**Security Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures.**

M. Krichen, W. Y. H. Adoni, A. Mihoub, M. Y. Alzahrani and T. Nahhal, "Security

Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures," 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 2022, pp. 184-189, doi: 10.1109/SMARTTECH54121.2022.00048.

* The security challenges in drone communications emphasize potential threats and attacks that need to be addressed as drones become more popular.
* It highlights the wide range of applications for drones across different industries, from healthcare to agriculture, showcasing their growing importance.
* The article introduces four key technologies (Blockchain, Machine Learning, Fog Computing, and SDN) to improve drone communication security, emphasizing their roles in data integrity, attack detection, latency optimization, and network control.

The article discusses the security challenges associated with drone communications and provides an overview of potential threats, attacks, and countermeasures. Drones, or Unmanned Aerial Vehicles (UAVs), have become popular and offer numerous benefits. However, they also present security risks.

The article highlights the different types of drones and control methods, emphasizing their growing importance in the healthcare, agriculture, and e-commerce sectors.

The main weaknesses of the drones were identified in flight controllers, ground control stations, and hardware components. The article also points out the dependence on sensors, which can be used to compromise drone operations. Communication issues are another concern.

The article then talks about how to improve the drone issues. Four key technologies are discussed:

Blockchain Technology: This technology guarantees data integrity and security, facilitates real-time tracking of drones, and maintains privacy. It can also provide a means of identifying and preventing unauthorized drone operations.

Machine Learning Techniques: Machine learning is operated to improve data reliability, detect and mitigate attacks, and enhance privacy protection in drone communications.

Fog Computing Technology: Fog computing offers decentralized security measures, optimizes latency in drone communications, and handles tasks like data encryption and intrusion detection.

Software Defined Networks (SDN): SDN enables centralized control and management of network traffic, allowing for the prevention of attacks and the enhancement of security in drone communication networks.

In conclusion, the article highlights the need for stakeholders to be aware of the security challenges associated with the increase of drones. While drones offer significant benefits, they also introduce issues that require careful consideration. The use of formal methods for security assessment is suggested for future research to ensure the safe and responsible use of drones.