Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey

Gaurav Choudhary, Vishal Sharma,
Ilsun You, Kangbin Yim
Department of Information Security Engineering
Soonchunhyang University, ROK
Email: {gauravchoudhary7777, ilsunu}@gmail.com,
vishal_sharma2012@hotmail.com, yim@sch.ac.kr

Ing-Ray Chen
Department of Computer Science
Virginia Tech
VA, USA
Email: irchen@vt.edu

Jin-Hee Cho
U.S. Army Research Laboratory
MD, USA
Email: jin-hee.cho.civ@mail.mil

***Abstract*—Unmanned Aerial Vehicles (UAV)-based civilian or military applications become more critical to serving civilian and/or military missions. The significantly increased attention on UAV applications also has led to security concerns particularly in the context of networked UAVs. Networked UAVs are vulnerable to malicious attacks over open-air radio space and accordingly intrusion detection systems (IDSs) have been naturally derived to deal with the vulnerabilities and/or attacks. In this paper, we briefly survey the state-of-the-art IDS mechanisms that deal with vulnerabilities and attacks under networked UAV environments. In particular, we classify the existing IDS mechanisms according to information gathering sources, deployment strategies, detection methods, detection states, IDS acknowledgment, and intrusion types. We conclude this paper with research challenges, insights, and future research directions to propose a networked UAV-IDS system which meets required standards of effectiveness and efficiency in terms of the goals of both security and performance.**

***Index Terms*—Unmanned aerial vehicle, intrusion detection system, security, attack, vulnerability.**

I. Introduction

The proliferation of unmanned aerial vehicles (UAVs) and their diverse applications in many different domains have been realized due to their merit of dynamic reconfigurability, fast response, and ease of deployment. In particular, the applications of networked UAVs have attracted major industry players such as Google, Facebook, Boeing, and Amazon. In addition, their applications in serving military and civilian missions have been explored in diverse domains to provide public safety, surveillance, medical services, and/or military mission support [13]. In Table I, we discuss the key application domains where UAVs can be applied to assist given missions in different domain context.

The key merit of UAVs is known as its high reconfigurability and mobility. However, its mobility also exposes an issue of controllability towards the aerial vehicles and causes link distortion in UAV networking. Despite these concerns, UAV-assisted networks have been recognized for the benefit of easy deployment of wireless connectivity that does not require any physical infrastructure [19, 20].

UAVs provide high benefits to assist the goals of many different applications, as summarized in Table I. However, they also introduce the following challenges [21]: (1) the architectural design of drone communication lacks a standard or unification; (2) UAV-assisted communication networks suffer from an issue of dedicated spectrum sharing; (3) UAV deployment and path planning should be considered during spectrum allocations due to its potential impact on energy efficiency; and (4) UAV communications introduce additional overhead to architectural design, deployment, and consistency with large and reliable networks along with their security. In this work, we particularly focus on security challenges.

This paper provides the following **key contributions**:

- We survey the key state-of-the-art UAV-IDS approaches and associated taxonomies which can provide a good overview to answer what a UAV-IDS system is, what the key components need to be considered in the UAV-IDS, and what the key security concerns should be considered, associated with the key components of the UAV-IDS.
- We discuss the main research challenges and hurdles to build a cyber-physical hardened UAV-IDS system under highly resource-constrained, hostile, dynamic, and distributed environments reflecting the key characteristics of military tactical characteristics.
- We suggest future research directions to move towards based on the discussed research challenges and learned lessons / insights.

The remainder of the paper is organized as follows. Section II provides the background and goal of UAV-IDS. Section III discusses the taxonomies used in the structure and classification of UAV-IDS. Section IV discusses the evaluation techniques of the state-of-the-art UAV-IDS approaches. Section V discusses research challenges derived from the inherent characteristics of UAV-IDS environments. Section VI concludes the paper and suggests future work directions.

