Risk Assessment and Resilience: Bayesian Networks in Drone Cybersecurity

Anton Puliyski and Vladimir Serbezov

Technical University of Sofia, Department Aeronautics, Sofia 1000, 8 "Kl. Ohridski" Blvd

Abstract. The unmanned aircraft systems, or drones can be vulnerable to hacking, which can compromise the integrity and confidentiality of the data they collect and transmit. Hackers can also take control of the drone's navigation and other functions, which can lead to accidents or unauthorised use of the drone.

To protect against these types of attacks, it's important for drone manufacturers and operators to implement strong cybersecurity measures, such as secure communication protocols, data encryption, and regular software updates. Additionally, regulatory bodies are working on guidelines and regulations for drone operators to ensure the safety and security of these systems. In an era where drones are integral to critical operations, the application of Bayesian networks plays a pivotal role in assessing the risk of cyber threats. Bayesian networks offer a systematic approach to modelling the complex interplay of variables that contribute to the security of drone systems. By employing Bayesian networks, we can quantitatively analyze the likelihood and impact of potential cyberattacks, enabling informed decisions for enhancing drone cybersecurity measures.

This article explores the synergy between Bayesian network analysis and drone cybersecurity to ensure the resilience of these assets in the face of evolving threats. A simple Bayesian network, representing the drone cyber security measures and vulnerabilities is developed and some characteristic scenarios are simulated with it. The results show the resultant security level of the system. Conclusions about the adequacy of the model and the need for further studies and development of the used Bayesian network are made.

Keywords: drones, uav, cybersecurity, bayesian networks, risk model

1. INTRODUCTION

In recent years, drones have rapidly proliferated across industries, moving beyond military use to impact daily life in transportation, agriculture, and security. Their versatility in reaching remote areas and capturing high-quality data makes them indispensable tools. Drones' integration into smart cities is transforming urban living by enhancing efficiency, sustainability, and safety through intelligent monitoring and swift disaster responses. This synergy promises a future where technology, particularly drones, contributes significantly to a safer, more efficient, and improved quality of urban life.

These innovations can also contribute to economic growth and innovation by creating hubs for talent and entrepreneurship. Attracting talent and investment can lead to job creation and a boost to the local economy.

Despite mentioned positive aspects, the concept of smart cities also faces challenges. The increased use of interconnected digital systems can make them more vulnerable to cyberattacks, including data breaches, ransomware and breaches of critical infrastructure. Thus, while drones and smart cities provide innovative solutions to improve lives and manage cities, it is important to balance technological advancements with level of cyber resilience of the systems.

2. DRONES AND CYBERSECURITY

The unmanned aircraft systems, or drones can be vulnerable to hacking, which can compromise the integrity and confidentiality of the data they collect and transmit. Hackers can also take control of the drone's navigation and other functions, which can lead to accidents or unauthorized use of the drone.

Hacking attacks targeting drones used for urban security could have serious consequences. For example, hackers could break into the drone's video surveillance system and alter or block the live feed. This can result in security officers being unable to recognize and respond to incidents in real time, undermining the effectiveness of city security.

On the other hand a hacker attack on the drone's navigation system can cause serious problems with their control. For example, hackers could change the coordinates on which the drones are moving, which could lead to uncontrolled landings or even blocking access to important areas. This can be used to create chaos or prevent drones from completing their tasks, such as delivering medical shipments for example.

It is also possible for hackers who manage to break into the control system of drones to take control of them, stealing sensitive data or using them for malicious purposes. Unauthorized access to drones can lead to a deterioration of urban safety and violation of personal rights.

To protect against these and many more types of attacks, it's important for drone manufacturers and users to implement strong cybersecurity measures, such as secure communication protocols, data encryption, and regular software updates, etc. Additionally, regulatory bodies have to work on guidelines and regulations for drone operators to ensure the safety and securety of these systems.

