_P, U_C, U_D, D\}.$$

To obtain the steady-state probabilities, a two stage method is employed. For this method, the elements of kernel matrix $K(t)$ defined as $K_{m,n}(t) = P\{Y_1 = n, t_1 \leq t \mid Y_0 = m\}$, where $m, n \in \Omega$ and $\{(Y_n, t_n), n \geq 0\}$ is the underlying Markov renewal sequence of random variables. Alternatively, $K_{m,n}(t)$ can be understood as the probability that if the SMP has just entered state m ; the next transition occurs within time t and the next state will be n . Let $F_{m,n}$ be the cumulative distribution function (CDF) for the transition from state m to n of the state space. The entries of matrix $K(t)$ is further computed as follows:

Let

$$\Lambda_1 = \frac{\lambda_3^1}{\lambda_3^2 - \lambda_3^1}, \quad \Lambda_2 = \frac{\lambda_3^2}{\lambda_3^2 - \lambda_3^1},$$

$$A_1 = \lambda_1 + \lambda_2 + \lambda_3^1, \quad A_2 = \lambda_1 + \lambda_2 + \lambda_3^2$$

Table 1 Distributions of sojourn times in the proposed stochastic model

CDF	Distribution	CDF	Distribution
F_{U,U_P}	Exp (λ_1)	F_{U,U_C}	Exp (λ_2)
F_{U,U_D}	Hypo-Exp (λ_3^1, λ_3^2)	$F_{U_P,D}$	Exp (λ_4)
$F_{U_C,D}$	Exp (λ_5)	$F_{U_D,D}$	Exp (λ_6)

$$\begin{aligned}
K_{U,U_P}(t) &= \int_0^t (1 - F_{U,U_C}(t))(1 - F_{U,U_D}(t))dF_{U,U_P}(t) \\
&= \lambda_1 \left[\frac{\Lambda_2(1 - e^{-(A_1)t})}{A_1} - \frac{\Lambda_1(1 - e^{-(A_2)t})}{A_2} \right], \\
K_{U,U_C}(t) &= \int_0^t (1 - F_{U,U_P}(t))(1 - F_{U,U_D}(t))dF_{U,U_C}(t) \\
&= \lambda_2 \left[\frac{\Lambda_2(1 - e^{-(A_1)t})}{A_1} - \frac{\Lambda_1(1 - e^{-(A_2)t})}{A_2} \right], \\
K_{U,U_D}(t) &= \int_0^t (1 - F_{U,U_P}(t))(1 - F_{U,U_C}(t))dF_{U,U_D}(t) \\
&= \frac{\lambda_3^1 \lambda_3^2}{\lambda_3^2 - \lambda_3^1} \left[\frac{(1 - e^{-(A_1)t})}{A_1} - \frac{(1 - e^{-(A_2)t})}{A_2} \right], \\
K_{U_D,D}(t) &= \int_0^t dF_{U_D,D}(t) = (1 - e^{-\lambda_6 t}), \\
K_{U_C,D}(t) &= \int_0^t dF_{U_C,D}(t) = (1 - e^{-\lambda_5 t}), \\
K_{U_P,D}(t) &= \int_0^t dF_{U_P,D}(t) = (1 - e^{-\lambda_4 t}).
\end{aligned}$$

We use the Laplace transform $\mathcal{L}\{f(t)\}(s) = \tilde{f}(s) = \int_0^\infty e^{-st} f(t) dt$. A useful transform is

$$\mathcal{L}\left\{\frac{1 - e^{-at}}{a}\right\}(s) = \frac{1}{a} \left(\frac{1}{s} - \frac{1}{s+a} \right) = \frac{1}{as} - \frac{1}{a(s+a)}.$$

Applying $\mathcal{L}\{\cdot\}$ to each kernel element yields

$$\begin{aligned}
\tilde{K}_{U,U_P}(s) &= \lambda_1 \left[\Lambda_2 \left(\frac{1}{A_1 s} - \frac{1}{A_1(s+A_1)} \right) - \Lambda_1 \left(\frac{1}{A_2 s} - \frac{1}{A_2(s+A_2)} \right) \right], \\
\tilde{K}_{U,U_C}(s) &= \lambda_2 \left[\Lambda_2 \left(\frac{1}{A_1 s} - \frac{1}{A_1(s+A_1)} \right) - \Lambda_1 \left(\frac{1}{A_2 s} - \frac{1}{A_2(s+A_2)} \right) \right], \\
\tilde{K}_{U,U_D}(s) &= \frac{\lambda_3^1 \lambda_3^2}{\lambda_3^2 - \lambda_3^1} \left(\frac{1}{A_1 s} - \frac{1}{A_1(s+A_1)} - \frac{1}{A_2 s} + \frac{1}{A_2(s+A_2)} \right),
\end{aligned}$$

and for the degraded-to-failed kernels

$$\tilde{K}_{U_P,D}(s) = \frac{1}{s} - \frac{1}{s + \lambda_4}, \quad \tilde{K}_{U_C,D}(s) = \frac{1}{s} - \frac{1}{s + \lambda_5}, \quad \tilde{K}_{U_D,D}(s) = \frac{1}{s} - \frac{1}{s + \lambda_6}.$$

All other $\tilde{K}_{m,n}(s)$ are zero in the current model.