TABLE I
DOMAINS AND APPLICATIONS OF UAVS

Domain	Key example applications	Achieved roles by UAVs
Law enforcement surveillance	Search and rescue	Equipped with camera
Public safety communications	Voice communications in case of disaster	Aerial base stations
Environmental applications	Climate change	Equipped with sensors
Logistics	Goods shipping / delivery in urban areas	Drone as a transportation medium
Military applications	Searches for lost or injured soldiers	Armed with live video remote communications to ground troops, essential gear, or weapons
Medical field applications	Delivering aid packages, medicines, vaccines, blood and other medical supplies to remote areas	Drone as a transportation medium
Video and photography	Events (e.g., social gatherings, sports games, or competitions)	Equipped with camera
Agriculture	Crop monitoring and soil and field analysis	Equipped with sensors

II. OVERALL DESCRIPTION OF UAV-IDS ENVIRONMENTS

An unmanned aerial vehicle based intrusion detection system (UAV-IDS) is developed to detect anomaly behaviour or illegal activities in a network by automatically analyzing the behaviors or activities based on given hypothesis and/or policies, which are governed by the security rules of the given network [2]. The UAV-IDS monitors system configuration, data files, and/or network transmission to check whether there exists an attack. Hence, the UAV-IDS is to mitigate the effect of the attacks aiming to prevent any covert / overt operations from exposed vulnerabilities of the system. In addition, UAV-IDSs aim to detect the misuse of UAVs. Misuse can be defined as any undesirable activity which can cause any harmful effect in terms of either performance or security to an entire swarm of the UAVs. Attacks explore the vulnerabilities of UAV systems, where the vulnerabilities can be the result of misconfigurations of UAV networks, an implementation fault, flawed designs and/or protocols [4].

Fig. 1 shows an example scenario for an UAV-IDS. UAV-IDSs monitor signals, command traffic, control instructions, working behavior, energy consumption, and/or operations of UAV components. In addition, it analyzes the data flow and gather information from different components of UAVs during their operations as a network node. The UAV-IDSs are capable of enhancing reliability and/or security of UAV communications in an efficient and effective manner.

A UAV-IDS can be placed on a UAV or a ground control system and maintains the security and reliability of the UAV and the ground control system. The placement of a UAV-IDS can be determined based on the level of required security, such as required security levels in terms of confidentiality, integrity, availability, and authorization. In addition, a UAV-IDS is responsible for ensuring guarding the UAV system against unlawful activities or attacks. The incorporated security policies for UAVs provide low-complex rules to detect anomalies or potential threats. These policies can be designed through different approaches or algorithms based on the requirements of the UAV system. Most existing IDSs for UAVs use behaviour-based detection mechanisms [23].

III. TAXONOMIES OF UAV-IDS SYSTEM COMPONENTS

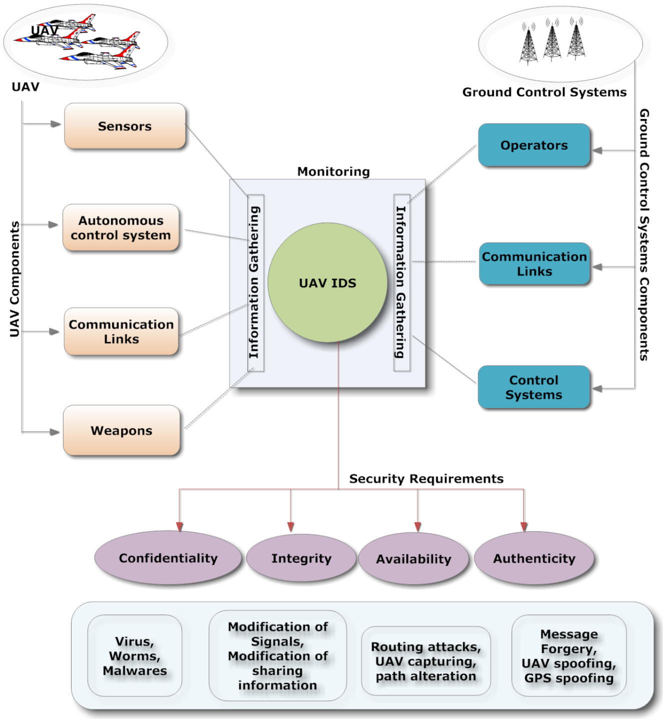

Fig. 1. An operational overview of UAV-IDS.

We summarize the key component taxonomies of the UAV-IDS system in Fig. 2 which discusses its key components, including information gathering sources, deployment strategies, detection methods, detection states, acknowledgment, and intrusion types. We give the detail of each component as below.