Fortunately, the wireless control and navigation systems of unmanned aerial vehicles resemble the way our well-known wireless information infrastructure communicates, and in certain cases is the same. This provides an opportunity to leverage the expertise of the cyber securety domain and consider how the various related factors can be combined to establish high levels of cyber resilience. The challenge facing the integration process is related to the rapidly changing environment and the dynamics of the mentioned factors from the point of view of their prioritisation in the process of risk assessment and forming the right cyber strategy. Automating this process can contribute both at the initial stages of integration and at the stage of maintaining the system in a cyber-resistant form.

This article explores the synergy between Bayesian network analysis and drone cybersecurity to ensure the resilience of these assets in the face of evolving threats. A simple Bayesian network, representing the drone cyber security measures and vulnerabilities is developed and some characteristic scenarios are simulated with it. The results show the resultant security level of the system. A similar approach has been used in other scientific works [1-3].

3. DESCRIPTION OF DRONE CYBER SECURITY BAYSIAN (PROBABILISTIC) NETWORKS

Probabilistic networks enable quantitative risk assessment, examining the likelihood of successful cyberattacks and their impact on drone systems. This approach identifies system weaknesses, empowering operators to enhance cybersecurity measures. Factors influencing cyber resilience vary in intensity and importance based on context. Bayesian networks adapt to this contextual variation, offering a nuanced and context-aware cybersecurity assessment for drone systems.

In order to illustrate what is claimed in this article, a very simplified model can be drawn up, which includes five factors, which in different degrees of representation in different scenarios result in different values indicating the level of cyber resistance of a drone system. The five factors are as follows: connection encryption, pentesting, training, access authorization and system updates.

The encryption safeguards a drone's communication network from cyber threats, and stronger encryption enhances overall cybersecurity in the Bayesian network by structuring certainty estimates. Pentesting, a systematic process, is crucial for detecting vulnerabilities and reducing the risk of cyberattacks, enriching the Bayesian network for a realistic assessment. Staff training prevents human error and social engineering, emphasizing contextual modelling in Bayesian networks. Access authorization,

central to cybersecurity, prevents unauthorized access and system abuse, adding precision to risk assessments in the Bayesian network. System updates ensure resilience to new attacks, complementing the Bayesian network by constantly updating security estimates.

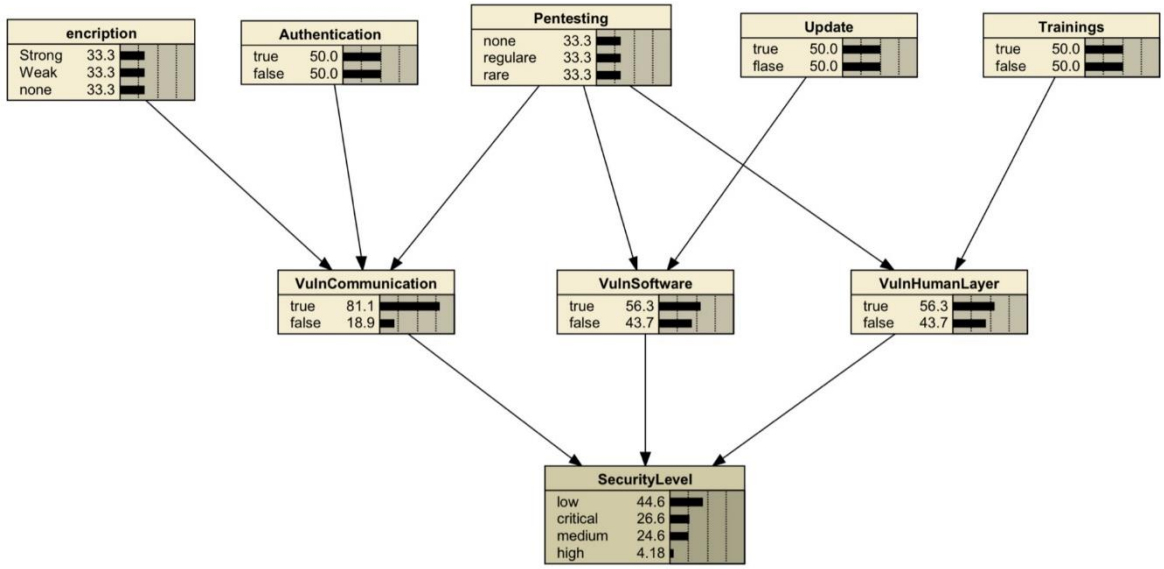


Fig. 1 Simplified Bayesian network for Drone Cyber Security Level.

