



Reliability analysis of anti-UAV systems: an analytical approach

Priyanka Kalita¹ · Raina Raj² · S. Dharmaraja³

Accepted: 9 October 2024 / Published online: 26 October 2024

© The Author(s), under exclusive licence to Operational Research Society of India 2024

Abstract

Unmanned Aerial Vehicle (UAV) is a remotely controlled or autonomously operated aircraft used for various applications such as surveillance, communication, research, etc. UAVs are nowadays being recognized as potential threats, prompting a surge in the development of anti-UAV technologies. An anti-UAV system is designed to detect, track, and neutralize unauthorized or potentially harmful UAVs. Using the fundamental aspects of the anti-UAV system, a stochastic model is constructed to investigate the reliability attributes. For the evaluation of the underlying model, continuous time Markov chain (CTMC) and semi-Markov process (SMP) are employed to capture the behaviour of the system's states. The steady-state probabilities are computed for the SMP model using the two-stage method. Whereas both the transient and steady-state probabilities are obtained for CTMC model. The numerical findings of reliability measures for both types of models are described through graphs. To verify the accuracy of the presented model, a simulation approach is employed.

Keywords Anti-UAV systems · CTMC · Reliability · Semi-Markov process · Simulation

Raina Raj and S. Dharmaraja have contributed to this work.

✉ Priyanka Kalita
priya.24723@gmail.com
Raina Raj
rainaraj.curaj@gmail.com
S. Dharmaraja
dharmar@maths.iitd.ac.in

¹ Bhattadev University, Bajali, Pathsala, Assam, India

² Bharti School of Telecommunication Technology & Management, Indian Institute of Technology Delhi, New Delhi, India

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

1 Introduction

Unmanned Aerial Vehicles (UAVs) which are nowadays commonly known as drones are becoming an integral part of our lives due to their widespread deployment in various applications [1]. With the introduction of UAVs to military, UAVs are now gaining attention as a threat of safety and security, which leverages the emergence of the anti-UAV (or counter-drone) technologies. Anti-UAV systems are designed to defend against drone accidents or terrorism and needed to be advanced to cope with future UAV flight systems. The first study on anti-UAV or anti-drone systems is recorded in [2]. They studied the survivability analysis performed for the U.S. Army's Aquila UAV program and the Joint Short Range UAV program that provide insight into anti-UAV capabilities and its requirement.

UAVs which have proven their value on the battlefield, rely heavily on GPS for navigation and flight integrity. To continue mission success for UAVs, one of the key techniques studied in [3] is GPS anti-jamming. To destroy the GPS anti-jamming, most of the anti-UAV systems adopt military-grade components to achieve the confirmatory destruction of malicious UAVs. However, several difficulties occur when locating military-grade anti-UAV systems in civilian areas. Military counter-drone measures typically use jamming systems [4] to disable the target UAV control channel. The jammer generates an extremely high amplitude of RF signal in the target frequency band to prevent communication. For military scenarios, the site is controlled by the military, and the operator pre-acquires the proper field manual for jamming conditions, hence, the side effect of jamming can be ignored or managed [5]. However, for non-military applications, RF jamming to neutralize high-speed UAVs risk the temporal paralyzing of existing wireless network systems, such as mobile access or wireless sensor networks.

Thus, most national regulations prevent non-military use of jamming systems ([6, 7]), and hence civilian anti-UAV systems need to investigate alternative approaches to stop illegal or unauthorized drones. Now a days, many countries are using anti-UAV system as their military weapon, but no work has been recorded in the literature for the reliability analysis of an anti-UAV system.

2 Relevant work

An abstract architecture of anti-UAV system is exhibited in Fig. 1. To kill a malicious UAV, an anti-UAV system should equipped with UAV detection technique and neutralization technique. In this section, UAV detection technologies, neutralization technologies and mathematical models for anti-UAV system are reviewed.

2.1 UAV-detection technologies

The UAV detection technology is based on various essential feature of UAV's to detect their presence, ascertain their location, and identify other appropriate

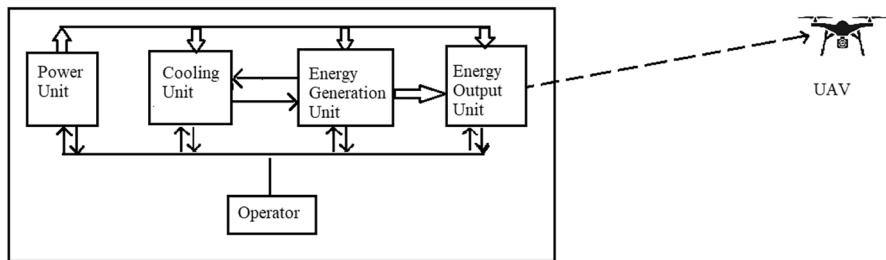


Fig. 1 Architecture of an anti-UAV system [31]

imputes. UAV's typically release distinct signals, including but not limited to radio frequency (RF) signals, Bi and multi model, acoustic waves, thermal signatures, and induce micro-Doppler signature within the surrounding environment. To detect these kind of signals or wave frequency, different detection technology is adopted namely, radar detection, RF detection, acoustic detection, and visual or image based detection.

Radar detection: Radar is a useful tool for detection and tracking of large aircraft. High frequency radar systems such as mm- wave radars support high resolution in range and enable capturing micro-Doppler signature [8]. Wang et al. [9] discussed the difficulties of existing radar system on small UAV detection, and provides an viewpoint on the development of UAV target detection. When studying the radar signatures, it is observed that there is small gap between small wing UAV's and normal UAV's. Recently, Kapoulas et al. [10] developed a new Radar technology named Radar Cross Section (RCS) simulation to detect a small UAV.

