Security Modeling of Autonomous Systems: A Survey

FARHA JAHAN and WEIQING SUN, University of Toledo
QUAMAR NIYAZ, Purdue University Northwest
MANSOOR ALAM, University of Toledo

Autonomous systems will soon be integrating into our lives as home assistants, delivery drones, and driverless cars. The implementation of the level of automation in these systems from being manually controlled to fully autonomous would depend upon the autonomy approach chosen to design these systems. This article reviews the historical evolution of autonomy, its approaches, and the current trends in related fields to build robust autonomous systems. Toward such a goal and with the increased number of cyberattacks, the security of these systems needs special attention from the research community. To gauge the extent to which research has been done in this area, we discuss the cybersecurity of these systems. It is essential to model the system from a security perspective, identify the threats and vulnerabilities, and then model the attacks. A survey in this direction explores the theoretical/analytical system and attack models that have been proposed over the years and identifies the research gap that needs to be addressed by the research community.

CCS Concepts: • **Computing methodologies** → **Modeling and simulation**; **Model development and analysis**; • **Computer systems organization** → **Robotic autonomy**; *Evolutionary robotics*; • **Security and privacy** → *Systems security*; Security services; • **Human-centered computing** → *Human computer interaction (HCI)*;

Additional Key Words and Phrases: Cybersecurity, modeling, autonomous system (AS), Unmanned Aerial Vehicles (UAVs), driverless car, robots

ACM Reference format:
Farha Jahan, Weiqing Sun, Quamar Niyaz, and Mansoor Alam. 2019. Security Modeling of Autonomous Systems: A Survey. *ACM Comput. Surv.* 52, 5, Article 91 (September 2019), 34 pages.
https://doi.org/10.1145/3337791

1 INTRODUCTION

With the advancement in the field of artificial intelligence (AI) and machine learning (ML) in the last few decades, the increased usage of autonomous systems is evident in almost every domain. The design and development of autonomous vehicles in several developed countries to ease transportation is no secret. On the other hand, domains such as agriculture, healthcare, military, and space exploration have found many use cases for these systems. The driverless car revolution has

Authors' addresses: F. Jahan, W. Sun, and M. Alam, University of Toledo, Toledo, OH, 43606; emails: farha.jahan@rockets.utoledo.edu, {weiqing.sun, mansoor.alam2}@utoledo.edu; Q. Niyaz, Purdue University Northwest, Hammond, IN, 46323; email: qniyaz@pnw.edu.

0360-0300/2019/09-ART91 $15.00
https://doi.org/10.1145/3337791

already begun, and the self-driving technology has been embraced by Tesla, Uber, and Waymo (McBride 2018). Robots will soon be integrated into our lives as a home assistant, a pet (Dormehl 2017), or a friend like Sophia (the AI) (Galeon 2017).

The primary objective to develop an autonomous system is to collaborate with humans and assist them in various tasks. These tasks could be the ones that require: precision such as surgeries; operation in challenging and life-threatening situations, such as space exploration, search and rescue missions, or nuclear power plants; or assistance to elders at home. However, improper implementation or malicious intent may lead to disasters. An incident was reported in a San Francisco mall where a patrolling robot failed to recognize a toddler and accidentally attacked him (Kashmir Hill 2016). Recently, a self-driving Uber vehicle was caught up in a fatal accident (Wakabayashi 2018). Armed and autonomous weapons are manufactured by high-tech military organizations in the USA, China, and South Korea. Sci-Fi novels and movies like "I, Robot" and "Terminator" have created a negative image and fear for these systems that they may go against humans and harm them. There is an ongoing campaign against killer robots (fully autonomous weapons) that would have complete decision controls on their target (CCW 2018). If malicious users hack or control such systems by exploiting their vulnerabilities, machines turning against humans would not just be concepts and scenes from movies. These autonomous systems are still in the evolving stage. Analyzing the security and safety issues associated with these machines and thoroughly testing them before they are made part of our lives (Caughill 2017; Galeon 2017) become essential.

The researchers from different focus groups have put a lot of effort to bring us to the current level of understanding regarding autonomy. In the last few years, excellent surveys on autonomy have been published (Baxter et al. 2012; Beer et al. 2014; Mostafa et al. 2017). Goodrich et al. (2007) presented an overview of human-robot interaction (HRI). Huang has described autonomy related terminologies and jargon in Huang (2004). Level of trust could be a significant factor in deciding the autonomy levels in autonomous systems—discussed in Shahrdar et al. (2017). However, to the best of our knowledge, the research community lacks literature that discusses the cybersecurity of autonomous systems in general. The primary objective of this work is to provide an in-depth study of cybersecurity modeling of different classes of autonomous systems. The work can help carry out further research on the security modeling of a generalized autonomous system architecture. In addition, we discuss the historical evolution of the concepts and factors that define autonomy and its levels. In general, the term "autonomy" discusses the representation and implementation of its levels determined by factors and functionality of the system from being manual to fully-autonomous and in-between. Having a perspective of the application domain and the scope of implementation may provide a different look to the security modeling of these systems. The following are the key contributions of the article toward the body of knowledge on autonomous systems:

- A discussion on the historical evolution of autonomy and the current trends in this area,
- A discussion on the cybersecurity of these systems that are being explored in industry and academia alike,
- Threats, vulnerabilities, and attack modeling of various autonomous systems.

This article is organized as follows. Section 3 reflects on the historical evolution of autonomy, approaches, and current trends in this domain. Section 4 discusses cybersecurity issues related to these systems. Section 5 discusses the system modeling along with threats, vulnerabilities, and attacks modeling. Section 6 summarizes the overall concept of the article. Finally, we discuss some of the research challenges and future directions in Section 7 and conclude in Section 8. The complete structure of the article is shown in Figure 1.