The diagonal matrix $E(t)$ has entries

$$E_{ii}(t) = 1 - \sum_j K_{ij}(t),$$

i.e., the survival (no-transition) probability in state i up to time t . Taking Laplace transforms and using linearity,

$$\tilde{E}_{ii}(s) = \mathcal{L}\{E_{ii}(t)\}(s) = \frac{1}{s} - \sum_j \tilde{K}_{ij}(s).$$

Hence, $\tilde{E}(s)$ is diagonal with known diagonal entries $\frac{1}{s} - \sum_j \tilde{K}_{ij}(s)$.

The transform-domain equation is

$$\tilde{V}(s) = \tilde{E}(s) + \tilde{K}(s) \tilde{V}(s),$$

which rearranges to

$$(I - \tilde{K}(s)) \tilde{V}(s) = \tilde{E}(s).$$

Provided $I - \tilde{K}(s)$ is invertible for the s of interest, we obtain the formal solution

$$\tilde{V}(s) = (I - \tilde{K}(s))^{-1} \tilde{E}(s).$$

This gives the Laplace–Stieltjes transform of the transient fundamental matrix $V(t)$.

The time-domain fundamental matrix is obtained by the inverse Laplace transform:

$$V(t) = \mathcal{L}^{-1}\{\tilde{V}(s)\}(t).$$

Finally, with the initial distribution $P(0)$ (row vector), the transient state probabilities are

$$P(t) = P(0) V(t).$$

Finally, since D is absorbing (no outgoing transitions in the present model), the probability of being in D at time t is obtained by conservation of total probability:

$$P_D(t) = 1 - P_U(t) - P_{U_P}(t) - P_{U_C}(t) - P_{U_D}(t). \quad (2)$$

4.3 Continuous time Markov chain model

By relaxing the assumption of non-exponential distribution, the proposed model will convert to a CTMC. In this model, it is assumed that the mean sojourn time of all the states will follow an exponential distribution. Let $P_i(t)$, $i \in \Omega$ be the probability that the system is in state i at any time instance t .

4.4 Time-dependent solution of the CTMC

Let $\lambda = \lambda_1 + \lambda_2 + \lambda_3$. The forward Kolmogorov equations for the state probabilities $P_U(t)$, $P_{U_P}(t)$, $P_{U_C}(t)$, $P_{U_D}(t)$, $P_D(t)$ are

$$\begin{aligned}\frac{dP_U}{dt} &= -\lambda P_U(t), \\ \frac{dP_{U_P}}{dt} &= -\lambda_4 P_{U_P}(t) + \lambda_1 P_U(t), \\ \frac{dP_{U_C}}{dt} &= -\lambda_5 P_{U_C}(t) + \lambda_2 P_U(t), \\ \frac{dP_{U_D}}{dt} &= -\lambda_6 P_{U_D}(t) + \lambda_3 P_U(t), \\ \frac{dP_D}{dt} &= \lambda_4 P_{U_P}(t) + \lambda_5 P_{U_C}(t) + \lambda_6 P_{U_D}(t),\end{aligned}$$

with initial condition $P_U(0) = 1$ and $P_{U_P}(0) = P_{U_C}(0) = P_{U_D}(0) = P_D(0) = 0$.

After solving the above system of equations, we obtain

$$P_U(t) = e^{-\lambda t}.$$

Then the three driven linear first-order equations admit closed-form solutions. Assuming the non-resonant case (i.e., $\lambda \neq \lambda_4, \lambda_5, \lambda_6$), we obtain

$$P_{U_P}(t) = \frac{\lambda_1}{\lambda - \lambda_4} \left(e^{-\lambda_4 t} - e^{-\lambda t} \right), \quad (3)$$

$$P_{U_C}(t) = \frac{\lambda_2}{\lambda - \lambda_5} \left(e^{-\lambda_5 t} - e^{-\lambda t} \right), \quad (4)$$

$$P_{U_D}(t) = \frac{\lambda_3}{\lambda - \lambda_6} \left(e^{-\lambda_6 t} - e^{-\lambda t} \right). \quad (5)$$

Finally, $P_D(t)$ follows from probability conservation $\sum_i P_i(t) = 1$:

$$P_D(t) = 1 - P_U(t) - P_{U_P}(t) - P_{U_C}(t) - P_{U_D}(t).$$

Equivalently, substituting the expressions above,

$$\begin{aligned}P_D(t) &= 1 - e^{-\lambda t} - \frac{\lambda_1}{\lambda - \lambda_4} \left(e^{-\lambda_4 t} - e^{-\lambda t} \right) - \frac{\lambda_2}{\lambda - \lambda_5} \left(e^{-\lambda_5 t} - e^{-\lambda t} \right) \\ &\quad - \frac{\lambda_3}{\lambda - \lambda_6} \left(e^{-\lambda_6 t} - e^{-\lambda t} \right).\end{aligned} \quad (6)$$

The steady-state probabilities (q_i) of the system are computed with the help of time-dependent probabilities of the system using $\lim_{t \rightarrow \infty} P_i(t) = q_i$ and $\lim_{t \rightarrow \infty} P'_i(t) = 0$.

5 Reliability measures

In this section, the reliability of the top level and the bottom level will be computed. The anti-drone system functions hierarchically, with the bottom level representing the hardware configuration and the top level depicting the system's operational behaviour. At the bottom level, key components such as the power unit, detection sensors, signal processing unit, and jamming module operate in coordination to detect, track, and neutralize unauthorized drones. Redundant components are incorporated in critical units, and their interactions are modeled using a RBD to capture series-parallel dependencies. The top-level model describes the stochastic transitions among operational, degraded, and failed states that arise due to component-level failures. When all components exhibit exponentially distributed failure times, the system behaviour follows a CTMC. However, for subsystems with multi-phase degradation, such as laser or source modules, non-exponential lifetimes are considered, and the system is modeled using a SMP. This hierarchical modeling structure provides a logical foundation for the reliability assumptions adopted in the analysis.