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 [11]. The passive RF detection method depends on insubstantial surveillance to identify the communications between the UAV and its remote control within the electromagnetic spectrum [12].

Acoustic detection: When the UAV threats do not appear in Radar, acoustic detection systems can be used to detect that UAV. Specialized arrays of microphones is 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 [13].

Image based detection: The UAV detection algorithms depends on hyper-spectral images which can be utilized for UAV detection. In [14], Liu et al. presented a system which is capable of detecting, and tracking a UAV using single camera automatically. The challenge in image based UAV-detection is to detect a micro object or UAV in the air. Zheng et al. [15] studied the problem of air-to-air visual detection of micro UAVs by monocular cameras. To detect and classify more accurately a micro object as a UAV, image based technique is better than the other method.

2.2 UAV neutralization technologies

UAV neutralization technology is a component of anti-UAV system which refers to operations that defeat the threatening UAVs' movements. The neutralization technique is classified as destructive and non-destructive. To kill a malicious UAV, destructive technique is mostly used which considers laser, killer UAV, and anti-aircraft weapons.

Laser: To carbonise any target in a long range a laser beam and groups of optical lenses which focus the power in one point is needed [16]. The high energy enabled laser can burn holes in the mischievous UAV and they can destroy the autonomous UAV also [17].

Killer UAV: The killer drone is meant for legal UAV which track target UAV and attempt to damage them [18]. Killer drones require quickly responsive and real-time decision making regarding incoming malicious drones, high accuracy drone flying path estimation, and outstanding physical mobility [19].

Anti-aircraft weapons: Anti-aircraft weapons are counter to aerial weapons. anti-aircraft weapons such as missiles, Guns are being increasingly used into specialist roles, such as the Dutch Goalkeeper Close-In Weapon System (CIWS) for military purpose. CIWS is meant to protect the fleet at sea from attack by ballistic missiles or aircraft [20].

2.3 Relevant literature for reliability analysis

The literature contains an extensive number of studies that develop stochastic models to analyze the reliability of various systems. In this section, we will highlight some significant contributions to reliability analysis using stochastic modeling approaches. Semi-Markov processes have been widely employed in numerous engineering applications and represent a crucial mathematical framework for evaluating system dependability, as discussed in [21]. For instance, the authors in [22] examined repairable multi-state reliability systems with components whose lifetimes and repair times are independent. In another study [23], the authors focused on a specific reliability indicator in discrete-time semi-Markov systems, known as sequential interval reliability (SIR). Building on previous work, [24] proposed an arc-based semi-Markov usage model to test systems, extending traditional Markov chain models to the more general semi-Markovian framework.

Further, the work in [25] defined a discrete-time semi-Markov model and introduced a computational procedure to solve the corresponding Markov renewal equation, which is critical for obtaining reliability measurements. The authors in [26] contributed to the field by presenting nonparametric estimators for the mean time to failure (MTTF), mean up time (MUT), and mean down time (MDT) of an arbitrary finite semi-Markov process. Notably, in the pioneering study [27], a set of integral equations was derived for this dependability measure under the assumption that the system is modeled by an irreducible finite semi-Markov process. Together, these studies demonstrate the robust application of semi-Markov processes in reliability

analysis, offering a comprehensive mathematical foundation for evaluating system performance and dependability across various settings.

2.4 Challenges for reliability analysis of anti-UAV systems

There are many challenges obtaining the reliability analysis of an anti-UAV system [28].

- Reliability assessment challenge for the efficient and robust design of the anti-UAV systems. Here, the efficient design means that the system must have very low chances of failure of components.
- Reliability of an anti-UAV system can be obtained by developing the stochastic model but the challenge is that which stochastic model is closet to real-time behaviour of the system.

In this paper, we have addressed some of the challenges to obtain the reliability of an anti-UAV system by proposing a stochastic model. To validate our analytical results, we compare the analytical results with the simulation results.

The importance of our proposed research work can be attributed to the lack of studies on the reliability of complex anti-UAV systems. In the next section, some relevant works based on different technologies and mathematical model of anti-UAV systems are reviewed.

2.5 Mathematical model of anti-UAV systems

In the previous research work, very few authors developed the mathematical model of an anti-UAV system. Among them, Garcia et al. [29] studied a simulation model for visual based anti-UAV system to detect a UAV. The network's accuracy is 93.40% and it has successfully detected the UAVs. In [15], Zheng et al. developed a simulation model to find the accuracy of visual detection anti-UAV system. Chen et al. [30] studied a dynamical modelling and simulation for a capture technology based anti-UAV system. Zhao et al. [31] presented a systematic design of anti-UAV laser system. This work has been studied and analysed from the modelling perspective in the proposed study.

For the communication LTE-A system, the authors of [32] proposed stochastic models to analyse the reliability and survivability of the system. In the literature, no work has been recorded for the reliability analysis of an anti-UAV system. This motivates us to study the reliability analysis of an anti-UAV system. The proposed work is the first one to analyse the reliability of an anti-UAV system. In this study, we propose a generic architecture for an anti-UAV system. To assess the reliability of the proposed architecture, a stochastic model has been constructed. The hierarchical model contains two levels, i.e., top level and bottom level. To compute the reliability of the proposed system, Markov and semi-Markov process are used in the top level. In the bottom level, the reliability block diagram (RBD) is proposed. In [33],

Fesenko et al. presented an RBD model to find the reliability of UAV systems. The analytical results of reliability are verified using the simulation approach.

