Canadian Science Publishing

MINI REVIEW

Potential cyber threats, vulnerabilities, and protections of unmanned vehicles

Aybars Oruc

Abstract: This study seeks to contribute to the literature by presenting a discussion of potential cyber risks and precautionary measures concerning unmanned vehicles as a whole. In this study, Global Navigation Satellite System (GNSS) spoofing, jamming, password cracking, denial-of-service (DoS), injecting malware, and modification of firmware are identified as potential cyberattack methods against unmanned vehicles. Potential deterrents against the aforementioned cyberattack methods are suggested as well. Illustrations of such safeguards include creating an architecture of the multi-agent system, using solid-state storage components, applying distributed programming tools and techniques, implementing sophisticated encryption techniques for data storage and transmission, deploying additional sensors and systems, and comparing the data received from different sensors.

Key words: unmanned vehicles, cyber threats, vulnerabilities, protection measures.

Résumé : Cette étude vise à contribuer à la documentation en présentant une discussion sur les cyberrisques potentiels et les mesures de précaution concernant les véhicules sans pilote dans leur ensemble. Dans la présente étude, l'arnaque, le brouillage, le craquage des mots de passe, le déni de service, l'injection de logiciels malveillants et la modification de microprogrammes du système mondial de navigation par satellite (« GNSS ») sont identifiés comme méthodes de cyberattaque potentielles contre les véhicules sans pilote. Des moyens de dissuasion potentiels contre les méthodes de cyberattaque susmentionnées sont également suggérés. Des exemples de ces mesures de protection comprennent la création d'une architecture du système multi-agents, l'utilisation de composants de stockage à semi-conducteurs, l'application d'outils et de techniques de programmation distribués, la mise en œuvre de techniques de chiffrement sophistiquées pour le stockage et la transmission de données, le déploiement de capteurs et de systèmes supplémentaires et la comparaison des données reçues de différents capteurs. [Traduit par la Rédaction]

Mots-clés : véhicules sans pilote, cybermenaces, vulnérabilités, mesures de protection.

1. Introduction

Technology is developing rapidly, and many different technologies have been combined to make unmanned vehicles a reality. Technological categories include sensors, communication, information, networking, and automation. Automation combines control systems and sensors to accomplish a task requiring many systems.

Received 13 August 2021. Accepted 10 November 2021.

A. Oruc. Norwegian University of Science and Technology, 2815, Gjøvik, Norway.
E-mail for correspondence: aybars.oruc@ntnu.no.

Unmanned vehicles are totally dependent on data for reliable operation (Madan et al. 2019). The cyber systems in autonomous vehicles collect data as well as store, process, and compose new data to perform assigned tasks. Unintentional vulnerabilities in the vehicles' software and cyberattacks attempted by malicious actors arouse numerous suspicions regarding unmanned vehicles' safety, security, and reliability issues.

This study is important to understand the cyber risks of unmanned vehicles including integrity, availability, and confidentiality threats. Moreover, potential attack methods against unmanned vehicles are given and possible precaution measures are suggested. A literature review was performed in well-known scientific digital libraries in order to reply to the research questions of the study. The study is useful for researchers working on cyber security or unmanned vehicles.

2. Related work

Parkinson et al. (2017) investigates the cyber threats of autonomous and connected vehicles, with a special focus on the cyber risks of intelligent automobiles. The authors note a lack of research in the literature about the cyber vulnerabilities of gyroscopes and inclination sensors in unmanned vehicles. Meanwhile, Madan et al. (2019) focuses on the cyber vulnerabilities of unmanned aerial vehicles (UAVs), discussing STRIDE threat modeling and risk assessment method of Common Vulnerability Scoring System belonging to UAVs. Another study (Yağdereli et al. 2015) propose several risk mitigation measures against cyber threats and vulnerabilities belonging to unmanned vehicles. In contrast to other papers, the paper emphasizes the vulnerabilities of the controller area network bus. Hartmann and Steup (2013) state the vulnerabilities of UAVs to cyberattacks. The components of the vehicle and ground control station are identified with the data flow. Moreover, a cyber risk assessment method specifically for UAVs is proposed for further study.