Combining these factors in a Bayesian network creates a testing model that not only provides a qualitative assessment of current level cyber resilience, but also allows operators to adapt to dynamically changing conditions and innovations in cybersecurity. The integrated approach is essential in the fight against ever-evolving cyber threats, driving advances in drone cybersecurity.

Systematic analysis of the selected five cybersecurity factors in drone systems allows their categorization into three essential subgroups representing software, communication, and human-level vulnerabilities. Grouping in this way can facilitate the work of different teams and conduct an easier audit process. The design of the model allows the presence of one factor in more than one subgroup - for instance pentesting, which is applicable in all subgroups simultaneously, since its regular conduct affects each one.

The subgroup **Software Vulnerability** is related with two of chosen factors as follows:

1) **Pentesting:** Systematic and regular pentesting testing contributes to the detection and removal of software vulnerabilities, protecting the system from possible attacks and unforeseen security problems.

2) **System Updates:** Regular updates and patching the software components ensure that the system is resistant to new types of attacks and provides additional protection against potential software vulnerabilities.

The subgroup **Vulnerability of Communication** is related with three of chosen factors as follows:

1) **Pentesting:** The pentesting process applies not only to the software, but also to the communication network, providing additional guarantees for the security of the data transmitted over the drone connection.

2) **Access Authorization:** Effective management of access to communication channels prevents unauthorised connections and reduces the risk of misuse of information.

3) **Connection Encryption:** Strong encryption of communication links further strengthens protection against potential attacks, preventing unauthorised access to transmitted data.

The subgroup **Vulnerability of Human Level** is related with two of chosen factors as follows:

1) **Pentesting:** The pentesting process also plays an important role in detecting human-related vulnerabilities and provides opportunities for social engineering remediation and personnel training.

2/ **Training:** The level of staff training further defines human vulnerabilities by increasing team members' awareness and responsiveness to cybersecurity challenges.

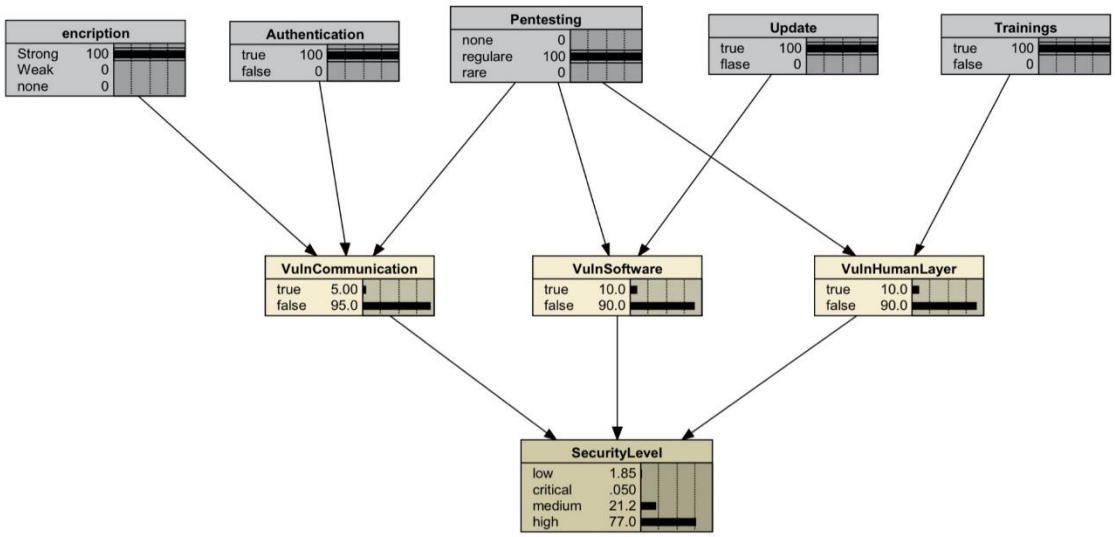


Fig. 2 Use case for High Security Level for drone system.