5.1 Reliability measures for the bottom level model

- *Reliability of the bottom level system*

$$R_b(t) = \left[1 - \left(1 - e^{-(t/\eta_d)^{\beta_d}} \right)^2 \right] \times \left[1 - \left(1 - e^{-(t/\eta_j)^{\beta_j}} \right)^2 \right] \times e^{-((t/\eta_{spu})^{\beta_{spu}} + (t/\eta_{jcu})^{\beta_{jcu}})} \quad (7)$$

- *Mean Time To Failure (MTTF)* The Mean Time To Failure (MTTF) represents the expected operational lifetime of a system or component before it fails. For the proposed system, the MTTF is computed as follows:

$$\text{MTTF} \approx \int_0^{t_{\max}} R_b(t) dt, \quad (8)$$

where $t_{\max}$ is chosen sufficiently large such that $R_b(t_{\max}) \rightarrow 0$.

5.2 Reliability measures for the top level model

In the preceding section, the reliability of the detection system was evaluated using the RBD approach for the bottom-level configuration.

- 1 The time dependent probabilities of the top level model being in any state is provided as follows for semi-Markov and CTMC cases:

- *Semi-Markov model*

$$P_D(t) = 1 - P_U(t) - P_{U_P}(t) - P_{U_C}(t) - P_{U_D}(t). \quad (9)$$

- *CTMC model*

$$P_U(t) = e^{-\lambda t}, \quad (10)$$

$$P_{U_P}(t) = \frac{\lambda_1}{\lambda - \lambda_4} \left(e^{-\lambda_4 t} - e^{-\lambda t} \right), \quad (11)$$

$$P_{U_C}(t) = \frac{\lambda_2}{\lambda - \lambda_5} \left(e^{-\lambda_5 t} - e^{-\lambda t} \right), \quad (12)$$

$$P_{U_D}(t) = \frac{\lambda_3}{\lambda - \lambda_6} \left(e^{-\lambda_6 t} - e^{-\lambda t} \right), \quad (13)$$

$$P_D(t) = 1 - e^{-\lambda t} - \frac{\lambda_1}{\lambda - \lambda_4} \left(e^{-\lambda_4 t} - e^{-\lambda t} \right) - \frac{\lambda_2}{\lambda - \lambda_5} \left(e^{-\lambda_5 t} - e^{-\lambda t} \right) - \frac{\lambda_3}{\lambda - \lambda_6} \left(e^{-\lambda_6 t} - e^{-\lambda t} \right). \quad (14)$$

- 2 The reliability of the top level system is given as follows:

$$R(t) = 1 - P_D(t). \quad (15)$$

6 Numerical illustration

In this section, numerical investigations are carried out to examine the viability of the suggested model in order to attain the steady-state availability and reliability outcomes.

6.1 Sensitivity analysis of the bottom level model

The MTBF values reported in Table 2 are representative ranges drawn from reliability handbooks and published tables. They are provided to give realistic parameter choices for numerical illustrations and sensitivity studies in stochastic reliability models. Actual MTBF for a specific component depends on: (i) component grade (commercial vs. military/aerospace), (ii) environmental stresses (temperature, vibration, humidity), (iii) duty cycle and loading, (iv) derating and thermal management, and (v) the failure counting / test standard used (e.g., MIL-HDBK-217, Telcordia).

Table 2 Representative MTBF values for anti-drone system components

Component	MTBF (hours)	References
Detection sensor (DS)	100,000–660,000	[30, 31]
Jamming device (JD)	500–2000	[32, 33]
Signal processing unit (SPU)	30,000–400,000	[34, 35]
Jamming control unit (JCU)	50,000–150,000	[36, 37]
Power supply unit (P)	40,000–200,000	[38, 39]

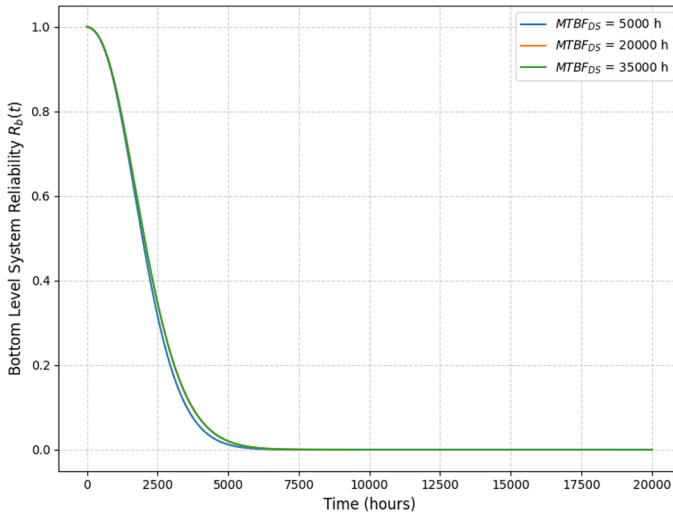
**Fig. 4** Reliability of bottom-level system for different MTBF values of detection sensor component

Figure 4 illustrates the reliability function $R_b(t)$ for varying MTBF values of the detection sensor, while maintaining a constant shape parameter β_d . It is evident from the curves that an increase in the MTBF of the detection sensor leads to an overall improvement in system reliability. A similar trend is observed in Figs. 6 and 7, which depict the effect of MTBF variations for the jamming device and the SPU, respectively. However, the reliability curves corresponding to the detection sensor and SPU exhibit relatively smaller differences across different MTBF values, indicating that variations in these components have a comparatively lower influence on the overall reliability of the bottom-level system compared to the jamming device.