As per fiscal year 2020 (Klein 2019), the U.S. Department of Defense (DoD) has budgeted around $1 billion more for unmanned vehicles to be used by the U.S. Navy than the combined budgets for unmanned vehicles of the U.S. Army and U.S. Air Force. Although many have focused on the cyber risks of unmanned ground vehicles (UGVs), unmanned surface vehicles, and UAVs, the literature lacks any mention of cybersecurity risks of unmanned underwater vehicles (UUVs), unmanned spacecraft, and unmanned trains.

3. Materials and methods

This study focuses on the potential threats, vulnerabilities, safeguards of unmanned vehicles, and technical mitigation measures. This study included a review of the scientific digital libraries of ACM, IEEE Xplore, Springer, and ScienceDirect. Furthermore, Google Scholar, ProQuest, and Semantic Scholar were consulted to identify relevant academic articles. Moreover, alternative resources were used as a complementary element as well as a contribution to the literature. The sources of this article involved only English-language content.

4. Threats, vulnerabilities, and protections

4.1. Cyber incidents involving unmanned vehicles

Past cyber incidents highlight the importance of cybersecurity for unmanned vehicles. A variety of cyber incidents have been reported as summarized in Table 1.

Another attack was conducted in 2009 when insurgents in Iraq captured live video feeds from U.S. UAVs. The video records were found on the laptop of an Iraqi insurgent, and an incident investigation revealed that "SkyGrabber" software (costing only $26) had been used to capture the video records. Using only this software and some basic equipment like a satellite dish, any individual could capture satellite-based signals. At the time, U.S. UAVs

Table 1. A variety of cyber attacks against unmanned vehicles.

Year	Vehicle	Targeted state	Accused actor	Attack method	Impact
2009	UAV	U.S.	Iraqi insurgents	Exploit communication weakness	Capturing live video feeds
2011	UAV (RQ-170 Sentinel)	U.S.	Iran	GPS spoofing	Total loss
2011	UAV (Predator, Reaper)	U.S.	Unknown	Malware (keylogger)	Logging and transmitting drone pilots's keystrokes

did not use encryption, as it would cause a slowdown of real-time data transmittal; however, removing the encryption caused unauthorized access (Mount and Quijano 2009; Hartmann and Steup 2013).

"RQ-170 Sentinel," a UAV developed by the U.S.-based company Lockheed Martin, was captured by Iranian military forces on 4 December 2011, after landing in Iranian territory. U.S. authorities officially confirmed the loss of the UAV. Two theories have been proposed to explain this loss: a Global Positioning System (GPS) spoofing attack or a technical malfunction. Both possibilities reveal UAV vulnerabilities (Hartmann and Steup 2013).

A U.S. UAV fleet was infected with a type of malware that affected the cockpits of U.S. "Predator" and "Reaper" drones at Creech Air Force Base in Nevada in September 2011. The malware was detected by the U.S. military's Host-Based Security System. The malware, called "keylogger", had the aim of logging the drone pilots' keystrokes and then transmitting them over the public Internet to malicious actors (Shachtman 2011; Hartmann and Steup 2013).

It seems in the literature, cyber attacks were conducted against UAVs for military purposes. A potential cyberattack against unmanned vehicles equipped with weapons may lead to catastrophic accidents and political tension. Moreover, unmanned vehicles developed for military purposes may have more sensitive data than civilian-purpose unmanned vehicles. A probable cyberattack could reveal security-related and political concerns.

4.2. Cyber threats to unmanned vehicles

Functionality and connectivity enhance the risk of cyber threats and vulnerabilities (Parkinson et al. 2017). Cyber threats currently affect unmanned vehicles in three essential categories: "confidentiality threats," "integrity threats," and "availability threats."