This categorization strategy helps in understanding and managing specific vulnerabilities in various aspects of drone systems, ensuring a more holistic defence against potential cyber threats. In addition the probabilistic model is also open to be combined with established cybersecurity industry standards and frameworks. If we want to improve the complexity of the tool in the direction of analysis, we can choose, for example, to combine it with the MITER ATT&CK Framework. It provides an extensive catalogue of tactics, techniques, and procedures that cybercriminals use in various stages of an attack. Without claiming to be exhaustive and for the purposes of this article we will give an example of how the framework can be applied to the model in several directions.

The integration of MITER ATT&CK Tactics and Techniques might be used for identifycation of possible attacks against drone systems. Probabilistic networks can analyze values of factors related to cyber security and determine the probability of a successful attack based on MITER ATT&CK Tactics and Techniques. For example, if an attacker uses social engineering, the model can estimate the probability of the tactic's success.

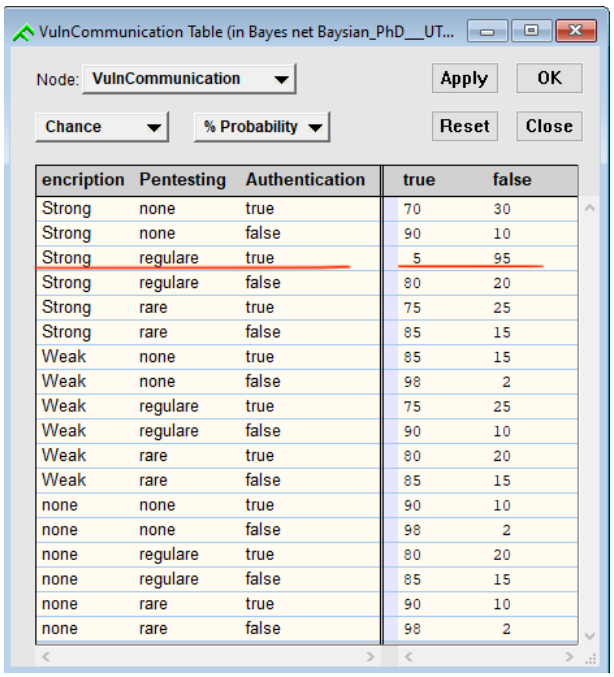
The integration could be applicable in cyber resilience assessment process with verification of defence measures. The model can analyze the effectiveness of defence measures against specific MITER ATT&CK Techniques. For example, if the system uses an embedded software detection mechanism, the probabilistic network can determine the probability of a failed deployment attempt.

When we are talking about cyber security improvement probabilistic networks can make recommendations for improving cybersecurity by assessing the likelihood of successful implementation of the recommended measures. For example, if two-factor authentication is recommended, the model can calculate how this will reduce the probability of a successful attack.

Probability networks also can be dynamically updated as new Tactics and Techniques are added to the MITER ATT&CK Framework. This dynamic approach allows the model to stay current and assess innovations in cyber-

threats. The combination of these two tools provides a comprehensive and flexible method for analyzing and improving the cyber security of drone systems, while enabling clear tracking of cyber threats and attacks in accordance with MITER ATT&CK Framework standards. In addition, we believe there is scope for further research on how AI algorithms could facilitate a more automated and time-saving assessment process and improvements leading to higher levels of cyber resilience of the systems.