2.6 Contribution

The significance of our research lies in filling a critical gap in the existing literature regarding the reliability of intricate anti-drone systems. By highlighting the scarcity of studies in this area, we underscore the importance of understanding the reliability of such systems, which are increasingly vital in addressing the emerging threat of unauthorized drone incursions. This motivates us to lead our investigation into the reliability analysis of an image-based anti-drone system. The proposed work represents the pioneering effort to scrutinize the reliability of such a system. Our research bridges this gap by developing a novel architectural framework tailored to image-based anti-drone systems and employing a hierarchical stochastic model combining continuous time Markov chains, SMP, and RBDs. This multi-level approach not only pioneers the reliability analysis of these specific systems but also offers a more comprehensive and robust method for evaluating their performance, validated through a rigorous comparison of analytical and simulation results.

In this work, we develop a new architectural framework for an anti-drone system based on the work [31]. To obtain the reliability of this proposed architecture, we have constructed a hierarchical stochastic model consisting of two base levels: the top level and the bottom level. In the top level, we employ CTMC and SMP and in the bottom level, RBD is employed to calculate the reliability of the proposed system. In [33], Fesenko et al., represented an RBD model employed to determine the reliability of drone systems. Further, for the validation of the proposed model, we have compared our analytical reliability results with the simulation results.

To summarize this article, the potential stochastic model is described in Sect. 3, followed by the analysis in Sect. 4. The suggested model's reliability indicators are presented in Sect. 5, while Sect. 6 provides in-depth graphical representation of reliability measures. Finally, Sect. 7 concludes with suggestions for further research.

3 Model specification

In this work, the proposed model is considered for the anti-drone system studied in [31]. The proposed model represents a hierarchical stochastic model for anti-UAV system. The model contains two levels namely top level and bottom level. The detailed description of the top level and bottom level components is given as follows:

- *Power unit:* It is used to supply the power to all the components of the anti-UAV system. In case of failure of power unit, a backup power unit starts providing service in place of the main power unit. The failure of both the power units causes the complete shutdown of the system [31].

- *Cooling unit*: The main purpose of the cooling unit is to maintain the temperature of the laser source. The generation of energy from the source creates a lots of heat. Because of this, the temperature of the laser source system increases. In case of failure of cooling unit, a backup cooling unit is kept. The failure of both the cooling units results in the complete shutdown of the system [31].
- *Energy source*: It has following sub components.
 - *Energy generation unit*: The energy generation unit supplies the energy to create energy in some form e.g., laser rays. Here, the electrical energy is changed into optical energy. It is considered as one of the crucial component of the anti-UAV system. Therefore, there is no backup for this system. The same energy generation unit is considered in Gravitas, which is a anti-drone system made by Japan in 2023. In the further analysis, the energy generation unit will be referred as laser source.
 - *Cable*: The cable connects the power supplied by source to energy output component. This cable is made of fiber and for each source, there will be one cable.
 - *Energy output unit*: This component produces the energy to destroy the target.
 - *Lens*: Lenses are used to direct the energies to a fixed spot on the target.
 - *Operator*: After fixing the spot on target, the operator component fires the energies to destroy the target.

4 Reliability analysis

There is a dependency in the top level system, hence, we have constructed a CTMC model, on the other hand, in the bottom level, there is an independence of failure in the system, hence, an RBD model is used (Fig. 2).

4.1 Semi-markov process model

The suggested model allows for the assumption that the component failure times would follow exponential distributions. However, hypo-exponential distribution is used to

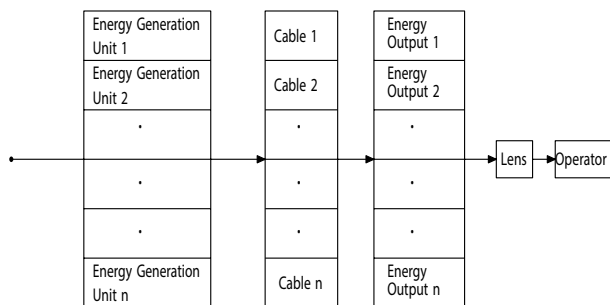


Fig. 2 RBD of bottom level

simulate the lifetime of source and laser component. Table 1 describes the distributions of sojourn times followed by each state based on the failure nature 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 mean sojourn time of some states, and Markov attributes of the time epochs, the underlying stochastic process can be appropriately modeled using SMP [34]. The state space of the proposed stochastic model is given as follows:

$$\Omega = \{U, U_P, U_C, U_{LS}, U_{P_{BP}}, U_{P_C}, U_{C_{BC}}, U_{P_{BP_C}}, U_{P_{C_{BC}}}, D\}.$$

State U shows when the completer system is in active state. State U_P shows that the power source has been failed and the backup power source has started working in this case. It also exhibits that except the power source, the other components of the system are in working state. Similarly, U_C shows that the cooling unit is in break-down state and the backup cooling unit has started working in its place, whereas other components are in working state. State $U_{P_{BP}}$ is the state when the backup power supply has also stopped working whereas the other components are functioning. State $U_{P_{BP_C}}$ exhibits that the backup power supply and the cooling unit both stopped functioning. Therefore, the system transit to state D . On the similar track, state $U_{P_{C_{BC}}}$ shows when the backup cooling unit and power supply stop working, the system will transit to state D . Whereas, if the energy generation unit stops working, the whole system will abruptly stop working even if the other components are in working state (Fig. 3).

