An Intelligent Monitoring and Warning Framework in Drone Swarm Digital Twin Systems

Umit Demirbaga*†, Gagangeet Singh Aujla‡, Maninderpal Singh§, Amritpal Singh¶, Hongjian Sun¶, Joseph Camp§
*Department of Medicine, University of Cambridge, United Kingdom
†Department of Computer Engineering, Bartin University, Türkiye
‡Department of Computer Science, Durham University, United Kingdom
§Electrical and Computer Engineering Department, Southern Methodist University, Dallas, USA
¶Department of Engineering, Durham University, United Kingdom
Email: ud220@cam.ac.uk, gagangeet.s.aujla@durham.ac.uk, maninderpals@smu.edu,
{amritpal.singh,honjian.sun}@durham.ac.uk, camp@smu.edu

ICC 2024 - IEEE International Conference on Communications | 978-1-7281-9054-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICC51166.2024.10622736

***Abstract*—In drone swarms, where multiple drones collaborate closely to achieve shared objectives within constrained spatial domains, the intricacies of these interrelated actions can lead to potential issues. Despite rigorous pre-deployment planning, the inherent probability of complications persists. These complications stem from onboard computational resources, hardware failures, and network communication disruptions. While the malfunction of an individual drone may seem inconsequential, it can escalate into a substantial predicament when it disrupts the seamless coordination of the entire swarm. Therefore, the need to proactively monitor drones for predictive failure analysis and the subsequent examination of failed drones to mitigate future occurrences becomes imperative. This paper introduces a comprehensive framework for systematically collecting and processing data within drone swarms. The framework gathers critical information about onboard characteristics and communication metrics. These data points are subjected to advanced analysis using Complex Bayesian Networks to probabilistically uncover complex and hidden relationships between random features. The results demonstrate exceptional accuracy, with influences ranging from 99% to 79%, that ensures the reliability and effectiveness of the predictive capabilities in enhancing drone safety and network performance.**

***Index Terms*—Drone swarms, Digital twin systems, Metric dependencies, Bayesian networks, Performance analysis**

I. Introduction

Nowadays, deploying multiple drones in defence operations is pushing technological barriers, and they are seen as low-cost alternatives to overwhelm anti-aircraft systems. Besides military operations, drone swarms can be deployed in various non-military operations like search and rescue, humanitarian aid supply in disaster scenarios, large-scale agriculture surveying, and many more. When drone swarms are deployed in different aerial applications, one vital component is the intercommunication of the drones (D2D) and drone-to-infrastructure (D2I) communications [1], [2]. Though drones can perform fully autonomous operations using advanced technologies (like artificial intelligence and computer vision), they are less popular due to power constraints linked to the trade-off between flight time and onboard computational chores [3]. So, drones often send data to ground stations for computationally intensive tasks and return the computed results.

The swarms can be laid down differently [4], centralized, semi-autonomous distributed, and fully autonomous distributed deployments. One such scenario of the semi-autonomous distributed swarm (Hybrid swarm) is presented in Fig. 1 where drone swarms act as service relays.

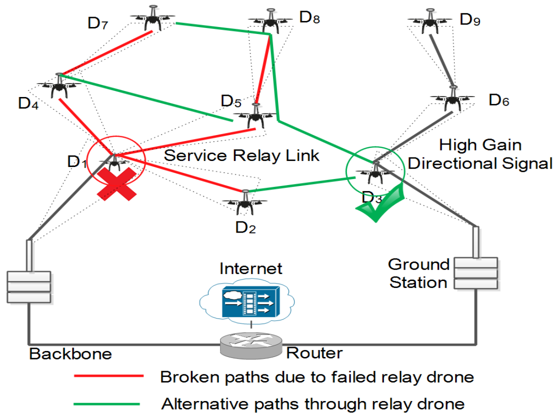


Fig. 1. Hybrid swarm with relay services using directional antennas

The depicted scenario considers when some relay nodes fail, and backup relay nodes are required to keep the system running by providing necessary network services. In swarms, the mobility of drones brings in many challenges, e.g., drones behaving unexpectedly during their flight and failing drones in the swarms [5]. There have been incidents reported where drones exhibited faulty or unexplained behavior. For example, in a drone swarm of around 500 drones, due to unexplained reasons, around 440 drones crashed into one another, and some drones even escaped the geo-fence, leading to what is known as docklands drone swarm accident[1]. Such incidents are unacceptable due to public safety concerns; hence, keeping a vigilant eye on all swarm participants becomes critical, among which the onboard characteristics of drones and network interactions are on the line of fire as failure of either can prove fatal. Some of the vital drone characteristics [6] of interest include physical parameters (battery discharge rate, remaining

[1] https://www.atsb.gov.au/media/2023/docklands-drone-swarm-accident

battery capacity), performance metrics (CPU and RAM utilization), and external factors (the effect of weather, i.e., wind on required rotary power to maneuver). Similarly, network parameters are of interest while ensuring the optimal coverage to the drones, like received signal power and supportable data rate, as these factors let the dynamic topology policies adapt for alternative ad-hoc networks for service relaying.