Figure 5 depicts the variation of system reliability over time for different values of the Weibull shape parameter (β_d) of the detection sensor. It is observed that as β_d increases, the reliability curve becomes steeper, indicating a faster degradation rate and dominant wear-out behavior. Conversely, smaller β_d values correspond to early-life or random failure characteristics, resulting in a slower reliability decay during the initial operational period.

The computed MTTF values presented in Table 3 shows a positive correlation between the MTBF of the components and the overall system lifetime. As the MTBF increases, the system MTTF also increases proportionally, indicating that improvements in the component's reliability directly enhance the operational longevity of the bottom-level anti-drone system.

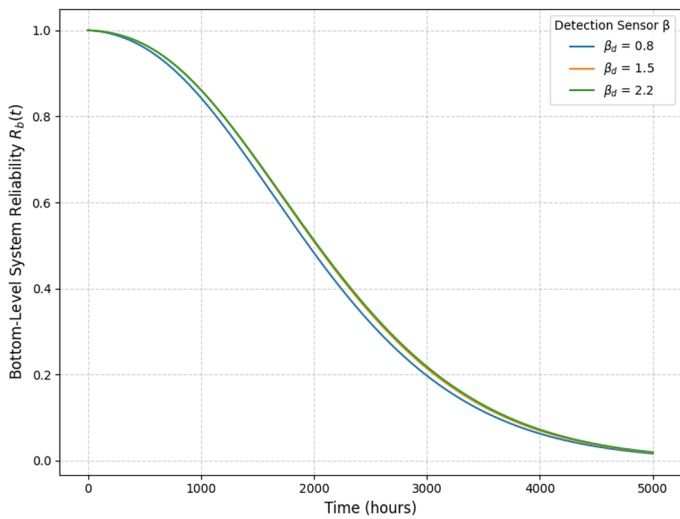


Fig. 5 Reliability of bottom-level system for different β values of detection sensor component

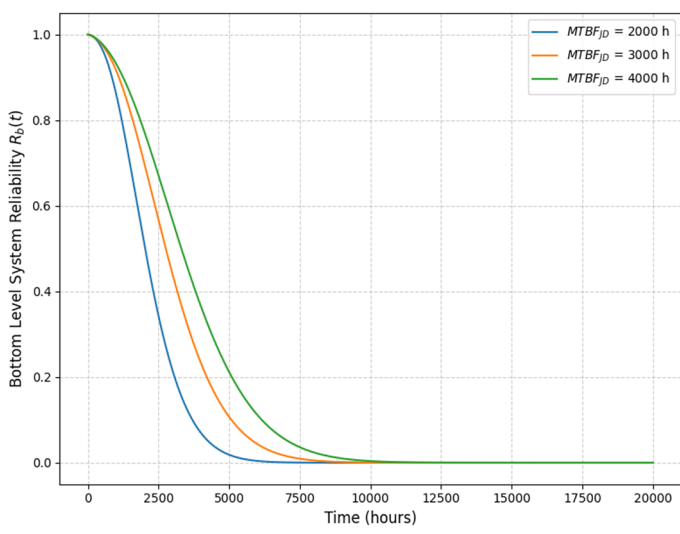


Fig. 6 Reliability of bottom-level system for different MTBF values of jamming device component

6.2 Sensitivity analysis of the top level model

Table 4 comprises the values of the parameters required for producing the results. It's crucial to recall that these numbers are selected merely for the sake of numerical illustration. Some of the parameters in Table 4 are referred from the work [40]. Due to the unavailability of the existing literature, rest of the parameters have been assumed in order to carry out the analysis.

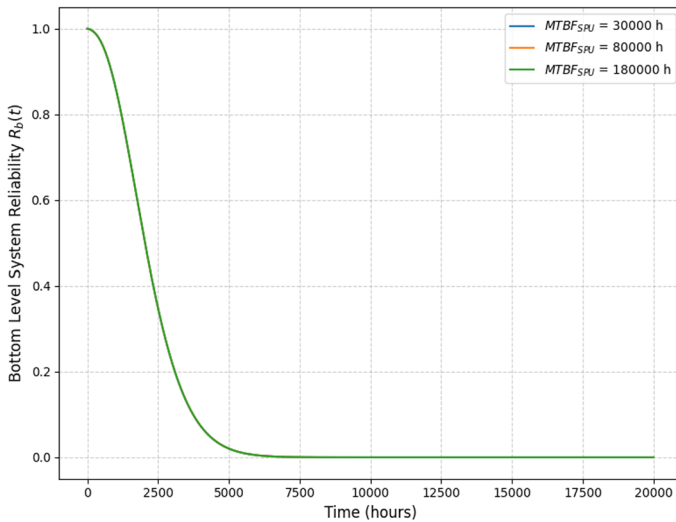


Fig. 7 Reliability of bottom-level system for different MTBF values of SPU component

Table 3 System MTTF corresponding to different MTBF values of the detection sensor