To obtain the steady-state probabilities, 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. Here, Y_n denotes the state of the system with respect to time point t_n . 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

Table 1 Distributions of sojourn times in the proposed stochastic model

CDF	Distribution	CDF	Distribution
F_{U,U_P}	$\text{Exp}(\lambda_1)$	F_{U,U_C}	$\text{Exp}(\lambda_2)$
$F_{U,U_{LS}}$	$\text{Hypo-Exp}(\lambda_3^1, \lambda_3^2)$	$F_{U_P,U_{P_{BP}}}$	$\text{Exp}(\lambda_4)$
$F_{U_P,U_{P_C}}$	$\text{Exp}(\lambda_5)$	$F_{U_C,U_{P_C}}$	$\text{Exp}(\lambda_6)$
$F_{U_C,U_{C_{BC}}}$	$\text{Exp}(\lambda_7)$	$F_{U_{P_{BP}},D}$	$\text{Exp}(\lambda_9)$
$F_{U_{P_{BP}},U_{P_{BP_C}}}$	$\text{Exp}(\lambda_{10})$	$F_{U_{P_C},U_{P_{C_{BC}}}}$	$\text{Exp}(\lambda_{12})$
$F_{U_{C_{BC}},U_{P_{C_{BC}}}}$	$\text{Exp}(\lambda_{13})$	$F_{U_{C_{BC}},D}$	$\text{Exp}(\lambda_{14})$
$F_{U_{LS},D}$	$\text{Exp}(\lambda_8)$	$F_{U_{P_C},U_{P_{BP_C}}}$	$\text{Exp}(\lambda_{11})$

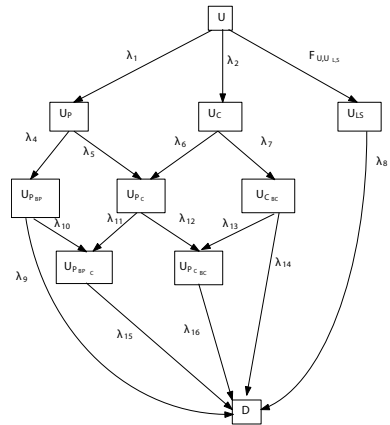
m to n of the state space. Let $\Lambda_1 = \frac{\lambda_3^1}{\lambda_3^2 - \lambda_3^1}$, $\Lambda_2 = \frac{\lambda_3^2}{\lambda_3^2 - \lambda_3^1}$, $A_1 = \lambda_1 + \lambda_2 + \lambda_3^1$, $A_2 = \lambda_1 + \lambda_2 + \lambda_3^2$. Note that, $\frac{1}{\lambda_3} = \frac{1}{\lambda_3^1} + \frac{1}{\lambda_3^2}$ is the mean of hypo-exponential distribution. The entries of matrix $K(t)$ is further computed as follows:

$$\begin{aligned}
 K_{U,U_P}(t) &= \lambda_1 \left[\frac{\Lambda_2(1 - e^{-(A_1)t})}{A_1} - \frac{\Lambda_1(1 - e^{-(A_2)t})}{A_2} \right], \\
 K_{U,U_C}(t) &= \lambda_2 \left[\frac{\Lambda_2(1 - e^{-(A_1)t})}{A_1} - \frac{\Lambda_1(1 - e^{-(A_2)t})}{A_2} \right], \\
 K_{U,U_{LS}}(t) &= \frac{\lambda_3^1 \lambda_3^2}{\lambda_3^2 - \lambda_3^1} \left[\frac{(1 - e^{-(A_1)t})}{A_1} - \frac{(1 - e^{-(A_2)t})}{A_2} \right], \\
 K_{U_P,U_{P_{BP}}}(t) &= \frac{\lambda_4}{\lambda_5 + \lambda_4} (1 - e^{-(\lambda_5 + \lambda_4)t}), \\
 K_{U_P,U_{P_C}}(t) &= \frac{\lambda_5}{\lambda_5 + \lambda_4} (1 - e^{-(\lambda_5 + \lambda_4)t}), \\
 K_{U_C,U_{P_C}}(t) &= \frac{\lambda_6}{\lambda_6 + \lambda_7} (1 - e^{-(\lambda_6 + \lambda_7)t}), \\
 K_{U_C,U_{C_{BC}}}(t) &= \frac{\lambda_7}{\lambda_6 + \lambda_7} (1 - e^{-(\lambda_6 + \lambda_7)t}), \\
 K_{U_{LS},D}(t) &= (1 - e^{-\lambda_8 t}), \\
 K_{U_{P_{BP}},D}(t) &= (1 - e^{-\lambda_{15} t}), \\
 K_{U_{P_{C_{BC}}},D}(t) &= (1 - e^{-\lambda_{16} t}), \\
 K_{U_{P_{BP}},D}(t) &= \frac{\lambda_9}{\lambda_9 + \lambda_{10}} (1 - e^{-(\lambda_9 + \lambda_{10})t}), \\
 K_{U_{P_{BP}},U_{P_{P_C}}}(t) &= \frac{\lambda_{10}}{\lambda_9 + \lambda_{10}} (1 - e^{-(\lambda_9 + \lambda_{10})t}), \\
 K_{U_{P_C},U_{P_{P_C}}}(t) &= \frac{\lambda_{11}}{\lambda_{11} + \lambda_{12}} (1 - e^{-(\lambda_{11} + \lambda_{12})t}), \\
 K_{U_{P_C},U_{P_{C_{BC}}}}(t) &= \frac{\lambda_{12}}{\lambda_{11} + \lambda_{12}} (1 - e^{-(\lambda_{11} + \lambda_{12})t}), \\
 K_{U_{C_{BC}},U_{P_{C_{BC}}}}(t) &= \frac{\lambda_{13}}{\lambda_{13} + \lambda_{14}} (1 - e^{-(\lambda_{13} + \lambda_{14})t}), \\
 K_{U_{C_{BC}},D}(t) &= \frac{\lambda_{14}}{\lambda_{13} + \lambda_{14}} (1 - e^{-(\lambda_{13} + \lambda_{14})t}).
 \end{aligned}$$