A. Information Gathering Sources

A UAV is embedded with a cyber-physical system consisting of sensors and/or actuators. Sensors provide data (or information) to an actuator that can control the UAV. The collected data are used for analysis to make mission-related critical decisions. The information gathering sources can be classified as follows: [10]

- **Sensors**: Sensors collect information in terms of signals and/or behavior through sensors like inertial sensors, location sensors, and/or threat sensors. The sensor may be implicitly tied with a UAV or explicitly tied to a specific task object, like weather capturing sensors. The

information retrieval by a malicious node from any of onboard sensors in a critical situation can impact the performance of a UAV in a networked scenario.
- **Communications links**: Communication links support transmissions directly to UAVs in mission areas and/or allow simultaneous sharing of information among multiple UAVs and the ground system. They also secure data transfers by monitoring the traffic between a source and a destination.
- **Ground control system (GCS)**: The GCS has a significant component in UAVs and is charged of conducting intelligent surveillance and reconnaissance based on data generated by the unmanned aircraft's payload.
- **UAV components**: The components within a UAV include a power supply unit, antennas, transceiver units, navigation systems, and an inbuilt UAV control system. All inter- and intra-communications take place through these components, in which the information is exchanged among these components for an effective control and maneuvering of UAVs. This information should be examined for security purposes and timely patches should be available upon the detection of potential threats.
- **Deployment strategies**: The deployment of an IDS in UAVs is critical because effective optimization is required for balancing the trade-off between IDS operations and UAV transmissions. The system should be maintained to enhance performance of the UAV with their effective operations and environmental conditions along with controllable activities of the deployed IDS. The IDS can be deployed based on two methods:
    1) **Ground-coordinated or network-initiated basis**: In the ground coordinated IDS, all the gathered information is analyzed on the ground station and appropriate decisions are made on the basis of analyzed data; and
    2) **Autonomous or host basis**: With an autonomous deployment of IDSs, UAVs acting as hosts to deploy IDSs should conduct data analysis and control other UAVs, along with coordinating between these two. In this deployment type, the IDS is placed within the system control of UAVs in the form of hardware or software.

B. *Intrusion Detection Systems (IDSs)*

The key mechanism of IDSs can be classified as follows:

- **Specification-based [26]**: A UAV-IDS is incorporated with respective rules specified based on the expected behaviors of UAVs. These specified rules are applied to monitor successful executions of the UAV system.
- **Signature-based [27]**: This method aims to detect known attacks based on pre-defined, known signatures. Upon detecting anomaly activities, a detection operation is triggered to identify a matched signature to ensure the detection of an intrusion.
- **Anomaly-based [14]**: Anomaly behavior is detected based on a failure or an illegal activity observed in a system. With the goal of detecting known and/or unknown attacks, this method uses learning or a filtering mechanism, which can significantly enhance the detection of unknown attacks in the absence of pre-defined signatures of the unknown attacks.
- **Hybrid-based [1]**: This method is a hybrid approach by integrating two or more detection methods, such as specification plus anomaly, in order to provide a strong detection policy that can catch known and/or unknown attacks.