A. *Motivation*

Considering the above discussion, it becomes essential to understand the key reasons that can lead to potential drone failures while a drone is maneuvering. Generally, some unexpected behavior or incident is visible in the case of drone failure, but it may not be the actual cause of the drone failure or malfunction. A deeper reason may have led to this unexpected observation (i.e., failure). Consider, for example, two cases (as depicted in Figure 2), one or more drones in the drone swarm depict two different kinds of unexpected failures.

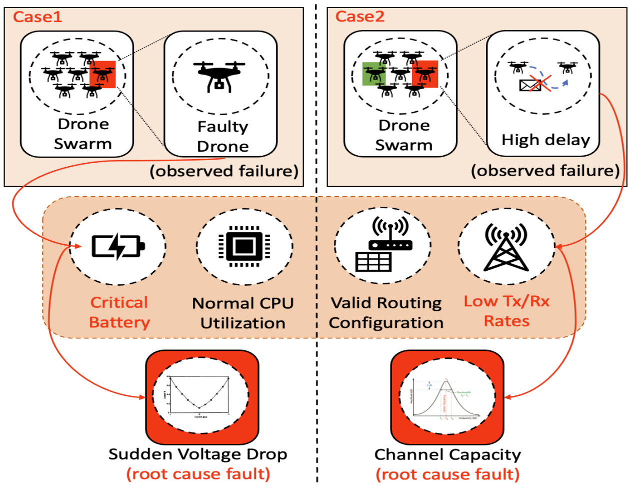


Fig. 2. Motivation cases

In this example, the localization or identification of the root cause behind the observed failures (e.g., faulty drone for case 1 and high delay for case 2) can be conducted only through a deep analysis of the vital drone parameters (e.g., battery) and network statistics (e.g., affordable transmission rates). Regarding case 1, the vital drone physical parameter, i.e., battery, is critical. It may be tough to understand the exact reason behind the critical battery status as there may be several reasons (e.g., over-discharged or over-charged). However, a deep analysis of all the vital physical parameters can help to locate the root cause behind the critical battery, and here, in this case, it is a sudden voltage drop.

In case 2, the critical parameter, i.e., transmitter-receiver rates, are low, and this may also be related to several reasons (channel capacity, bandwidth issues, supportable data rate). However, analysis showed that channel capacity was the key reason behind the sudden drop in the transmitter-receiver rates, leading to an observed high delay. From this example, analysis of all the parameters can help to localize the root cause behind the observed failures in the drone swarms. As elaborated above, the factors involving different onboard and network interaction needs to be explored to lead toward root cause analysis of drone failures. In case 2, the received signal strength indicator (RSSI) is one of the critical factors that can help to localize the root cause. The RSSI [7] is defined below.

$$\mathbb{RSSI} \rightarrow \mathbb{R}_{\mathbb{TX}} + \mathbb{TX}_{gain} - \mathbb{P}_{loss} - \mathbb{S}_{att} + \mathbb{RX}_{gain} \quad (1)$$

where, $\mathbb{R}_{\mathbb{TX}}$ signifies the radio transmit power, $\mathbb{TX}_{gain}$ and $\mathbb{RX}_{gain}$ are the transmitter and receiver antenna gains, $\mathbb{P}_{loss}$ is the path loss of signal power, $\mathbb{S}_{att}$ is the signal attenuation.

The $\mathbb{RSSI}$ signifies the actual signal strength at a given point within the given coverage area. If $\mathbb{RSSI}$ is low, it can be linked to several other parameters used within the Eq. (1). So, monitoring these parameters can help establish the correlation between the signal strength and its impact on drone failure.

Also, the channel capacity impacts the deployment of swarms significantly; during the deployment, the communication channels between the drones cannot support the required capacity, and the system will experience issues leading to failures. So, the channel capacity [8] is defined below.

$$\mathbb{C} = \mathbb{W}log_2\left(1 + \frac{\overline{\mathbb{P}}}{\mathbb{N}_0\mathbb{W}}\right) \quad (2)$$

where, $\mathbb{W}$ is the total bandwidth (in Hertz), $\mathbb{N}_0$ is the power spectral density of noise, and $\frac{\overline{\mathbb{P}}}{\mathbb{N}_0\mathbb{W}}$ is the received signal-to-noise ratio.