Define the matrix $K(\infty)$ which represents the transition probabilities for the underlying model and whose row sum is 1.

$$K_{m,n}(\infty) = \lim_{t \rightarrow \infty} K_{m,n}(t),$$

Fig. 3 SMP diagram of top level system



where $m, n \in \Omega$. For the embedded Markov chain (EMC) of the SMP, the steady-state probabilities for EMC (v_i) are computed as follows:

$$v = vK(\infty), \quad \sum_{i \in \Omega} v_i = 1. \quad (1)$$

Therefore, to compute the steady-state probabilities for SMP, the following formula is applied

$$\pi_i = \frac{v_i h_i}{\sum_{j \in \Omega} v_j h_j}, \quad i \in \Omega. \quad (2)$$

where v_i 's are the steady-state probabilities obtained from Equation (1) and h_i denotes the expected sojourn time, spent by the process in state i . These h_i 's are computed as follows:

$$h_U = \frac{\Lambda_2}{\lambda_1 + \lambda_2 + \lambda_3^1} + \frac{\Lambda_1}{\lambda_1 + \lambda_2 + \lambda_3^2}.$$

Since for the rest of the states, the mean sojourn time follows exponential distributions, therefore, it can be computed easily.

4.2 CTMC model

By relaxing the assumption of non-exponential distribution, the proposed model will convert to a CTMC. Let $P_i(t)$, $i \in \Omega$ be the probability that the system is in state i . $P_i(t)$ satisfies the following forward Kolmogorov equations.

$$\begin{aligned}
P'_U(t) &= -(\lambda_1 + \lambda_2 + \lambda_3)P_U(t) \\
P'_{U_P}(t) &= -(\lambda_4 + \lambda_5)P_{U_P}(t) + \lambda_1 P_U(t) \\
P'_{U_C}(t) &= -(\lambda_6 + \lambda_7)P_{U_C}(t) + \lambda_2 P_U(t) \\
P'_{U_{LS}}(t) &= -(\lambda_8)P_{U_{LS}}(t) + \lambda_3 P_U(t) \\
P'_{U_{BP}}(t) &= -(\lambda_9 + \lambda_{10})P_{U_{BP}}(t) + \lambda_1 P_U(t) \\
P'_{U_{PC}}(t) &= -(\lambda_{11} + \lambda_{12})P_{U_{PC}}(t) + \lambda_5 P_{U_P}(t) + \lambda_6 P_{U_C}(t) \\
P'_{U_{CBC}}(t) &= -(\lambda_{13} + \lambda_{14})P_{U_{CBC}}(t) + \lambda_7 P_{U_C}(t) \\
P'_{U_{PBP_C}}(t) &= -\lambda_{15}P_{U_{PBP_C}}(t) + \lambda_{10}P_{U_{BP}}(t) + \lambda_{11}P_{U_{PC}}(t) \\
P'_{U_{PCBC}}(t) &= -\lambda_{16}P_{U_{PCBC}}(t) + \lambda_{12}P_{U_{PC}}(t) + \lambda_{13}P_{U_{CBC}}(t) \\
P'_{D'}(t) &= \lambda_9 P_{U_{BP}}(t) + \lambda_{15}P_{U_{PBP_C}}(t) + \lambda_{16}P_{U_{PCBC}}(t) \\
&\quad + \lambda_{14}P_{U_{CBC}}(t) + \lambda_8 P_{U_{LS}}(t).
\end{aligned} \tag{3}$$

Let's assume that the system is in working state at the initial state, i.e., $P_U(0) = 1$. 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 bottom level will be computed and their expressions will be provided.

5.1 Reliability of bottom level for the laser source system

Reliability of bottom level is same as the reliability of the laser source system. The reliability of the laser source system with n beams, denoted by $R_{LS}(n, t)$, using RBD model is computed as follows. Reliability for a beam $R_b(t)$, is given by $R_b(t) = P(T_b > t)$, where the random variable T_b denotes the time to failure of a beam. Assume that the time T_b follows exponential distribution. After, determining the reliability of each beam, the reliability of the laser source system with n beams is given by

$$\begin{aligned}
R_{LS}(n, t) &= \left(1 - (1 - e^{-\lambda_s t})\right)^n \times \left(1 - (1 - e^{-\lambda_c t})\right)^n \\
&\quad \times \left(1 - (1 - e^{-\lambda_l t})\right)^n \times e^{-(\lambda_{le} + \lambda_{op})t},
\end{aligned} \tag{4}$$

Here, λ_s is the failure rate of source component, λ_c is the failure rate of cable, λ_l is the failure rate of laser component, λ_{le} is the failure rate of lenses, and λ_{op} is the failure rate of operator system.

5.2 Reliability of top level for the complete system

Reliability of top level is same as the reliability of the complete system. Reliability of system, denoted by $R(t)$, is given as follows

$$R(t) = 1 - P_D(t), \quad (5)$$

where $P_D(t)$ can be computed by solving the set of forward Kolmogorov equations (3).

5.3 Steady-state probabilities of the top level system using SMP and CTMC models

In Sect. 4, the steady-state probabilities of the top level system are computed using both the SMP and CTMC models.