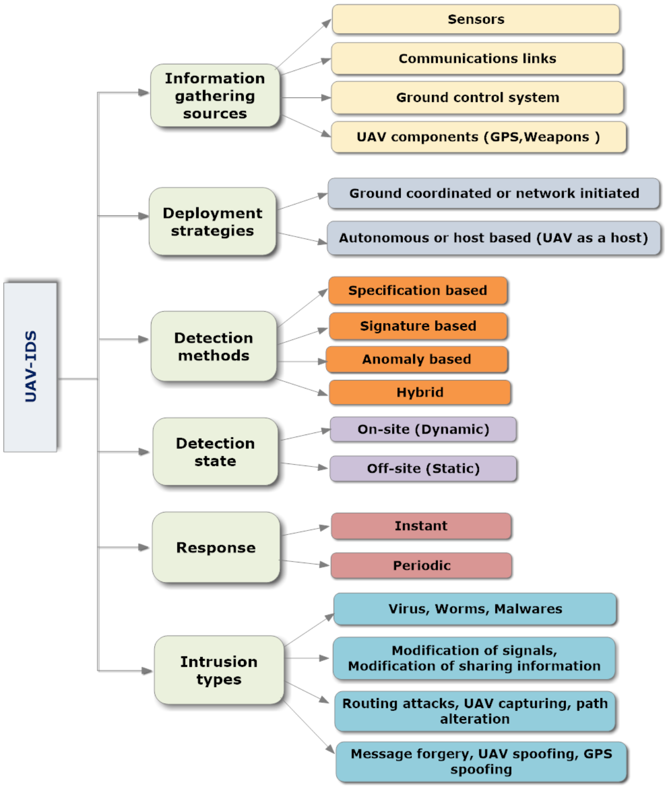
UAV-IDS
Information gathering sources
Sensors
Communications links
Ground control system
UAV components (GPS,Weapons)
Deployment strategies
Ground coordinated or network initiated
Autonomous or host based (UAV as a host)
Detection methods
Specification based
Signature based
Anomaly based
Hybrid
Detection state
On-site (Dynamic)
Off-site (Static)
Response
Instant
Periodic
Intrusion types
Virus, Worms, Malwares
Modification of signals, Modification of sharing information
Routing attacks, UAV capturing, path alteration
Message forgery, UAV spoofing, GPS spoofing

Fig. 2. Taxonomy of UAV-IDSs.

C. *Detection States*

Based on the source of information, we can categorize two major detection states:

- **On-site (or dynamic)**: The detection state is evaluated based on data collected and monitored from real-time operations; the detection analysis and decisions are made at on-site UAVs.
- **Off-site (or static)**: The detection state is evaluated based on data collected by an IDS from all information sources; the detection is made based on the analysis of all collected data received in the IDS.

D. *IDS Acknowledgment*

Based on the result of data analysis, a UAV-IDS makes decision on whether there exists an attack via an IDS acknowledgment. This IDS acknowledgment has two forms:

TABLE II
SURVEY ON THE STATE-OF-THE-ART ON EXISTING UAV IDS APPROACHES.

Reference	Proposed scheme	Key method(s) / metrics
Blasch et al. [3]	War planning situation awareness tool	ROC for visualization
Lauf et al. [10]	Hybrid IDS	Maxima and cross-correlation detection
Shen et al. [23]	Markov game theoretic approach	Deployment of IDS, configuration of email-filtering, firewall settings, and shutdown or reset policies for servers.
Muniraj and Farhood [12]	Framework for detection of cyber-physical attacks on the sensors	Anomaly-based detectors based on knowledge of the physical system and statistical analysis.
Sedjelmaci et al. [17]	Hierarchical IDS	Threat classification & behavior monitoring
Mitchell and Chen [11]	Behavior rule-based evaluations	Minimizing false positives & false negatives
Kwon et al. [8]	Safety analysis under stealthy cyber attacks	Real-time safety assessment
Lauf and Robinson [9]	Distributed resource system	Intrusion-tolerance strategy
Shen et al. [24]	Game theoretic approach	Based on the three levels: object, situation and threat.
Sedjelmaci et al. [15]	Security game framework	Optimal setting identification based on intrusion detection rate with minimum overhead using Bayesian game
Trafton and Pizzi [25]	Network service suite	Framework for information assurance of UAVs

- **Instant acknowledgement**: In this acknowledgment, an IDS monitoring is performed at real-time and decisions or alarms are generated in the form of instant acknowledgments.
- **Periodic acknowledgement**: In this acknowledgement, an IDS continuously gathers the data but the decisions are based on the periodical analysis of received data.

E. Intrusion Types

A UAV-IDS should be able to detect the following intrusion types:

- Virus, worms, and/or malware;
- Modification of signals, modification of sharing information;
- Routing attacks, UAV capturing, and/or path alteration; and
- Message forgery, UAV spoofing, and/or GPS spoofing.

IV. SURVEY OF EXISTING UAV-IDS APPROACHES

UAV networks are highly sensitive over which critical information will be exchanged between UAVs and the ground station. Table 2 summarizes the state-of-the-art UAV-IDS approaches, aiming to enhance security and performance with the end goal to build a cyber-physical hardened system being protected against inside and outside attackers on networked UAVs. Below we survey these existing approaches using our proposed taxonomies discussed in Section III.