So, in case 2, if we experience a high delay due to low transmitter-receiver rates, after analysis, the root cause detected was concerned with the channel capacity. Thus, as per Eq. (2) there are several metrics like, $\mathbb{W}$ or $\mathbb{N}_0$ or received signal-to-noise ratio that can impact the channel capacity.

Some of the existing works [9], [10] proposed some solutions to detect drone faults. Like, in [9], the importance of time synchronization on the performance of drone swarms has been considered as key to evading failures in drone swarms. Likewise, in [10], a reliability-based drone swarm structuring approach was developed for dealing with swarm failures. Although these approaches focused on drone failures, none went beyond limited factors (like time synchronization or swarm structures). Moreover, they need to consider analyzing vital drone parameters or network statistics to understand the key reason behind the failures.

B. *Contributions*

However, analyzing the vital parameters or metrics is not straightforward. It has to deal with several challenges linked with a) vital metrics or drone data collection, b) data size, and c) appropriate analysis methods. Thus, we create a digital twin for drone swarms to collect realistic data about drone vital parameters and performance statistics subjected to complex Bayesian networks to uncover relationships between these parameters and drone failures. The following contributions have been provided in this paper.

- Proposing an innovative drone monitoring system that systematically collects and processes data related to onboard characteristics and communication metrics within a drone swarm to identify potential issues proactively.

- Presenting a robust drone warning system that utilizes Complex Bayesian Networks to address safety and network-related challenges by introducing a drone safety system that can predict drone safety warning levels and network anomalies.

II. Proposed Work

This section provides comprehensive details about the components of the proposed digital twin of the drone swarm network. A digital twin is a virtual replica of the physically configured components in the drone swarm system. The digital twin of the physical drone swarm collects real-time data with the help of a monitoring agent configured on the physical systems and performs advanced data analysis to understand the relationship between drone metrics and the observed failures to enhance the physical system's performance. The analyzed data may be used to provide intelligent decisions to pinpoint the faults or highlight the performance failures on time. The pipeline of the proposed system shown as a digital twin is depicted in Fig. 3. The proposed system contains two layers; the top layer is the physical layer comprising the drone swarm, core network, and drone base station, whereas the bottom layer contains a virtual replica of the drone swarm, monitoring component, data analysis system, and warning generation component. The data is collected from the physical layer and sent to a data analyzer, which uses a Complex Bayesian Network to understand the hidden relationships between the drone metrics and drone safety and performance. Based on the outcomes of the data analyzer, the warning generator alerts the base station, which in turn feeds back the action into the actual environment. The major components of the proposed system are elaborated in the subsequent sections.

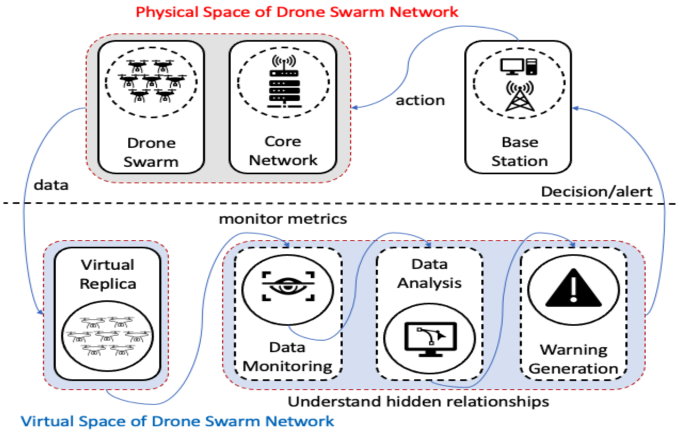


Fig. 3. Digital Twin of the Drone Swarm Network

A. Smart Monitoring System

Monitoring is critical to collecting drone vital metrics and parameters that can further point out any emergent faults or pinpoint the potential root cause faults responsible for any performance degradation in drone swarm systems. Hence, the proposed drone swarms digital twin system employs a comprehensive monitoring component for data collection. The architecture of the monitoring process is elaborated in Fig. 4. The monitoring component contains four key sub-parts: a) smart agent, b) collector, c) filter, and d) publisher. The monitoring component is activated through a smart agent deployed as a virtual API at the interface of the digital twin. They monitor the physical parameters (e.g., battery health, range of flight), computational metrics (e.g., CPU usage), and network parameters (e.g., bandwidth). The *Smart Agents* are also configured on the base station, where the collector aggregates all the statistics and metrics. The collector aggregates the different categories of the monitoring logs and forwards the collected data to the *Filter* agent. The *Filter* agent removes the non-important data logs and irrelevant data to reduce the overhead of the analyzing system. The filtered data logs are forwarded to the data analysis system by the publisher through RabbitMQ, an open-source distributed message broker.