Jamming device MTBF (hours), $\beta = 1.5$	System MTTF (hours)
2000	2178.15
3000	2960.15
4000	3550.80
Detection sensor MTBF (hours), $\beta = 1.5$	System MTTF (hours)
5000	2101.20
20000	2191.91
35000	2193.74
SPU MTBF (hours), $\beta = 1.5$	System MTTF (hours)
30000	2193.49
80000	2194.15
180000	2194.19

Table 4 Default values of parameters considered for the numerical illustration and simulation

Parameters	Values	Parameters	Values
λ_1	0.2/s	λ_2	0.15/s
λ_3	0.4/s	λ_4	0.2/s
λ_5	0.31/s	λ_6	0.42/s

The time-dependent state probabilities presented in Figure 8 illustrate the dynamic behavior of the anti-drone system over time. Initially, the system is fully operational ($P_U(0) = 1$), and as failures occur, the probabilities of the degraded states ($P_{U_P}(t)$, $P_{U_C}(t)$, and $P_{U_D}(t)$) increase transiently before gradually decaying to zero. The probability of the failed state $P_D(t)$ increases monotonically with time and asymptotically approaches unity, indicating that the system ultimately reaches an absorbing failure condition. This trend confirms the non-repairable nature of the

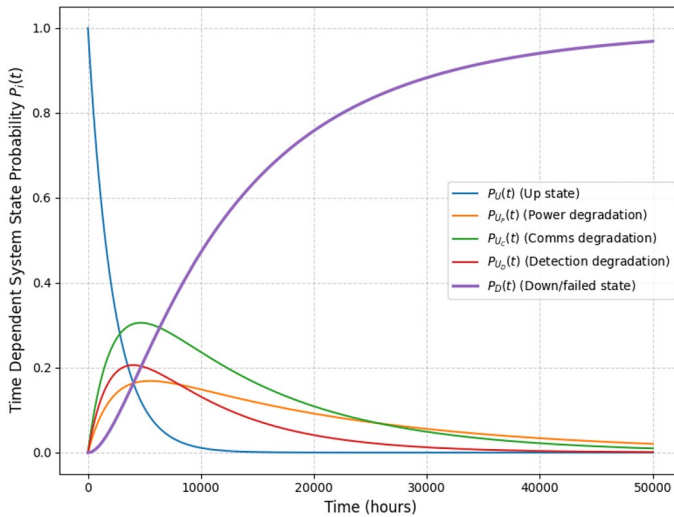


Fig. 8 Time dependent probabilities of top level CTMC model

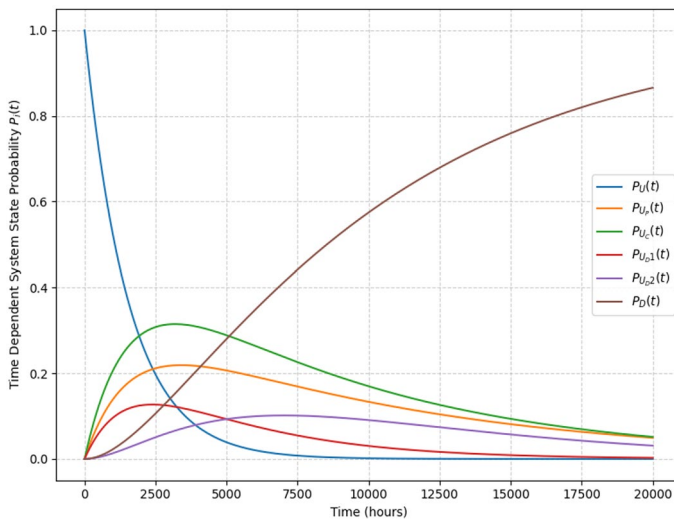


Fig. 9 Time dependent probabilities of top level SMP model

modeled system, wherein once a failure occurs, the system cannot return to its operational state and eventually settles in the absorbing down state.

Figure 9 presents the transient state probabilities obtained from the SMP model using a phase-type representation of the hypo-exponential transitions. The numerical results demonstrate that the probability of the system being in the fully operational state $P_U(t)$ gradually decreases over time, while the probability of the absorbing failure state $P_D(t)$ approaches unity. These curves effectively capture the temporal reliability behaviour of the anti-drone system under stochastic operating conditions.

Figure 10 compares the reliability profiles of the anti-drone system modeled using CTMC and SMP frameworks under identical MTBF conditions. It can be observed that the SMP model consistently yields slightly lower reliability values than the CTMC model, particularly in the intermediate time range, due to the inclusion of hypo-exponential sojourns that better capture non-exponential failure behaviour. This indicates that the SMP model provides a more realistic representation of component degradation and repair dynamics in practical anti-drone systems.

6.3 Comparison of analytical and simulated results

To ensure the validity and accuracy of the analytical stochastic model, a comprehensive simulation-based approach was employed for both the CTMC and SMP formulations of the proposed anti-drone system. The simulation model acts as an independent verification tool that replicates the stochastic behaviour of the system under identical reliability parameters as those used in the analytical computations (Table 4). The procedure begins by initializing the system in a fully operational state, followed by the generation of random failure times for each component according to their respective probability distributions. For the CTMC-based model, exponential distributions are used to represent the sojourn times between transitions, whereas for the SMP-based model, both exponential and hypo-exponential distributions are incorporated to capture complex multi-phase degradation behaviour.