Blasch et al. [3] proposed a war planning situation awareness tool by leveraging the Receiver Operating Characteristic (ROC) plots to visualize the effectiveness of their classifications. The effective classification is developed based on matrices where situation assessment is used to derive relations between a given classification and a location. Lauf et al. [10] developed a decentralized anomaly-based detection technique, which uses maxima and cross-correlation detection methods. The Maxima Detection System (MDS) allows the characterization of either one or zero suspicious nodes. Cross-correlation detection methods are capable of detecting multiple intrusions. However, this work does not capture the quality of the IDS based on detection errors including false positives and false negatives.

Shen et al. [23] took a game theoretic approach by considering three levels of states: object, situation, and threat. This approach projects attack activities while focusing on the states of the network. Shen et al. [24] further developed a cooperative surveillance strategy to improve the performance through adaptive Markov game based on the cooperative jamming strategies. These are performed on the basis of four defensive parameters, including IDS deployment, configurations of email-filtering, firewall settings, and shut down or reset policies for servers.

Muniraj and Farhood [12] focused on the attacks over small UAVs by identifying malicious activities over their sensors. In the proposed framework that detects cyber-physical attacks, sensors are designed based on the knowledge of physical system and statistical analysis techniques. However, the proposed scheme was not capable of detecting combination of piece-wise constant attacks of smaller magnitude. Sedjelmaci et al. [17] proposed an hierarchical IDS and intrusion response mechanism by classifying threats and monitoring UAV behavior to detect malicious activities.

Mitchell and Chen [11] proposed a specification-based detection technique to guard a UAV system against cyber-attacks. This work used a behavior rule-based UAV-IDS, in which the behavior rules are constructed based on defined attack models, considering reckless, random, and opportunistic attacks. This work minimized detection errors (i.e., false positives and false negatives) based on the critical tradeoff between security and performance of UAVs. Kwon et al. [8] developed a real-time safety assessment algorithm based on reachability analysis to deal with cyber attacks.

Lauf and Robinson [9] developed a distributed sensing mechanism to build a fault-tolerant resource management system. The proposed mechanisms uses a service discovery protocol (SDP) where SDP flooding can introduce a burst of communications leading to traffic congestion or bottleneck issues. Sedjelmaci et al. [16] proposed a threat estimation model based on estimated beliefs towards whether a threat exists in the system. In addition, this work incorporated specific detection policies to maintain data integrity and network availability. Sedjelmaci et al. [15] took one step further to propose a robust UAV assisted network against lethal attackers, namely a Security Game Framework (SGF), which is formulated based on Bayesian game among the suspected nodes. This approach formulates two attack-defense problems between IDS and the attacker, and between intrusion ejection system and the suspected nodes.

Trafton and Pizzi [25] proposed the so called Joint Airborne Network Services Suite, which aims to integrate an airborne military network by allowing the implementation of various possible hardware and software solutions. In this work, an IDS is considered as an integral part of their assurance strategy.

V. Research Challenges

UAVs are operated remotely while receiving control and command messages from ground stations. These command and control messages are transmitted over different channels and variable transmission rate. Security vulnerabilities can be exploited to compromise confidentiality, integrity, availability, and authorization of networked UAVs [6, 7]. Message security and control signal protections are achieved by cryptographic mechanisms. However, security issues, like unauthorized access, malicious control, illegal connection, or other malicious attacks, require strategic solutions without compromising performance. Identifying and mitigating threats in UAV networks efficiently and effectively is a first step to secure UAV networks [18, 22].

The significant increase of threats and/or attacks in UAV networks brought our attention on the issue of the deployment of IDS which will play a key role to achieve the effectiveness and efficiency of the UAV-IDS [5]. In a UAV environment, an IDS is being operated based on specific rules and/or policies to determine whether an observed activity is malicious or not. The results of the IDSs can be used to develop strategies to mitigate the identified risks. However, the design and development meeting these two requirements (i.e., effectiveness and efficiency of the developed IDS) is not a trivial goal because it often requires a time-consuming, high-overhead process which can often exceed the benefit of introducing high security in practice.