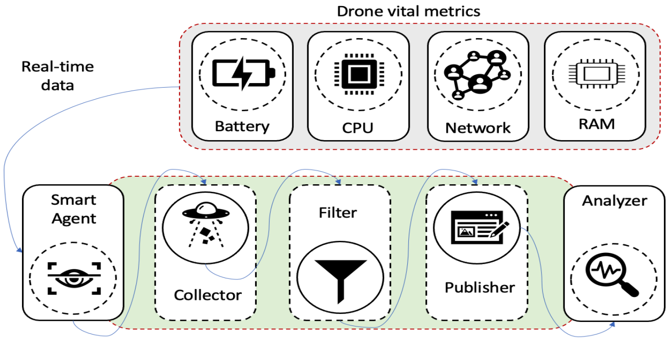


Fig. 4. Smart Monitoring System

B. Drone Warning System

The drone warning system constitutes an advanced technological solution that takes input from the real-time collection and performs the analysis. This analysis considers two cases (drone safety metrics and network statistics) discussed in the motivation section. We employ Bayesian networks (BNs) to analyze these cases due to their manifold benefits. BNs offer a unique set of advantages in data analysis and decision-making [11]. One key strength lies in their ability to adapt and learn from limited and fragmented data, making them particularly useful in scenarios with sparse datasets. Moreover, BNs exhibit remarkable versatility by accommodating a wide range of data types, including numerical, non-numerical, binary, categorical, and ordinal data, a feature that sets them apart from other modeling techniques like neural networks or decision trees. Additionally, BNs excel at integrating domain-specific or expert knowledge, a capability that surpasses traditional methods such as linear and non-linear regression. Using conditional reasoning and hidden variables, BNs can unveil intricate interdependencies that often remain concealed when employing alternative methodologies. These networks are also efficient in learning from data through structural learning algorithms, and if a BN structure is already established, they can be fine-tuned using the well-established expectation-maximization (EM) algorithm. Furthermore, BNs demonstrate their efficacy in real-time and non-real-time systems for predictive tasks and can be seamlessly extended to Dynamic Bayesian networks (DBN) to address temporal aspects. Importantly, they can be seamlessly integrated with utility theory to support decision-making under conditions of uncertainty by underscoring their broad applicability in various fields. In this work, we adopt a Complex Bayesian Network to analyze the cases considered. The detailed explanation is provided below.

In this work, we adopt a Complex Bayesian Network to predict drone health status by leveraging comprehensive datasets encompassing crucial metrics about drone health and network status. Complex Bayesian Networks enable us to delve into these diverse features' intricate and concealed relationships. By employing this approach, we aim to unravel the nuanced dependencies and interactions between the various drone performance and network metrics, ultimately providing valuable insights into predicting potential safety issues and enhancing drone operations' overall reliability and performance. Directed acyclic graphs (DAGs) are constructed using the Complex Bayesian Network and represent the probabilistic connections among these features. In the directed graphs, nodes represent different variables, and edges illustrate how they influence one another within a Complex Bayesian model.

1) Case 1-Drone Safety Warning: In the first case, the key objective is to analyze the drone's physical statistics and performance metrics to uphold safety standards during flight operations. This intricate system continuously observes and assesses vital parameters, including voltage, current, load, and RAM utilization, to evaluate the drone's operational performance. The amassed data is then subjected to comprehensive analysis to calculate the alert level, an important indicator of the drone's safety status. Should the warning level ascend to level 3, it is imperative to promptly ground the drone to avert potential mishaps or hazardous situations.

2) Case 2-Network Anomaly Detection System: In the second case, the key objective is to analyze the vital network parameters that ensure timely and reliable delivery of traffic packets generated from the drone swarm to the base station or other drones. The dataset includes 14 key features representing drone network metrics. The *label* feature gets two values where 0 represents normal while 1 represents anomalies.

3) Proposed Algorithm: To implement Complex Bayesian Networks in both scenarios, we deployed Algorithm 26. This algorithm is designed to make predictions based on drone network metrics data (N) and drone performance metrics data (A). It starts by sorting the nodes topologically in the directed acyclic graph G to create a list W (line 2). Then, each node *X_i* and *X_m* in W checks if *X_i* and *X_m* are observed in N and A, respectively. If observed, it sets their values accordingly, and if not, it uses rejection sampling to sample values from their conditional probability tables CPT (lines 8 and 14). For unobserved nodes, it estimates the CPT using Bayesian parameter estimation based on the respective data (lines 19 and 22). Finally, it calculates the predicted drone health status (P1) and predicted network anomaly (P2) based on the probability of each node given its parents and the CPT (lines 25 and 26). This method considers observed and unseen data and their relationships in the graph to forecast drone health and network status using Complex Bayesian networks.