The system state then advances according to the transition probabilities derived from the rate matrix Q , continuing until the failure state is reached or the observation horizon is exceeded. This process is repeated for a large number of independent trials (typically $N \geq 1000$), and at each time step, the reliability function $R(t)$ is estimated as the ratio of systems remaining operational to the total number of simulated runs. Repeating these trials yields empirical estimates of the reliability and MTTF, which are then compared against the analytical results to verify the consistency and robustness of the proposed stochastic reliability framework. Furthermore, a t -distri-

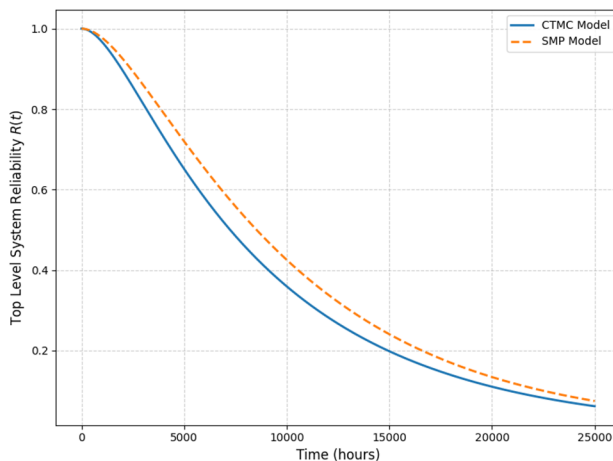


Fig. 10 Comparison of analytical results for SMP and CTMC models

bution-based statistical test is conducted to construct 95% confidence intervals for the simulated reliability values, ensuring that the observed deviations remain within statistically acceptable limits and thereby confirming the accuracy of the simulation model for validation purposes.

At each time interval, the reliability function $R(t)$ is estimated as the ratio of the number of systems that remain operational to the total number of simulation runs. The results are averaged over all trials to obtain the mean reliability curve, while the corresponding standard deviation is computed to determine the level of uncertainty in the simulation estimates. A t -distribution test is then applied to construct a 95% confidence interval (C.I.) for the reliability values, accounting for sampling variation and finite simulation size. The C.I. for the 95% accuracy of the results can be calculated by:

$$C.I. = \bar{X} \pm \frac{s * t_{0.05, k-1}}{\sqrt{k}}$$

where $\bar{X}$ is sample mean, s is the standard deviation, $t_{0.05, k-1}$ is tabulated value for 95% C.I. and $k - 1$ degree of freedom, and k is sample size.

To quantitatively evaluate the deviation between the simulation and analytical results, we have computed the relative error (in percentage) at each data point using the formula:

$$\text{Relative Error} = \frac{|\text{Simulation} - \text{Analytical}|}{\text{Analytical}} \times 100\%.$$

The computed confidence bounds confirm that the simulated results lie within a narrow range of the analytical reliability values for both CTMC and SMP models, thereby validating the accuracy and robustness of the proposed stochastic reliability framework.

Comparisons between theoretical and simulated results for the reliability measures of both CTMC and SMP models are presented in Figs. 11 and 12. Figure 11 illustrates the comparison between analytical and simulated $R(t)$ values over time t for the CTMC model. Meanwhile, Fig. 12 depicts the behavior of the $R(t)$ for SMP model. The graph showcases the comparison between the analytical and simulated results. In these visual representations, solid lines represent the findings from the analysis, while dotted lines represent the simulated outcomes. Vertical lines indicate the confidence interval. These graphs demonstrate a strong correspondence between the results obtained from both methods, thereby confirming the validity of the hypothesized model.

The simulation results were compared with the analytical reliability measures obtained from the CTMC and SMP models. The close agreement between analytical and simulated reliability curves (with errors below 1%) demonstrates that the simulation effectively validates the theoretical model. The underlying assumption of statistically independent component failures and exponentially or hypo-exponentially distributed sojourn times ensures the simulation remains consistent with the analyti-