Using SMP model, the steady-state probability of the top level being in upstate is computed from the set of Equations (2) as follows

$$P_{up} = \pi_U + \pi_{U_P} + \pi_{U_C} + \pi_{U_{P,BP}} + \pi_{U_{P,C}} + \pi_{U_{C,BC}} + \pi_{U_{P,BP,C}} + \pi_{U_{P,C,BC}} + \pi_{LS}. \quad (6)$$

Using CTMC model, the steady-state probability of the top level being in upstate is computed from the set of Equations (3) as follows

$$P_{up} = q_U + q_{U_P} + q_{U_C} + q_{U_{P,BP}} + q_{U_{P,C}} + q_{U_{C,BC}} + q_{U_{P,BP,C}} + q_{U_{P,C,BC}} + q_{LS}. \quad (7)$$

5.4 Mean time to failure

The average amount of time without a failure during use or testing is referred to as the MTTF of the system. The MTTF of the system can be provided by the following expression

$$\text{MTTF} = \int_0^{\infty} R(t)dt.$$

6 Numerical illustration

In this section, numerical investigations are carried out to examine the viability of the suggested model in order to attain steady-state probabilities and reliability measures which are presented in Sect. 5. The absence of precise model parameterization is addressed by examining the sensitivity of proposed model's characteristics to modest variations in specific parameter values considering parameter estimation is outside the purview of this paper. Table 2 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 2 are referred from the work [35]. Due to the unavailability of the existing literature, rest of the parameters have been assumed in order to carry out the analysis.

Figure 4 represents the reliability of the system with respect to time t considering different number of energy units. It can be observed that if the number of energy units are increased, the reliability of the system increases as more energy units will be available to destroy the target. Therefore, the reliability of the system increases.

Simulation approach is employed to validate the reliability aspects of the proposed model. The identical values of the parameters that are taken into account to arrive at the analytical values, as specified in Table 2, are used in a MATLAB program to this end. The simulation is run for 200 times for the identical set of parameters and 200 values of the metric are obtained. To examine the accuracy of the simulation results, the t -distribution test is used. The t -distribution is used for small sample sizes, when the population standard deviation is not known. Next, the mean and standard deviation of the 200 values are computed and confidence interval (C.I.) for 95% accuracy of the results are obtained. The C.I. for the 95% accuracy of the results can be calculated by [36]:

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

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. Since the sample size is large (≥ 30), the t -distribution will be approximated by standard normal distribution.

Comparisons are drawn between the theoretical and simulation findings for the reliability measures of the CTMC and SMP models in Figs. 5 and 6. Figure 5 exhibits the comparison of analytical and simulated results of $R(t)$ with respect to time t for CTMC model. Figure 6 demonstrates the behaviour of the probability for system being in upstate (P_{up} , refer Equation (6)) with respect to the failure rate of energy unit (λ_3) for SMP model. The graph shows the comparison of obtained analytical and simulated results. In the graphs, the findings from the analysis are depicted using solid lines, whereas the simulated outcomes are represented as dotted lines. The vertical lines shows the confidence interval. The

Table 2 Default values of parameters considered for the numerical illustration and simulation

Parameters	Values (per sec)	Parameters	Values (per sec)
λ_1	0.2	λ_2	0.15
λ_3	0.4	λ_4	0.2
λ_5	0.31	λ_6	0.42
λ_7	0.25	λ_8	0.25
λ_9	0.21	λ_{10}	0.2
λ_{11}	0.5	λ_{12}	0.5
λ_{13}	0.8	λ_{14}	0.33
λ_{15}	1.8	λ_{16}	1.2

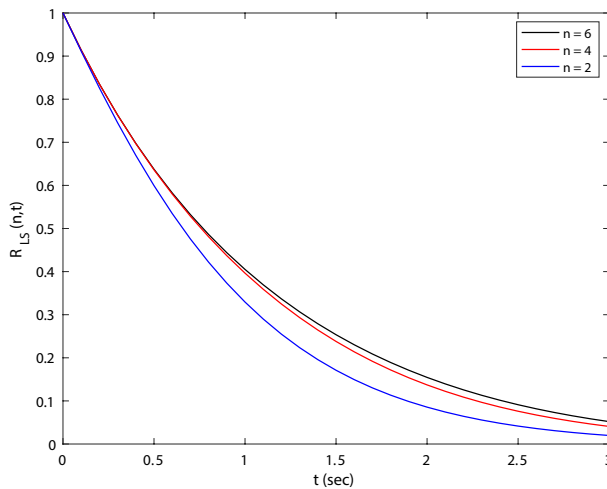


Fig. 4 Reliability of bottom level system

graphs indicate that findings of the both methods correspond quite well, verifying the hypothesised model.

Figure 7 shows the difference between the obtained reliability results (P_{up}) for CTMC and SMP models (refer, Equations (6) and (7)). Figure 8 shows the decreasing behaviour of $MTTF$ with respect to the failure rate λ_3 . The main purpose of considering the failure states in different distributions is to attempt to represent the realistic scenario through modelling. The experiment demonstrates that the choice of failure distribution has a substantial impact on the values of performance measures. The significant differences observed in the results indicate that each metric analyzed is significantly influenced by the type of failure distribution employed.