Algorithm 1: Complex Bayesian Network

```
Input:  $N$: Drone network metrics data,
        $A$: Drone performance metrics data,
        $G$: Directed acyclic graph,
        $V$: Nodes,
        $E$: Directed edges,
        $CPT$: Conditional probability table.
Output: $P_1(HealthStatus|N, G)$: Predicted drone health status,
        $P_2(NetworkStatus|A, G)$: Predicted network anomaly.
1  // Sort the nodes in the graph topologically to obtain a list $W$
2  $W \leftarrow$ Sort $V$ in $G$
3  for each $X_i$ and $X_m$ in $W$ do
4      if ($X_i$ is observed in $N$) then
5          $X_i \leftarrow$ Set$N$ ;
6      end
7      else
8          $X_i \leftarrow RejectionSampl(P(X_i|Pa(X_i), CPT))$ ;
9      end
10     if ($X_m$ is observed in $A$) then
11         $X_m \leftarrow$ Set$A$ ;
12     end
13     else
14         $X_m \leftarrow RejectionSampl(P(X_m|Pa(X_m), CPT))$ ;
15     end
16 end
17 for each $X_i$ and $X_m$ in $W$ do
18     if ($X_i$ is not observed in $N$) then
19         $CPT \leftarrow BayesianParameEst(X_i, Pa(X_i), N)$ ;
20     end
21     if ($X_m$ is not observed in $A$) then
22         $CPT \leftarrow BayesianParameEst(X_m, Pa(X_m), A)$ ;
23     end
24 end
25 $P_1(HealthStatus|N, G) = \prod_i P(X_i|Pa(X_i), CPT)$ ;
26 $P_2(NetworkStatus|A, G) = \prod_i P(X_m|Pa(X_m), CPT)$ ;
```

III. Results

This section provides the results regarding Complex Bayesian Network implementation to probabilistically predict the drone warning level.

A. Prediction of Drone Safety Warning Level

The statistical insights derived from the drone's dataset[2], employed for model training and testing. This dataset encompasses a wide array of information, including power statistics, load characteristics, and RAM utilization. The *warning level* feature is of particular significance, which indicates the drone's operational health, ranging from 0 to 3.

TABLE I
CPT for voltage_filtered_v and drone warning level

volt_f	volt_f (< 17)	volt_f (17>= & <=18)	volt_f (> 18
warning level 0	0.010 %	11.114 %	89.600 %
warning level 1	0.010 %	5.033 %	0.079 %
warning level 2	0.010 %	1.790 %	0.079 %
warning level 3	99.967 %	82.060 %	10.239 %

Abbreviations: volt_f, voltage_filtered_v.

The CPT (Table I) illustrates the relationship between drone *warning levels* and *voltage_filtered_v* probabilistically, with each row representing a specific warning level and each column representing a range of voltage values. Notably, for *warning level 3* and *voltage_filtered_v (> 18),* the table reveals

[2] https://github.com/RuslanAgishev/drone_arm_data

a high conditional probability of 99.967% in which there is a strong association between elevated voltage levels and the drone operating in *warning level 3*. Conversely, the conditional probabilities for warning levels 1 and 2 are notably lower in this voltage range. These findings provide valuable insights into how voltage levels influence warning levels to aid in drone safety and risk assessment. The results presented in Fig. 5 reflect the accuracy of a complex Bayesian network model in predicting various performance metrics related to a drone system. Notably, the model achieved high accuracy for certain metrics, such as *scale* and *remaining*, with accuracies exceeding 99%. In contrast, metrics like *voltage_v* and *warning* exhibited lower accuracy levels, approximately 79% and 98%, respectively. These results provide valuable insights into the model's predictive performance for different drone metrics.