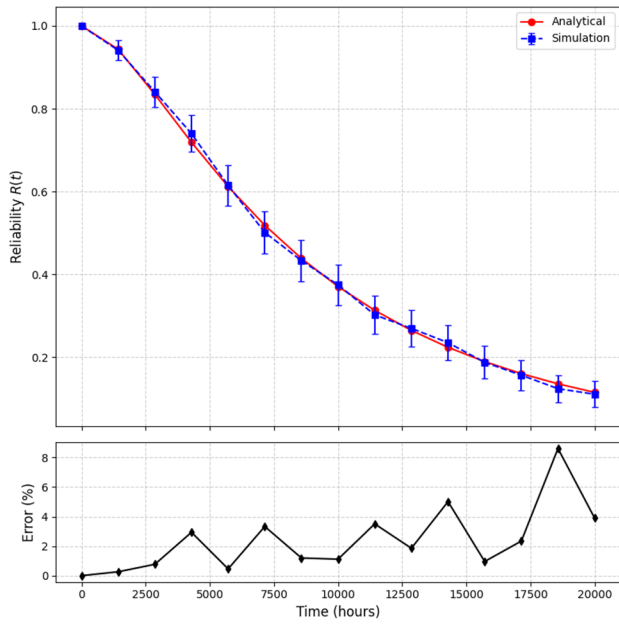


Fig. 11 Comparison of analytical and simulated results for CTMC model

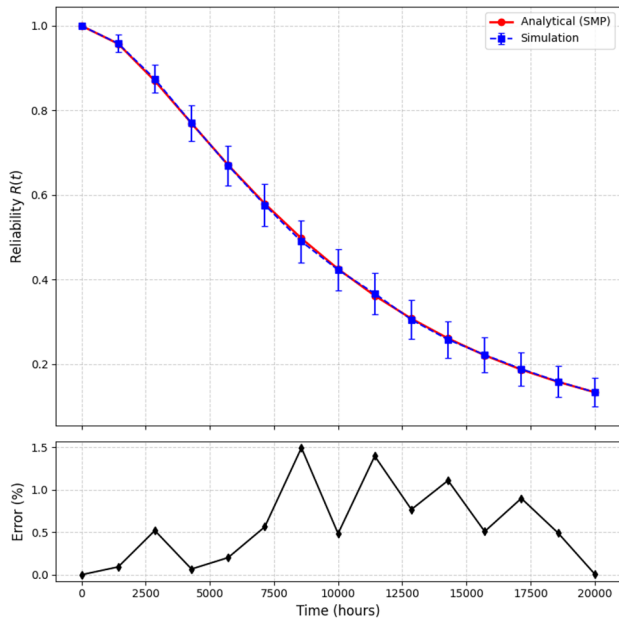


Fig. 12 Comparison of analytical and simulated results for SMP model

cal framework. This validation confirms the robustness of the proposed stochastic modeling approach for practical reliability assessment of anti-drone systems.

7 Conclusion and future scope

This study presents a comprehensive reliability framework for image-based anti-drone systems that integrate detection and jamming technologies. By employing both CTMC and SMP models, the proposed approach effectively captures the stochastic behavior of system states under diverse operational conditions. The inclusion of a hierarchical structure—comprising a bottom-level RBD and a top-level stochastic model—enables a realistic assessment of component interdependence, redundancy, and system-level transitions. The numerical and simulation analyses confirm that the proposed stochastic modeling approach accurately reflects real-world performance. A close agreement between analytical and simulated results validates the robustness of the framework. The findings highlight several important insights for enhancing system reliability:

- The failure rates of detection and jamming units significantly influence overall system reliability, emphasizing the necessity of redundant sensors and jamming devices in critical operations.
- The SMP-based reliability estimation provides a more realistic evaluation compared to the CTMC model, especially for components exhibiting non-exponential or multi-phase degradation patterns.
- The hierarchical modeling approach demonstrates that component-level reliability improvements (e.g., in the power or control unit) can produce a nonlinear enhancement in system-level reliability, supporting the use of multi-level reliability optimization strategies.

Overall, the proposed stochastic framework provides a quantitative foundation for the design and reliability improvement of modern anti-drone systems, contributing to safer and more resilient counter-drone technologies.

In future work, the model will be extended to incorporate random environmental influences (e.g., temperature variation, electromagnetic interference) that affect failure and repair rates. Furthermore, a comprehensive sensitivity analysis will be conducted to identify the most critical parameters influencing reliability. The framework may also be expanded using advanced stochastic–simulation hybrid approaches to model time-dependent degradation processes, enabling predictive maintenance and adaptive reliability management in dynamic operational environments.

Funding Not applicable.

Data availability Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Abualigah, L., Diabat, A., Sumari, P., Gandomi, A.H.: Applications, deployments, and integration of internet of drones (iod): a review. *IEEE Sens. J.* **21**(22), 25532–25546 (2021)
2. Kong, P.-Y.: A survey of cyberattack countermeasures for unmanned aerial vehicles. *IEEE Access* **9**, 148244–148263 (2021)
3. Kumar, C., Mohanty, S.: Current trends in cyber security for drones. In: 2021 International Carnahan Conference on Security Technology (ICCST), pp. 1–5 (2021). IEEE
4. Jackman, A.: Consumer drone evolutions: trends, spaces, temporalities, threats. *Defense Secur. Anal.* **35**(4), 362–383 (2019)
5. Beel, J.J.: Anti-uav defense for ground forces and hypervelocity rocket lethality models. PhD thesis, Monterey, California. Naval Postgraduate School (1992)
6. Kang, B., Ahn, H., Choo, H.: A software platform for noise reduction in sound sensor equipped drones. *IEEE Sens. J.* **19**(21), 10121–10130 (2019)
7. Kaplan, B., Kahraman, İ., Ekti, A.R., Yarkan, S., Görçün, A., Özdemir, M.K., Çirpan, H.A.: Detection, identification, and direction of arrival estimation of drone FHSS signals with uniform linear antenna array. *IEEE Access* **9**, 152057–152069 (2021)
8. Kuschel, H., Cristallini, D., Olsen, K.E.: Tutorial: passive radar tutorial. *IEEE Aerosp. Electron. Syst. Mag.* **34**(2), 2–19 (2019)
9. Wang, Y., Chen, Y., Choi, J., Kuo, C.-C.J.: Towards visible and thermal drone monitoring with convolutional neural networks. *APSIPA Trans. Signal Inf. Process.* **8**, 5 (2019)
10. Wurth, T.J., Wells, J.S.: A global positioning system (gps) interference electronics support measure (esm) payload system for unmanned aerial vehicles (uavs). In: *Unattended/Unmanned Ground, Ocean, and Air Sensor Technologies and Applications VI*, vol. 5417, pp. 218–226 (2004). SPIE
11. Kapoulas, I.K., Hatziefremidis, A., Baldoukas, A., Valamontes, E.S., Statharas, J.: Small fixed-wing UAV radar cross-section signature investigation and detection and classification of distance estimation using realistic parameters of a commercial anti-drone system. *Drones* **7**(1), 39 (2023)
12. Gopal, V.: Developing an effective anti-drone system for India's armed forces 16 (2020)
13. Castrillo, V.U., Manco, A., Pascarella, D., Gigante, G.: A review of counter-uas technologies for cooperative defensive teams of drones. *Drones* **6**(3), 65 (2022)
14. Wenzhun, H., Yongsheng, W., Xiangyang, Y.: Studies on novel anti-jamming technique of unmanned aerial vehicle data link. *Chin. J. Aeronaut.* **21**(2), 141–148 (2008)
15. Shi, X., Yang, C., Xie, W., Liang, C., Shi, Z., Chen, J.: Anti-drone system with multiple surveillance technologies: architecture, implementation, and challenges. *IEEE Commun. Mag.* **56**(4), 68–74 (2018)
16. Jurn, Y.N., Mahmood, S.A., Aldhaibani, J.A.: Anti-drone system based different technologies: Architecture, threats and challenges. In: 2021 11th IEEE International Conference on Control System, Computing and Engineering (ICCSCE), pp. 114–119 (2021). IEEE
17. Sazdić-Jotić, B., Pokrajac, I., Bajčetić, J., Bondžulić, B., Obradović, D.: Single and multiple drones detection and identification using RF based deep learning algorithm. *Expert Syst. Appl.* **187**, 115928 (2022)
18. Deshmukh, S., Sharma, V.: An sdr-based anti-drone system with detection, tracking, jamming, and spoofing capabilities. In: 2022 IEEE Microwaves, Antennas, and Propagation Conference (MAP-CON), pp. 388–393 (2022). IEEE
19. Advisory, F.E.: Cell jammers, gps jammers, and other jamming devices, document fcc red 1329 (2). Washington, DC, USA (2011)
20. Abunada, A.H., Osman, A.Y., Khandakar, A., Chowdhury, M.E.H., Khattab, T., Touati, F.: Design and implementation of a rf based anti-drone system. In: 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), pp. 35–42 (2020). IEEE