7 Conclusions and future works

The relentless pursuit of innovation in anti-UAV technologies is critical as UAVs continue to present challenges and potential risks in various sectors, urging the development of robust and efficient detection and neutralization systems. As the threat landscape evolves, the ongoing refinement and technological advancements in anti-UAV measures promise to maintain secure airspace and provide a shield against the ever-changing tactics employed by those seeking to exploit UAV capabilities for malicious purposes. Harnessing the core principles of the anti-UAV system, a sophisticated stochastic model is meticulously formulated to explore the system's reliability attributes. To evaluate the underlying model, both CTMC and SMP are effectively utilized to capture the dynamic behavior of the system's states. By calculating steady-state probabilities for the SMP, essential numerical findings are succinctly portrayed using informative graphs. In a conscientious effort to validate

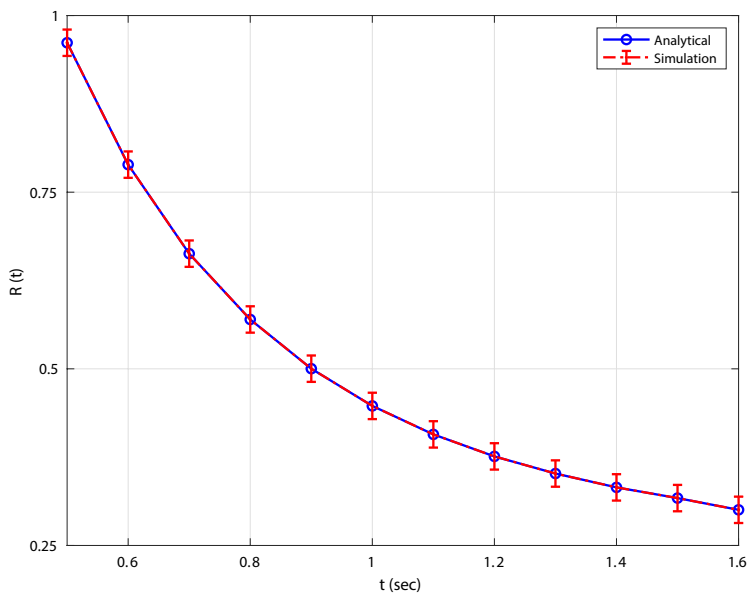


Fig. 5 Comparison of analytical and simulated results for CTMC model

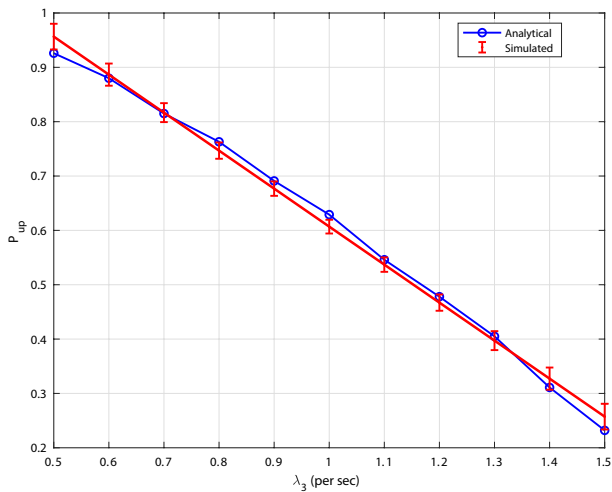


Fig. 6 Comparison of analytical and simulated results for SMP model

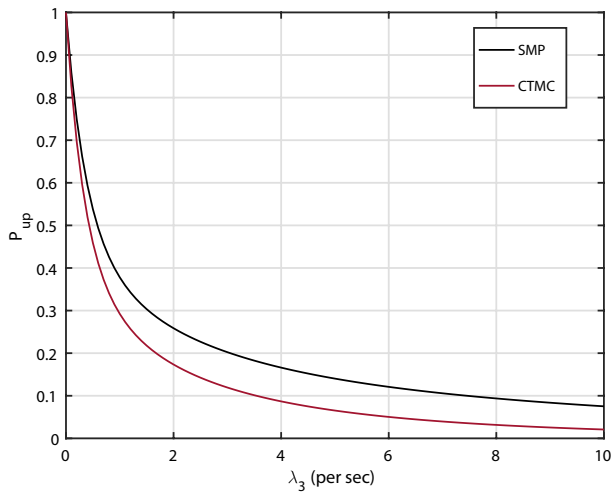


Fig. 7 Comparison of analytical results for SMP and CTMC models

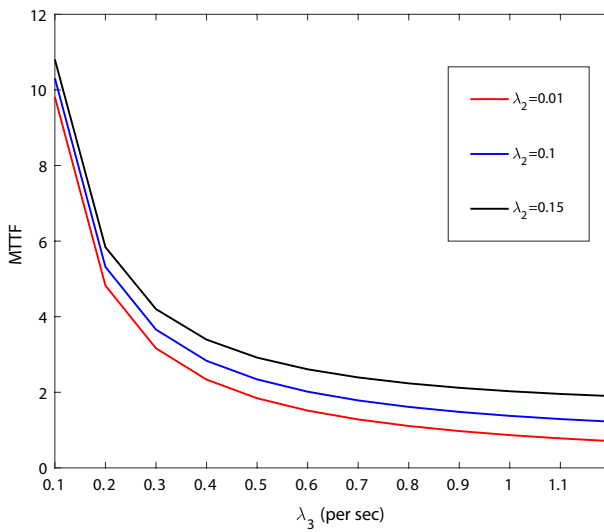


Fig. 8 Mean time to failures versus λ_3

the precision and effectiveness of the proposed model, a simulation approach is employed.

Random environment can be a challenge to obtain the reliability of an anti-UAV system. In future, this stochastic model will be analysed with random environment scenario. For the future work, a sensitivity analysis will be provided over the different parameters of the system. Also, the detailed stochastic models will be developed for the dynamic behaviour of the components of the system.