To achieve the UAV-IDS system that meets required levels of effectiveness (i.e., minimizing detection errors with minimum service interruptions) and efficiency (i.e., reducing computational and communication overhead), we identify the following challenges on the table to pave a way to build a cyber-physical hardened UAV-IDS system:

- **Detection latency**: The detection latency can be used as a measure of agility of an IDS. However, there is a critical tradeoff in that triggering the IDS more often leads to incurring more communication/computation overhead, which naturally results in low efficiency, and vice-versa. Hence, we need to make a good balance to achieve both efficiency and effectiveness in order to build an affordable, secure UAV-IDS systems in practice.
- **IDS computational cost**: The computational cost associated with IDSs is closely related to how much we want to achieve the accuracy of the IDS and security vulnerabilities we allow in a given system. Again, this issue is not trivial because more cost not only incurs high overhead, but brings more benefit in enhancing security.
- **Implementation overhead**: The high implementation overhead of IDSs causes power consumption and degrades the performance of UAVs resulting in a network shutdown.
- **Threat & behavior modeling**: IDS detection techniques incorporate behaviors of UAVs. The rules are designed by reflecting the UAVs' behavior and/or possible threats. However, accurate observations of threat/attack behaviors and accordingly their correct modeling is not a trivial task although achieving it can provide an enormous benefit to expedite the development of better defense strategies.
- **Effective threat assessment**: An effective threat assessment is critical to mitigating vulnerabilities and risks associated with threats occurred. In particular, developing effective threat assessment policies is the key to enhance both security and performance of UAV-IDS systems.
- **Maximum network throughput with minimum cost**: This is a typical tradeoff issue any network can face as these two goals are conflicting to each other. However, based on dynamic monitoring to capture an accurate system state, both goals that are dynamically set can be achievable.
- **Lightweight IDS with minimum resource consumption**: As UAVs are battery-operated and resource-constrained, the development of lightweight IDS mechanisms is highly challenging but a must to achieve in networked UAVs.
- **Effective monitoring and attack response**: The response against an attack is naturally related to how quickly the attack is detected by a given IDS. This implies that the effectiveness of the IDS is closely related to how quickly the system can respond to the detected attack. This is indeed the issue of the agility of a system which should take appropriate actions in order to minimize damages or vulnerabilities caused by the intrusion which exploits system vulnerabilities. The contested nature of UAV environments, characterized by resource-constraints, high hostility, high dynamics, and distributed nature, also adds more challenges to achieve this goal.

VI. Conclusion & Future Research Directions

In this work, we provided a brief overview of the state-of-the-art UAV-IDS mechanisms. In addition, we discussed related design challenging issues to develop effective and efficient UAV-IDS mechanisms, considering high resource-constraints, high hostility characterized by sophisticated attack/threat behaviors, and distributed nature causing high security vulnerabilities. We also defined the taxonomies to describe the key components of UAV-IDS systems based on the state-of-the-art existing works. Lastly, we discussed key research challenges that should be considered for future research plans, aiming to build an affordable, secure cyber-physical UAV-IDS system.

As future work directions, we plan to conduct the following:

- **Define an attack model that captures key attack behaviors targeting for UAV-IDS systems**. We will derive an attack graph and build a set of corresponding countermeasures to deal with those attacks.
- **Develop a behavior rule specification-based UAV-IDS** that uses minimum memory while maximizing detection accuracy by checking the anomaly of an observed behavior. Formal verification and Bayesian estimation based ground truth check for anomaly behaviors can be used to validate the developed set of specification rules.
- **Measure the effectiveness and efficiency of the developed lightweight UAV-IDS** using the metrics of agility or resilience.

Acknowledgment

This work was supported by the Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (2015-0-00508, Development of Operating System Security Core Technology for the Smart Lightweight IoT Devices). This work is also supported in part by the U.S. AFOSR under grant number FA2386-17-1-4076. Dr. Ilsun You is the corresponding author.

References

[1] M. A. Aydın, A. H. Zaim, and K. G. Ceylan, "A hybrid intrusion detection system design for computer network security," *Computers & Electrical Engineering*, vol. 35, no. 3, pp. 517–526, 2009.

[2] E. Biermann, E. Cloete, and L. M. Venter, "A comparison of intrusion detection systems," *Computers & Security*, vol. 20, no. 8, pp. 676–683, 2001.