21. Shin, J.-M., Kim, Y.-S., Ban, T.-W., Choi, S., Kang, K.-M., Ryu, J.-Y.: Position tracking techniques using multiple receivers for anti-drone systems. *Sensors* **21**(1), 35 (2020)
22. Wang, P., Luo, J., Tang, J., Qin, Y., Cui, J., Zhang, L.: Progress and prospects of anti-drone radar detection technology. In: 2021 CIE International Conference on Radar (Radar), pp. 2331–2334 (2021). IEEE
23. Khan, M.A., Menouar, H., Eldeeb, A., Abu-Dayya, A., Salim, F.D.: On the detection of unauthorized drones-techniques and future perspectives: a review. *IEEE Sens. J.* **22**(12), 11439–11455 (2022)
24. Liu, Y., Liao, L., Wu, H., Qin, J., He, L., Yang, G., Zhang, H., Zhang, J.: Trajectory and image-based detection and identification of UAV. *Vis. Comput.* **37**, 1769–1780 (2021)
25. Zheng, Y., Chen, Z., Lv, D., Li, Z., Lan, Z., Zhao, S.: Air-to-air visual detection of micro-uavs: an experimental evaluation of deep learning. *IEEE Robot. Autom. Lett.* **6**(2), 1020–1027 (2021)
26. Zhao, S., Xie, R., Wan, J.: Design of anti-drone laser weapon systems. In: High-Power Lasers and Applications XI, vol. 11544, pp. 24–30 (2020). SPIE
27. Garcia, A.J., Lee, J.M., Kim, D.S.: Anti-drone system: a visual-based drone detection using neural networks. In: 2020 International Conference on Information and Communication Technology Convergence (ICTC), pp. 559–561 (2020). IEEE
28. Chen, Y., Li, Z., Li, L., Ma, S., Zhang, F., Fan, C.: An anti-drone device based on capture technology. *Biomim. Intell. Robot.* **2**(3), 100060 (2022)
29. Castañeda, L.B., Arunachalam, V., Dharmaraja, S.: Introduction to Probability and Stochastic Processes with Applications. John Wiley & Sons, New York (2012)
30. Imperx Inc.: Imperx Industrial Cameras: Reliability and MTBF Data. (2023). Imperx Inc. Available from manufacturer datasheet
31. JAI Ltd.: JAI Industrial CCD/CMOS Camera Specifications. (2022). JAI Ltd. Datasheet MTBF values
32. Reliability data for ground jamming and communication equipment. Technical report, Rome Laboratory, U.S. Air Force (2009)
33. Defense Technical Information Center: Ground Jammer Reliability and Field Maintenance Data. Defense Technical Information Center, Fort Belvoir (2021)
34. Premio Inc.: Industrial PC MTBF and Reliability Reports. Premio Inc., Los Angeles (2023)
35. Texas Instruments: Dependability Data for Industrial DSP Boards. Texas Instruments, Dallas (2020)
36. Advantech Co., Ltd.: MTBF and Reliability Reports for Embedded Controllers. Advantech Co., Ltd., Taipei (2021).
37. Siemens AG: Reliability and MTBF Report for Industrial Controllers. Siemens AG, Munich (2022).
38. Vicor Corporation: Reliability of Power Supplies and Converters: MTBF Analysis. Vicor Corporation, Andover (2020).
39. Delta Electronics: Reliability Data for Industrial and Military Power Units. Delta Electronics, Taipei (2021).
40. Choudhary, N., Khaitan nee Gupta, V.: High altitude aeronautical platform for voip: dependability analysis. *Wirel. Pers. Commun.* **125**(3), 2277–2303 (2022)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.