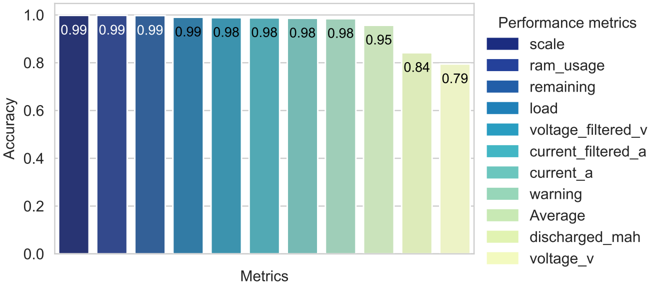
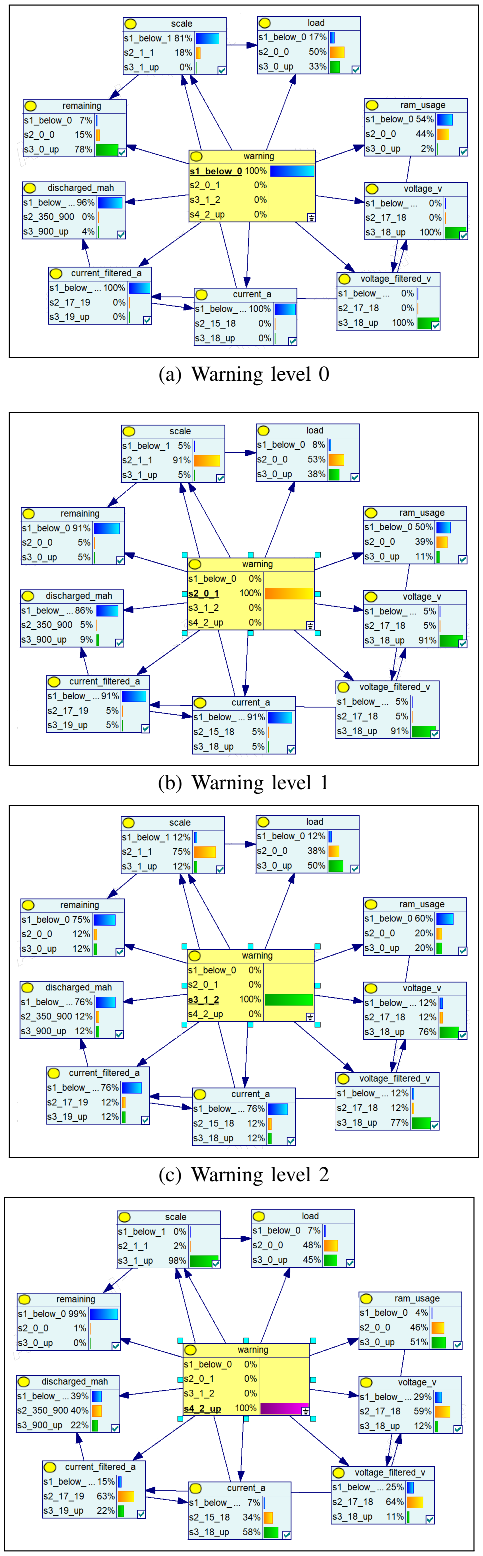


Fig. 5. Prediction accuracies for each drone performance metrics

Fig. 6 shows the dependencies and the probabilities for all drone performance metrics and four drone warning levels ranging from 0 to 3. Fig. 6(a) shows the dependencies and probabilities while the drone is safe (warning level is 0). As expected, all the *voltage* levels are quite high in this state, while *current* values are at their lowest level. When the warning level increases (see Fig. 6(b), Fig. 6(c)), the probability of the mentioned values changes in the opposite direction. For example, the likelihood of *remaining* feature reduces dramatically for the highest values. When the warning level is at the highest threshold (Fig. 6(d)), the probability of *scale* metric for the highest threshold is around 98%, while the remaining level experiences the lowest level with the maximum probability.

B. Anomaly Detection Using Complex Bayesian Network

The dataset offers statistical insights into various aspects of network behavior, with statistics calculated for each. *dur* signifies the total duration of records, *sbytes* and *dbytes* quantify the transaction bytes between source and destination, while *sttl* and *dttl* depict time-to-live values in both directions. Metrics such as *sloss* and *dloss* measure signal loss, retransmitted, or dropped packets, and *sinpkt* and *dinpkt* detail interpacket arrival times. Jitter is assessed through *sjit* and *djit*, while *tcprtt* gauges TCP connection setup times. *is_ftp_login* reveals whether an FTP session is accessed with a user and password. *ct_ftp_cmd* counts flows with FTP commands, and *label* signifies the presence of attacks (1) or normal records (0). These features collectively offer valuable information for understanding and analyzing drone network status.