4.2.1. Confidentiality threats

A malicious actor may endanger the confidentiality of an unmanned vehicle by capturing and disclosing sensitive data. This type of threat has more importance for military-purpose vehicles, in particular, because of having potentially sensitive information, such as operation plans, probable targets, and surveillance records (Madan et al. 2019).

4.2.2. Integrity threats

Two essential impacts on integrity are involved in this category. First, the data can be changed or corrupted by a malicious actor before the recipient receives them. Second, the attacker assumes the identity of the sender and sends fake data. The recipient supposes the data were sent by the real sender. Corrupted data can have serious implications, affecting the decision-making process (Madan et al. 2019).

4.2.3. Availability threats

Unmanned vehicles use different types of data received from sensors for motion control, which are processed by various software. These data are transmitted between the vehicle and the control center. In this case, the attacker aims to damage software in the unmanned vehicles and block data transmission, employing any of three essential methods, which include jamming, denial-of-service (DoS), and injecting malware (Madan et al. 2019).

4.3. Probable attack methods against unmanned vehicles

Potentially, six types of cyberattack methods may be implemented against unmanned vehicles: Global Navigation Satellite System (GNSS) spoofing, DoS, jamming, password-cracking attacks, injecting malware, and modifying firmware.

4.3.1. GNSS spoofing

In a GNSS spoofing attack, actual GNSS signals are simulated, and fake signals are transmitted to create false location knowledge. Manufacturers program GNSS receivers to use the strongest signal to enable the receiver to acquire a more accurate position. Consequently, spoofing signals must be stronger than real signals in a successful attack, prompting the GNSS receiver to accept spoofed GNSS signals instead of real GNSS signals. As a result, the receiver is unable to detect its current (and accurate) position (Humphreys et al. 2008; Parkinson et al. 2017).

4.3.2. Jamming

Jamming is one of the most crucial problems of wireless communication protocols. This type of attack causes a disruption of services by blocking radio frequencies. Various devices and services may be affected negatively by jamming, including Bluetooth-enabled devices, wireless networks, GNSS services, and mobile phones. Jamming can be conducted legally or illegally. The jamming device, called a jammer, transmits the signal at the same frequency as the target system or device. Adequate power allows the jamming signal to override the genuine signal. As a result of this attack, the receiver is unable to receive data from the real transmitter (Kesavulu et al. 2013).

Conducting a GNSS jamming attack on an unmanned vehicle is simpler than GNSS spoofing (Parkinson et al. 2017). Moreover, GNSS jamming is less dangerous than GNSS spoofing because the target receiver may detect the abnormal situation and warn an unmanned vehicle's operator (Humphreys et al. 2008). Nevertheless, the vehicle or the operator will be unable to determine the current location using the GNSS, thereby losing its navigation capability.

4.3.3. Password-cracking attacks

A password is required to access maintenance interfaces of the system, in general. The correct password may be uncovered by the use of several password-cracking methods, such as a dictionary attack, rainbow table attack, and brute force attack (Parkinson et al. 2017). Once they have cracked the password, the attackers can modify the operational parameters, negatively impacting the efficiency and reliability of the affected system.

A dictionary attack employs a list of words used individually or in combination to crack the victim's password. In comparison, a brute force attack is similar to a dictionary attack, except it may employ non-dictionary words with alphanumeric combinations. Although using this method to crack a password may take be a time-consuming process, the password can be identified eventually if the victim has not taken the requisite precautions. The rainbow table attack is also similar to a dictionary-based attack. This attack method

features a list of pre-computed hashes created from potential passwords, including a given algorithm (Parkinson et al. 2017).

4.3.4. DoS

The DoS is an effective cyberattack method against networks. In this case, the malicious actor transmits a high volume of null data packages to the network. The useless data packages consume network resources. The victim's network is unable to reply to the excessive requests received and eventually breaks down (David and Thomas 2019).

Distributed denial-of-service (DDoS), a variation of DoS, is harder to detect in terms of malicious traffic than a DoS attack because the attacker uses "zombie computers" during such an attack. The term "zombie computer" refers to a computer that has been infected with malware before the attack. The attacker triggers the unaware users' zombie computers to send malicious data packages to the victim's network (Gasti et al. 2013).