4. SIMULATION RESULTS AND ANALYSIS



encription	Pentesting	Authentication	true	false
Strong	none	true	70	30
Strong	none	false	90	10
Strong	regulare	true	5	95
Strong	regulare	false	80	20
Strong	rare	true	75	25
Strong	rare	false	85	15
Weak	none	true	85	15
Weak	none	false	98	2
Weak	regulare	true	75	25
Weak	regulare	false	90	10
Weak	rare	true	80	20
Weak	rare	false	85	15
none	none	true	90	10
none	none	false	98	2
none	regulare	true	80	20
none	regulare	false	85	15
none	rare	true	90	10
none	rare	false	98	2

Fig. 3 Probalistic table for Communication vulnerability subgroup.

As can be seen from Fig. 2, despite having all the security factors in place, the fact that a drone system cannot be guaranteed to be 100 % secure highlights the complexity of cyber security and the constant evolution of cyber threats. This fact can be attributed to several key aspects.

First, cybercriminals are constantly developping new techniques and strategies. Second, the human factor plays an essential role. Third, the dynamic nature of cyber threats and technological challenges requires systems to be constantly updated and improved.

Overall, even with integrated security measures, factors such as innovations in cybercrime, human error, and the dynamic cyber environment necessitate constant efforts to improve and optimize the cybersecurity of drone systems.

In Fig. 3, on the fourth row can be seen the logic behind the probabilistic assumptions for the communication vulnerability subgroup when combining three factors - pentesting, access authorization and encryption - highlight the complex and interactive nature of cyber security. Despite regular pentests, strict access authorization and the use of strong encryption, absolute security is not guaranteed. Pentesting identifies existing vulnerabilities, but cannot predict all attacks. Even with access authorization and strong encryption, social engineering or misuse of credentials remain potential risks. Despite encryption, man-in-the-middle attacks can still take place. Therefore, 100 % security requires a holistic approach, including technical and educational measures, analysis of new threats and continuous improvement of the system. This balance between factors and strategies is key to a high level of cyber security.

In conclusion, it is clear that the security of drone systems requires a complex and comprehensive approach. Despite integrated security measures, factors such as cyber threats, human error and a dynamic cyber environment underscore the need for ongoing simulations. Examining individual factors and their combination in different contexts is a key element in improving cyber security. Also simulations provide an opportunity to test systems in a controlled environment, exposing them to various cyber scenarios. This process not only helps in identifying vulnerabilities, but also in understanding how various factors interact and affect overall cybersecurity.

5. CONCLUSION

The use of probabilistic networks might provide significant benefits in establishing the cyber resilience of drone systems. This analytical tool provides a systematic and comprehendsive model that not only identifies potential vul-

nerabilities but also predicts the consequences of various cyberattacks. This predictive analytics is essential to effectively improve the security of drone systems, providing operators with the means to overcome emerging cyber threats.

The probabilistic network-based model offers a structured approach for creating a system security architecture and operates bidirectionally. It serves not only in establishing cyber resilience but also as a dynamic system auditing tool, enhancing security and responsiveness to evolving threats. Future research can explore applicable frameworks and standards in the cybersecurity domain. Analyzing factors influencing security is vital, and probabilistic networks facilitate this by incorporating various scenarios, offering context, and weighting their role in the system. The system's openness to change and dynamic adjustments to factors ensure adaptive cybersecurity, allowing regular updates and structural modifications based on the evolving cyber landscape, safeguarding drone systems against emerging risks and trends.

REFERENCES

1. Y. Kim, I. Lee, H. Kwon, K. Lee and J. Yoon, "BAN: Predicting APT Attack Based on Bayesian Network with MITRE ATT&CK Framework," in *IEEE Access*, vol. 11, pp. 91949-91968, 2023.
2. T. He and Z. Li, "A Model and Method of Information System Security Risk Assessment based on MITRE ATT&CK," *2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT)*, Sanya, China, 2021, pp. 81-86.
3. Sun, J., Wang, W., Da, Q., Kou, L., Zhao, G., Zhang, L., & Han, Q. (2018). An Intrusion Detection Based on Bayesian Game Theory for UAV Network. In *Proceedings of MOBIMEDIA, EAI*.