Security Issues for the Internet of Drones

Ron Vetter, University of North Carolina Wilmington

This installment of Computer's *series highlighting the work published in IEEE Computer Society journals comes from* IEEE Open Journal of the Computer Society.

Unmanned aerial vehicles (UAVs), also known as *drones*, are being adopted for a wide variety of applications. With recent advances in wireless communications (5G networks) and readily available compute resources (cloud computing), UAV networks are now evolving into an Internet of Drones (IoD) paradigm. This trend is increasing opportunities for the study and development of more sophisticated UAV applications (Figure 1).

Unfortunately, the IoD is plagued by a plethora of security problems. Yang et al.[1] review security issues and solutions for IoD security; discuss IoD-related security requirements; and identify the latest developments in IoD security research. They note that because of the inherently open nature of radio transmission in IoD systems, security becomes an important consideration in the requirements of building secure applications.

The article provides a list of the key issues in the design of secure IoD solutions. It describes the most common attacks targeting the IoD, including jamming, tampering, collisions, flooding, hijacking, and denial of service. Security solutions include applying authentication techniques, blockchain schemes, intrusion detection methods, and privacy preservation approaches.

The article concludes with a discussion of IoD security-related research challenges, including a discussion of the disadvantages relating to the computational cost of blockchain solutions. The authors state that IoD systems need to offer high security while at the same time being cost-efficient—a difficult balance to achieve; however, the advent of mobile edge computing may mitigate some of the design constraints.

Digital Object Identifier 10.1109/MC.2022.3226916
Date of current version: 8 February 2023

0018-9162/23©2023IEEE

EDITOR **RON VETTER**
University of North Carolina Wilmington; vetterr@uncw.edu

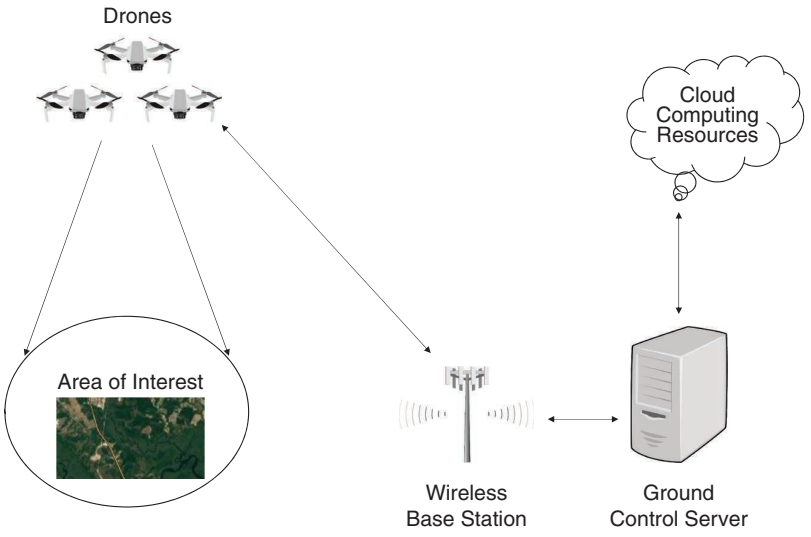

FIGURE 1. The Internet of Drones.

REFERENCE

1. W. Yang, S. Wang, X. Yin, X. Wang, and J. Hu, "A review on security issues and solutions of the Internet of Drones," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 96–110, Jun. 14, 2022, doi: 10.1109/OJCS.2022.3183003.

RON VETTER is a professor of computer science at the University of North Carolina Wilmington, Wilmington, NC 28403 USA, and the "Spotlight on Transactions" column editor for *Computer*. Contact him at vetterr@uncw.edu.

Digital Object Identifier 10.1109/MC.2023.3235124