scale s1_below_1 81% s2_1_1 18% s3_1_up 0%
load s1_below_0 17% s2_0_0 50% s3_0_up 33%
remaining s1_below_0 7% s2_0_0 15% s3_0_up 78%
ram_usage s1_below_0 54% s2_0_0 44% s3_0_up 2%
warning s1_below_0 100% s2_0_1 0% s3_1_2 0% s4_2_up 0%
discharged_mah s1_below_... 96% s2_350_900 0% s3_900_up 4%
voltage_v s1_below_... 0% s2_17_18 0% s3_18_up 100%
current_filtered_a s1_below_... 100% s2_17_19 0% s3_19_up 0%
current_a s1_below_... 100% s2_15_18 0% s3_18_up 0%
voltage_filtered_v s1_below_... 0% s2_17_18 0% s3_18_up 100%
scale s1_below_1 5% s2_1_1 91% s3_1_up 5%
load s1_below_0 8% s2_0_0 53% s3_0_up 38%
remaining s1_below_0 91% s2_0_0 5% s3_0_up 5%
ram_usage s1_below_0 50% s2_0_0 39% s3_0_up 11%
warning s1_below_0 0% s2_0_1 100% s3_1_2 0% s4_2_up 0%
discharged_mah s1_below_... 86% s2_350_900 5% s3_900_up 9%
voltage_v s1_below_... 5% s2_17_18 5% s3_18_up 91%
current_filtered_a s1_below_... 91% s2_17_19 5% s3_19_up 5%
current_a s1_below_... 91% s2_15_18 5% s3_18_up 5%
voltage_filtered_v s1_below_... 5% s2_17_18 5% s3_18_up 91%
scale s1_below_1 12% s2_1_1 75% s3_1_up 12%
load s1_below_0 12% s2_0_0 38% s3_0_up 50%
remaining s1_below_0 75% s2_0_0 12% s3_0_up 12%
ram_usage s1_below_0 60% s2_0_0 20% s3_0_up 20%
warning s1_below_0 0% s2_0_1 0% s3_1_2 100% s4_2_up 0%
discharged_mah s1_below_... 76% s2_350_900 12% s3_900_up 12%
voltage_v s1_below_... 12% s2_17_18 12% s3_18_up 76%
current_filtered_a s1_below_... 76% s2_17_19 12% s3_19_up 12%
current_a s1_below_... 76% s2_15_18 12% s3_18_up 12%
voltage_filtered_v s1_below_... 12% s2_17_18 12% s3_18_up 77%
scale s1_below_1 0% s2_1_1 2% s3_1_up 98%
load s1_below_0 7% s2_0_0 48% s3_0_up 45%
remaining s1_below_0 99% s2_0_0 1% s3_0_up 0%
ram_usage s1_below_0 4% s2_0_0 46% s3_0_up 51%
warning s1_below_0 0% s2_0_1 0% s3_1_2 0% s4_2_up 100%
discharged_mah s1_below_... 39% s2_350_900 40% s3_900_up 22%
voltage_v s1_below_... 29% s2_17_18 59% s3_18_up 12%
current_filtered_a s1_below_... 15% s2_17_19 63% s3_19_up 22%
current_a s1_below_... 7% s2_15_18 34% s3_18_up 58%
voltage_filtered_v s1_below_... 25% s2_17_18 64% s3_18_up 11%

(a) Warning level 0

(b) Warning level 1

(c) Warning level 2

(d) Warning level 3

Fig. 6. Dependencies and the probabilities for different drone warning levels

The CPT presented in Table II demonstrates the relationship between drone *anomaly detection* and *sloss* (signal loss) probabilistically. Notable, for the *Normal* drone state, the CPT reveals that the probability of observing a signal loss of less than 1 is 8.89%, between 1 and 5 is 21.42 %, and greater than 5 is 17.60%. Conversely, the probabilities shift significantly in the *Anamoly* situation, with a high likelihood of 78 % when the *sloss* is less than 1. This indicates a strong association between severe signal loss and detecting anomalies in the drone's operation, with a notable decrease in probability as signal loss increases.

TABLE II
CPT SLOSS AND DRONE ANOMALY DETECTION

sloss	**sloss ($<$ 1)**	**sloss (1 $\leq$ & $<=$ 5)**	**sloss ($>$ 5)**
Normal	8.96 %	21.42 %	17.60 %
Anomaly	78 %	45.12 %	13.98 %

Fig. 7 underscores the efficacy of employing a Complex Bayesian Network for network anomaly detection in drone systems. Notably, this model exhibits outstanding accuracy, with most performance metrics surpassing the 99% threshold and an impressive mean accuracy of approximately 97%. These results testify to the Complex Bayesian Network's aptitude for comprehensively capturing the dataset's intricate dependencies and probabilistic associations. The model's consistently high accuracy across various metrics underscores its trustworthiness in delivering precise assessments and predictions within a complex and interconnected network environment of drone systems.

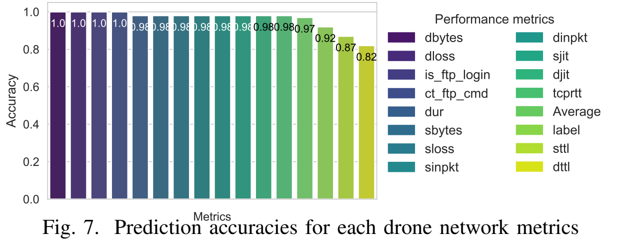


Fig. 7. Prediction accuracies for each drone network metrics

Fig. 8 demonstrates the dependencies and the probabilities for drone anomaly detection, which examines the anomaly cases. The metrics of *djit, tcprtt, is_ftp_login, ct_ftp_cmd* experience their lowest levels with the highest probabilities. Similarly, the other metrics except *sttl* have the highest probabilities at their lowest values. *sttl* shows a trend opposite to the other features, at its highest value with an 87% probability.