As a consequence of a possible DoS or DDoS attack to primitive sensors, in particular, an unmanned vehicle may be theoretically forced to travel at too low a speed (Parkinson et al. 2017).

4.3.5. Injecting malware

Malware is harmful software designed to run on a specific operating system, such as Mac OS, Windows, or UNIX. Different types of malware employed for different purposes are available under various names, including virus, worm, spyware, adware, trojan, bot, rootkit, keylogger, and ransomware. A malware program may damage the files in a computer, monitor the victim's activities, or constitute a backdoor for further attacks. Moreover, malware may be used for cyber warfare. For instance, "Stuxnet" malware was allegedly specifically coded against an Iranian nuclear facility by U.S. and Israeli intelligence services (Bettany and Halsey 2017).

Malware can infect control systems, especially unmanned automobiles having passengers, which may be infected through the onboard diagnostic port, embedded web browsers, media players, and removable ports (Parkinson et al. 2017).

4.3.6. Modification of firmware

Manufacturers often release new versions of the firmware used for systems in unmanned vehicles to fix various problems or increase performance. Such new firmware may completely change the behavior of an unmanned vehicle. If a malicious actor is able to make any modifications to the firmware or install modified firmware belonging to any systems in the unmanned vehicle, accidents may result (Parkinson et al. 2017).

4.4. Potential precautions against cyber threats

Encryption techniques offer effective methods to prevent confidentiality threats; however, experts must employ a strong method to prevent an attacker from easily decoding encrypted data. Policy-based and cryptography-based techniques are effective mitigation methods against integrity threats. Moreover, the data must be stored in encrypted form. Furthermore, if required, the data must be transmitted to the command center through an encrypted communication protocol (Madan et al. 2019).

Redundancy refers to the duplication of components or functions in a system (Lezoche and Panetto 2020). This notion should be considered at the early design stage of an unmanned vehicle, as losing a single component due to a possible cyberattack may result in the loss of the unmanned vehicle.

GNSS is a useful example that reveals the importance of redundancy. As mentioned, one theory to explain losing RQ-170 Sentinel in 2011 was a GNSS spoofing attack. GNSS vulnerabilities (GNSS spoofing and jamming attacks) can lead to the loss of an unmanned vehicle.

GNSS technologies have different variations, such as the U.S. based-GPS, Russia based-Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS), China's Běidǒu Wèixīng Dǎoháng Xìtǒng (BeiDou), and the European Union's Galileo (Jan and Tao 2016). The combination of different GNSS variations can be an effective mitigation measure against cyber threats (Moaiied and Mosavi 2016).

Enhanced LORAN (eLORAN), a high-power terrestrial radio navigation system, can be used as an alternative positioning solution (Seo and Kim 2013). As one example of practical application, South Korea plans to widely use eLORAN technology to provide safe navigation capability to vehicles in its vicinity (Seo and Kim 2013). It may also be possible to use eLORAN technology to enhance the safe navigation capability of unmanned vehicles.

Alternative navigation systems may also be implemented for unmanned vehicles. One potential solution is an Inertial Navigation System (INS), which was developed for positioning without any external signal. Today, this technology is used in aircraft, submarines, and guided missiles as well as unmanned vehicles, such as unmanned spacecraft (Gaylor and Lightsey 2003), UUVs (Ishibashi et al. 2007), UGVs (Meiling et al. 2017), and UAVs (Zhang and Hsu 2018). INS can be combined with GNSS to cross-check the current position of an unmanned vehicle. Moreover, it is useful for the environments where a vehicle would be out of range of GNSS, such as underwater or in space.

Modern GNSS units can also calculate the speed of a UGV even if GNSS cannot provide as sensitive speed data as a wheel sensor. In this case, the measured speed value on a wheel speed sensor may be confirmed by comparing the speed value on GNSS (Parkinson et al. 2017).