[3] E. P. Blasch, J. J. Salerno, and G. P. Tadda, "Measuring the worthiness of situation assessment," in *Proceedings of the 2011 IEEE National Aerospace and Electronics Conference (NAECON)*, 2011, pp. 87–94.

[4] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," *Computer Networks*, vol. 31, no. 8, pp. 805–822, 1999.

[5] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1-2, pp. 18–28, 2009.

[6] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 134–139, 2017.

[7] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 2012, pp. 585–590.

[8] C. Kwon, S. Yantek, and I. Hwang, "Real-time safety assessment of unmanned aircraft systems against stealthy cyber attacks," *Journal of Aerospace Information Systems*, vol. 13, no. 1, pp. 27–45, 2015.

[9] A. P. Lauf and W. H. Robinson, "Fault-tolerant distributed reconnaissance," in *IEEE Military Communications Conference (MILCOM'2010)*, 2010, pp. 1812–1817.

[10] A. P. Lauf, R. A. Peters, and W. H. Robinson, "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks," *Ad Hoc Networks*, vol. 8, no. 3, pp. 253–266, 2010.

[11] R. Mitchell and I. R. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 5, pp. 593–604, 2014.

[12] D. Muniraj and M. Farhood, "A framework for detection of sensor attacks on small unmanned aircraft systems," in *2017 IEEE International Conference on Unmanned Aircraft Systems (ICUAS)*, 2017, pp. 1189–1198.

[13] G. Pajares, "Overview and current status of remote sensing applications based on unmanned aerial vehicles (uavs)," *Photogrammetric Engineering & Remote Sensing*, vol. 81, no. 4, pp. 281–329, 2015.

[14] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Computer networks*, vol. 51, no. 12, pp. 3448–3470, 2007.

[15] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A bayesian game-theoretic methodology," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 5, pp. 1143–1153, 2017.

[16] H. Sedjelmaci, S. M. Senouci, and M.-A. Messous, "How to detect cyber-attacks in unmanned aerial vehicles network?" in *IEEE Global Communications Conference (GLOBECOM)*, 2016, pp. 1–6.

[17] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2017.

[18] V. Sharma and R. Kumar, "Teredo tunneling-based secure transmission between UAVs and ground ad hoc networks," *International Journal of Communication Systems*, vol. 30, no. 7, 2017.

[19] V. Sharma, M. Bennis, and R. Kumar, "UAV-assisted heterogeneous networks for capacity enhancement," *IEEE Communications Letters*, vol. 20, no. 6, pp. 1207–1210, 2016.

[20] V. Sharma, R. Sabatini, and S. Ramasamy, "UAVs assisted delay optimization in heterogeneous wireless networks," *IEEE Communications Letters*, vol. 20, no. 12, pp. 2526–2529, 2016.

[21] V. Sharma, R. Kumar, and R. Kumar, "QUAT-DEM: Quaternion-DEMATEL based neural model for mutual coordination between UAVs," *Information Sciences*, vol. 418, pp. 74–90, 2017.

[22] V. Sharma, R. Kumar, K. Srinivasan, and D. N. K. Jayakody, "Coagulation attacks over networked UAVs: concept, challenges, and research aspects," in *International Conference on Communication, Management and Information Technology (ICCMIT)*. Warsaw, Poland: IEEE, 2017, pp. 1–5.

[23] D. Shen, G. Chen, E. Blasch, and G. Tadda, "Adaptive markov game theoretic data fusion approach for cyber network defense," in *IEEE Military Communications Conference (MILCOM 2007)*, 2007, pp. 1–7.

[24] D. Shen, G. Chen, J. B. Cruz, and E. Blasch, "A game theoretic data fusion aided path planning approach for cooperative UAV ISR," in *2008 IEEE Aerospace Conference*, 2008, pp. 1–9.

[25] R. Trafton and S. V. Pizzi, "The joint airborne network services suite," in *IEEE Military Communications Conference (MILCOM'2006)*, 2006, pp. 1–5.

[26] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for AODV," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, 2003, pp. 125–134.

[27] V. Vaidya, "Dynamic signature inspection-based network intrusion detection," Aug. 2001, US Patent 6,279,113.