Funding There is no financial support in this research work.

Data availability NA

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. 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)
2. Beel, J.J.: Anti-uav defense requirements for ground forces and hypervelocity rocket lethality models. Technical report, Naval Postgraduate School, Monterey, CA (1992)
3. 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*, **5417**, 218–226 (2004). SPIE
4. Voorst, B.R.V.: Counter drone system. U.S. Patent 15 443 143 14 (2017).
5. 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)
6. Fcc enforcement advisory, cell jammers, gps jammers, and other jamming devices. document FCC RCD **1329** (2017)
7. Uk public general acts: wireless telegraphy act. U Legislation, London, U.K. (2006)
8. Taha, B., Shoufan, A.: Machine learning-based drone detection and classification: state-of-the-art in research. *IEEE Access* **7**, 138669–138682 (2019)
9. 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)*, 2331–2334 (2021). IEEE
10. 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)
11. Kaplan, B., Kahraman, İ., Ekti, A.R., Yarkan, S., Görçin, 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)
12. Aouladhadj, D., Kpre, E., Deniau, V., Kharchouf, A., Gransart, C., Gaquière, C.: Drone detection and tracking using rf identification signals. *Sensors* **23**(17), 7650 (2023)
13. 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)
14. 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)

15. 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)
16. Chaari, M.Z., Al-Maadeed, S.: Testing the efficiency of laser technology to destroy the rogue drones. *Secur. Def. Q.* **32**(5), 31–38 (2020)
17. Liu, L., Xu, Chengyang, Zheng, Changbin, Cai, Sheng, Wang, Chunrui, Guo, Jin: Vulnerability assessment of UAV engine to laser based on improved shotline method. *Def. Technol.* **33**, 588–600 (2024). <https://doi.org/10.1016/j.dt.2023.08.008>
18. Park, S., Kim, H.T., Lee, S., Joo, H., Kim, H.: Survey on anti-drone systems: Components, designs, and challenges. *IEEE Access* **9**, 42635–42659 (2021)
19. Akhloufi, M.A., Arola, S., Bonnet, A.: Drones chasing drones: reinforcement learning and deep search area proposal. *Drones* **3**(3), 58 (2019)
20. Meyers, J.S., Zeigler, S.M., Vick, A.J., Brackup, J.: Air base defense: rethinking army and air force roles and functions. RAND Corporation, United States (2020)
21. Petroni, F., Praticco, F., et al.: Reliability measures for indexed semi-markov chains applied to wind energy production. *Reliab. Eng. Syst. Saf.* **144**, 170–177 (2015)
22. Chrissaphinou, O., Limnios, N., Malefaki, S.: Multi-state reliability systems under discrete time semi-markovian hypothesis. *IEEE Trans. Reliab.* **60**(1), 80–87 (2011)
23. D'Amico, G., Gkelsinis, T.: On a mixed transient-asymptotic result for the sequential interval reliability for semi-markov chains. *Mathematics* **12**(12), 1842 (2024)
24. D'Amico, G.: Single-use reliability computation of a semi-markovian system. *Appl. Math.* **59**, 571–588 (2014)
25. Barbu, V., Boussemart, M., Limnios, N.: Discrete-time semi-markov model for reliability and survival analysis. *Commun. Stat-Theory Method.* **33**(11), 2833–2868 (2004)
26. Limnios, N., Ouhbi, B.: Nonparametric estimation of some important indicators in reliability for semi-markov processes. *Stat. Meth.* **3**(4), 341–350 (2006)
27. Csenki, A.: An integral equation approach to the interval reliability of systems modelled by finite semi-markov processes. *Reliab. Eng. Syst. Saf.* **47**(1), 37–45 (1995)
28. Xing, L., Johnson, B.W.: Reliability theory and practice for unmanned aerial vehicles. *IEEE Internet Things J.* **10**(4), 3548–3566 (2022)
29. A. J. Garcia, J.M.L., 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) 2, 559–561 (2020)
30. 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)
31. Zhao, S., Xie, R., Wan, J.: Design of anti-drone laser weapon systems. In: High-Power Lasers and Applications XI, **11544**, 24–30 (2020). SPIE
32. Gautam, A., Dharmaraja, S.: Reliability and survivability assessment of Ite-a architecture and networks. *Opsearch* **60**(1), 370–392 (2023)
33. Fesenko, H., Illiashenko, O., Kharchenko, V., Kliushnikov, I., Morozova, O., Sachenko, A., Skorobohatko, S.: Flying sensor and edge network-based advanced air mobility systems: reliability analysis and applications for urban monitoring. *Drones* **7**(7), 409 (2023)
34. Castañeda, L.B., Arunachalam, V., Dharmaraja, S.: Introduction to Probability and Stochastic Processes with Applications. John Wiley and Sons, New Jersey (2012)
35. Choudhary, Nikesh, Khaitan nee Gupta, Vandana: High altitude aeronautical platform for VoIP: dependability analysis. *Wirel. Pers. Commun.* **125**(3), 2277–2303 (2022). <https://doi.org/10.1007/s11277-022-09656-4>
36. Selvamuthu, D., Das, D.: Introduction to Probability, Statistical Methods. Design of experiments and statistical quality control, Springer, New York (2024)
37. Wang, C., Tian, J., Cao, J., Wang, X.: Deep learning-based uav detection in pulse-doppler radar. *IEEE Trans. Geosci. Remote Sens.* **60**, 1–12 (2021)

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.