IV. Conclusion

This paper presents a comprehensive and innovative framework for managing and optimizing drone swarm operations to address such collaborative environments' inherent complexities and challenges. By proactively monitoring drones and applying advanced analysis through Complex Bayesian Networks, we have achieved exceptional accuracy in predictive capabilities, with results ranging from 99% to 79%. These results underscore the reliability and effectiveness of our approach in enhancing both drone safety and network performance. Our framework fosters safer and efficient applications in various domains, from surveillance and delivery services to disaster response, by reducing operational risks and disruptions. This research enhances the usefulness of drone swarm digital twin systems, which lays a basis for future advancements.

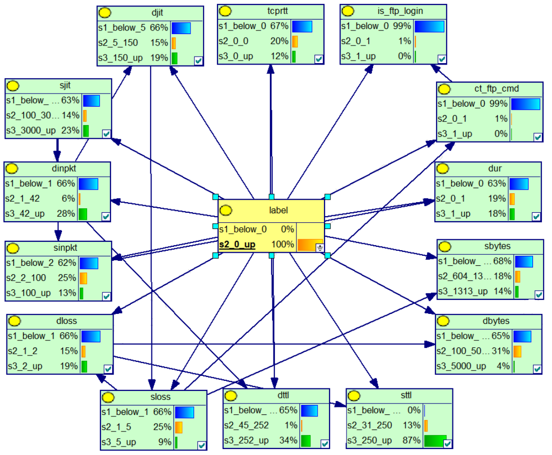


Fig. 8. Dependencies and the probabilities for drone anomaly detection

Acknowledgment

This work was supported by the Engineering and Physical Sciences Research Council (EPSRC) for project CHEDDAR: Communications Hub For Empowering Distributed ClouD Computing Applications And Research [Grant number EP/X040518/1].

References

[1] M. Singh, G. S. Aujla, and R. S. Bali, "A deep learning-based blockchain mechanism for secure internet of drones environment," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4404–4413, 2021.

[2] G. S. Aujla, S. Vashisht, S. Garg, N. Kumar, and G. Kaddoum, "Leveraging blockchain for secure drone-to-everything communications," *IEEE Communications Standards Magazine*, vol. 5, no. 4, pp. 80–87, 2021.

[3] M. P. Singh, G. S. Aujla, and R. S. Bali, "Blockchain for the internet of drones: Applications, challenges, and future directions," *IEEE Internet of Things Magazine*, vol. 4, no. 4, pp. 47–53, 2021.

[4] U. G. A. Office, "Science amp; tech spotlight: Drone swarm technologies," [Accessed on October 2023]. [Online]. Available: https://www.gao.gov/products/gao-23-106930#:~:text=of%20drone%20swarms-,Challenges,could%20put%20humans%20in%20danger.

[5] A. Tahir, J. Böling, M.-H. Haghbayan, and J. Plosila, "Development of a fault-tolerant control system for a swarm of drones," in *2020 International Symposium ELMAR*, 2020, pp. 79–82.

[6] S. H. Derrouaoui, Y. Bouzid, M. Guiatni, and I. Dib, "A comprehensive review on reconfigurable drones: Classification, characteristics, design and control technologies," *Unmanned Systems*, vol. 10, no. 01, pp. 3–29, 2022.

[7] F. Afroz, R. Subramanian, R. Heidary, K. Sandrasegaran, and S. Ahmed, "SINR, RSRP, RSSI and RSRQ measurements in long term evolution networks," *International Journal of Wireless & Mobile Networks*, vol. 7, no. 4, pp. 113–123, 2015.

[8] Z. Wei, H. Wu, Z. Feng, and S. Chang, "Capacity of UAV relaying networks," *IEEE Access*, vol. 7, pp. 27 207–27 216, 2019.

[9] F. Alsolami, F. A. Alqurashi, M. K. Hasan, R. A. Saeed, S. Abdel-Khalek, and A. Ben Ishak, "Development of self-synchronized drones' network using cluster-based swarm intelligence approach," *IEEE Access*, vol. 9, pp. 48 010–48 022, 2021.

[10] E. Zaitseva, V. Levashenko, R. Mukhamediev, N. Brinzei, A. Kovalenko, and A. Symagulov, "Review of reliability assessment methods of drone swarm (fleet) and a new importance evaluation based method of drone swarm structure analysis," *Mathematics*, vol. 11, no. 11, 2023.

[11] K. Mitra, A. Zaslavsky, and C. Åhlund, "Context-aware QoE modelling, measurement, and prediction in mobile computing systems," *IEEE Transactions on Mobile Computing*, vol. 14, no. 5, pp. 920–936, 2013.