The environment of unmanned vehicles must be observed constantly by reliable sensors. Correct data about the range and speed of objects in the vicinity of the unmanned vehicle must be obtained. RAdio Detection And Ranging (RADAR), Sound Navigation And Ranging (SONAR), and LIght Detection And Ranging (LIDAR) provide quantified data of the objects in the environment accurately under normal circumstances (Onori et al. 2015). Such sensors are useful in deploying an unmanned vehicle, providing the ability to detect and understand the motion of obstacles in the environment and avoid possible accidents. Thus, individual and isolated sensor systems can help identify potential threats. Comparison of the received data from different sensors is an effective precaution; sensors affected by a potential cyberattack may go on to transmit inaccurate data to components (Hartmann and Steup 2013). This faulty data may affect unmanned vehicles' decision-making process.

Unmanned vehicles comprise multiple subsystems—in other words, systems of systems. GNSS, communication equipment, and video cameras are some examples of subsystems on unmanned vehicles. Creating a "multi-agent system" architecture is possible on many unmanned vehicles. In particular, software agents can be effective in detecting potential cyberattacks (Yağdereli et al. 2015).

Both self-control systems and remote control systems are dependent on situational awareness. Although cameras may be used to increase a system's situation awareness, it is theoretically possible to jam the cameras. For example, the MQ9-Reaper UAV is equipped with three cameras (infrared, daylight, and light enhancing). These independent cameras provide optimal imagery and have the added benefit of decreasing the jamming risk (Hartmann and Steup 2013).

For data storage in unmanned vehicles, solid-state storage solutions are preferable to hard drive-based storage (Hartmann and Steup 2013). Unmanned vehicles may work in challenging environments. Vibration, forces from different directions, or magnetic fields can affect hard-drive-based storage negatively, potentially resulting in data loss.

Mitigation measures for reliable operation must be developed against potential cyberattacks and failure of hardware or software components. Accordingly, distributed

programming tools and techniques should be used in unmanned vehicles (Yağdereli et al. 2015).

5. Conclusion

Cyber risks must be assessed during the design and development process of unmanned vehicles. This study was conducted to present potential cyber risks and mitigation measures of unmanned vehicles. In this study, unmanned vehicles were divided into six categories. Threats were listed in three groups as confidentiality threats, availability threats, and integrity threats. Six cyberattack methods against unmanned vehicles were identified, and probable protection measures were suggested. The literature review also identified a research gap concerning UUVs, which are widely used in the industry, military, and academia but feature limited scientific research on cyber threats. Moreover, a comprehensive study could be highly beneficial, revealing cyber incidents involving unmanned vehicles, as the literature is lacking in this respect.

References

Bettany, A., and Halsey, M. 2017. What is malware? *In* Windows virus and malware troubleshooting. *Edited by* A. Bettany and M. Halsey. Apress. pp. 1–8. doi: 10.1007/978-1-4842-2607-0_1.

David, J., and Thomas, C. 2019. Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic. Comput. Secur. **82**: 284–295. doi: 10.1016/j.cose.2019.01.002.

Gasti, P., Tsudik, G., Uzun, E., and Zhang, L. 2013. DoS and DDoS in named data networking. *In* 2013 22nd International Conference on Computer Communication and Networks (ICCCN), Nassau, Bahamas, IEEE, 30 July–2 August 2013. pp. 1–7. doi: 10.1109/ICCCN.2013.6614127.

Gaylor, D., and Lightsey, E.G. 2003. GPS/INS kalman filter design for spacecraft operating in the proximity of International Space Station. *In* AIAA Guidance, Navigation, and Control Conference and Exhibit, Austin, Texas, AIAA, 11–14 August 2003. doi: 10.2514/6.2003-5445.

Hartmann, K., and Steup, C. 2013. The vulnerability of UAVs to cyber attacks – An approach to the risk assessment. *In* 5th International Conference on Cyber Conflict (CYCON 2013), Tallinn, Estonia, IEEE, 4–7 June 2013. pp. 1–23.

Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W., and Kintner, P.M. 2008. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *In* Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA, 16–19 September 2008. pp. 2314–2325.

Ishibashi, S., Tsukioka, S., Yoshida, H., Hyakudome, T., Sawa, T., Tahara, J., et al. 2007. Accuracy improvement of an Inertial Navigation System brought about by the rotational motion. *In* OCEANS 2007 – Europe, Aberdeen, UK, IEEE, 18–21 June 2007. pp. 1–5. doi: 10.1109/OCEANSE.2007.4302282.

Jan, S.-S., and Tao, A.-L. 2016. Comprehensive comparisons of satellite data, signals, and measurements between the BeiDou Navigation Satellite System and the Global Positioning System. Sensors, **16**(5): 689. doi: 10.3390/s16050689.

Kesavulu, O.S.C, and Harini, P. 2013. Enhanced packet delivery techniques using crypto-logic riddle on jamming attacks for wireless communication medium. Int. J. Latest Trends Eng. Technol. **2**(4): 469–478.

Klein, D. 2019. From Unmanned Systems magazine: Fiscal 2020 defense budget request includes billions for unmanned systems. Available from auvsi.org/unmanned-systems-magazine-fiscal-2020-defense-budget-request-includes-billions-unmanned-systems [accessed 14 November 2021].

Lezoche, M., and Panetto, H. 2020. Cyber-physical systems, a new formal paradigm to model redundancy and resiliency. Enterp. Inf. Syst. **14**(8): 1150–1171. doi: 10.1080/17517575.2018.1536807.

Madan, B.B., Banik, M., and Bein, D. 2019. Securing unmanned autonomous systems from cyber threats. J Def. Model. Simul. Appl. Methodol. Technol. **16**(2): 119–136. doi: 10.1177/1548512916628335.

Meiling, W., Yafeng, L., Guoqiang, F., Yi, Y., Tong, L., and Xiao, X. 2017. Key technologies of GNSS/INS/VO deep integration for UGV navigation in urban canyon. *In* 11th Asian Control Conference (ASCC), Gold Coast, QLD, Australia, IEEE, 17–20 December 2017. pp. 2546–2551. doi: 10.1109/ASCC.2017.8287576.

Moaiied, M.M., and Mosavi, M.R. 2016. Increasing accuracy of combined GPS and GLONASS positioning using fuzzy kalman filter. Iran. J. Electr. Electron. Eng. **12**(1): 21–28.

Mount, M., and Quijano, E. 2009. Iraqi insurgents hacked Predator drone feeds, U.S. official indicates. Available from edition.cnn.com/2009/US/12/17/drone.video.hacked/index.html [accessed 14 November 2021].

Onori, D., Laghezza, F., Scotti, F., Scaffardi, M., and Bogoni, A. 2015. Coherent radar/lidar integrated architecture. *In* 2015 European Radar Conference (EuRAD), Paris, France, IEEE, 9–11 September 2015. pp. 241–244. doi: 10.1109/EuRAD.2015.7346282.

Parkinson, S., Ward, P., Wilson, K., and Miller, J. 2017. Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans. Intell. Transp. Syst. **18**(11): 2898–2915. doi: 10.1109/TITS.2017.2665968.

Seo, J., and Kim, M. 2013. eLoran in Korea – Current status and future plans. *In* European Navigation Conference, Vienna, Austria, April 2013. pp. 23–25.

Shachtman, N. 2011. Computer virus hits U.S. drone fleet. Available from brookings.edu/opinions/computer-virus-hits-u-s-drone-fleet/ [accessed 14 November 2021].
Yağdereli, E., Gemci, C., and Aktaş, A.Z. 2015. A study on cyber-security of autonomous and unmanned vehicles. J. Def. Model. Simul. Appl. Methodol. Technol. **12**(4): 369–381. doi: 10.1177/1548512915575803.
Zhang, G., and Hsu, L.-T. 2018. Intelligent GNSS/INS integrated navigation system for a commercial UAV flight control system. Aerosp. Sci. Technol. **80**: 368–380. doi: 10.1016/j.ast.2018.07.026.