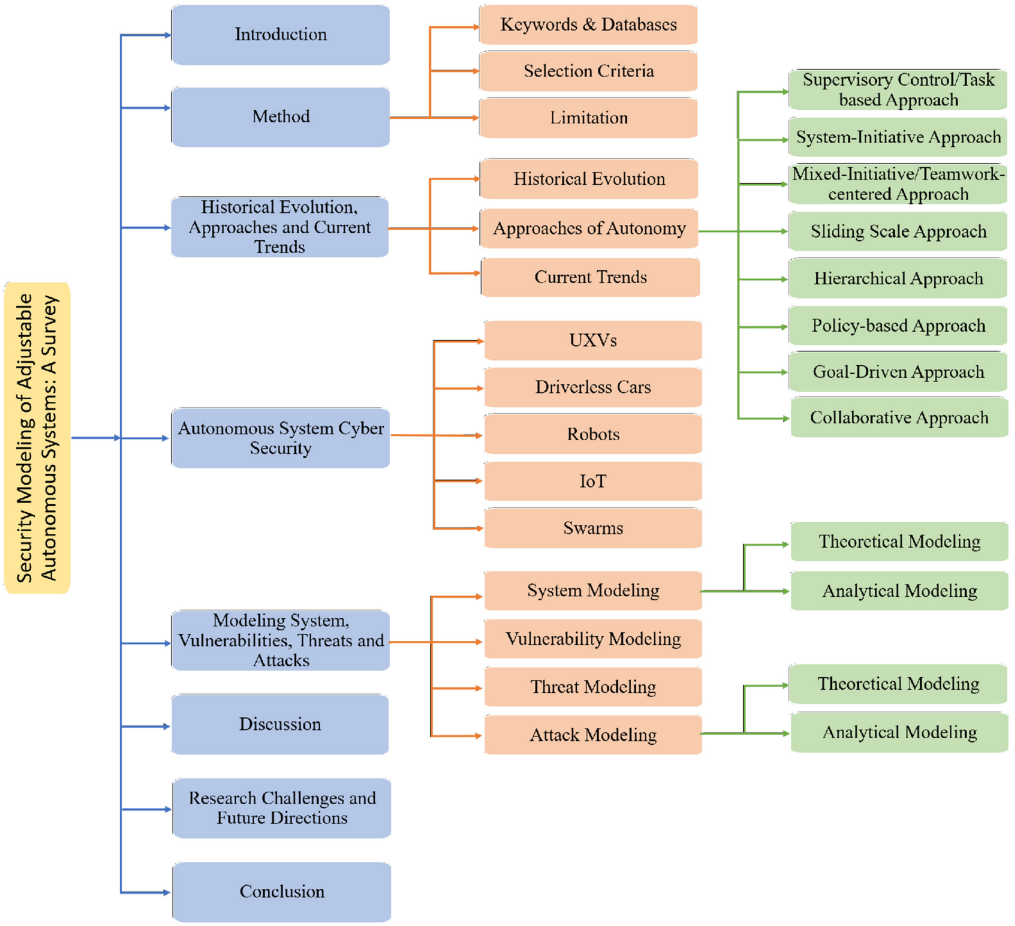

Fig. 1. Structure of the article.

2 METHOD

2.1 Keywords and Databases

Based on the industrial and academic domains that focus on autonomous systems, a group of keywords was chosen to limit the scope of this survey. The autonomous systems that we have explored in this study include unmanned vehicles (UXVs), robots, driverless cars, swarms, and autonomous Internet of Things (IoT), focusing more on the former three. The survey was restricted to security (threats, vulnerabilities, and attacks) and applications of these systems in the domains such as home assistants, healthcare, surveillance, search and rescue missions, and space exploration. The keywords used for the search process are listed in Table 1 and the resources availed for literature search include Google Scholar, ACM, and IEEE Xplorer digital libraries, and ScienceDirect.

2.2 Selection Criteria

After a detailed search, we evaluated the articles based on the following criteria:

—the history of automation and its levels
—approaches of autonomy and current trends

Table 1. Keywords Used

Core Concepts	Primary keywords
Autonomy	autonomous systems, level of automation (LoA), autonomy approaches, UXVs, driverless cars,
Artificial Intelligence	robots, software agents, IoT
Human Machine Teaming	swarms, transfer of control
Autonomous System Modeling	analytical and theoretical system modeling; threats, vulnerabilities, and attack modeling
Autonomous System Security	DDoS, jamming, ransomware, stealthy deception attack
	Secondary keywords
	supervisory control, mixed-initiative, goal-driven, collaborative control, sliding scale, hierarchical, healthcare, home-assistants, industrial robots

—cybersecurity of an autonomous system
—modeling of an autonomous system, vulnerabilities, threats, and attacks

We further refined the selected articles using primary and secondary keywords for each section. We identified the theoretical and analytical security modeling of the autonomous systems and carried out another level of filtration to obtain the most appropriate research work. Experimental modeling and evaluation of these systems were beyond our scope of research. Hundreds of articles were narrowed out in the search process based on the keywords and objectives. Out of these, a total of 88 articles were considered to discuss the cybersecurity of the autonomous systems and 26 articles to discuss the cybersecurity modeling of these systems.

2.3 Limitations

A fundamental constraint that we found during the review process is the lack of literature that discusses the security of individual as well as generalized autonomous systems. The study of cybersecurity is new in this domain and so is its implementation. This resulted in a limited number of primary articles reviewed for the security and modeling sections of the survey. The discussion focuses on the security of three autonomous systems (Unmanned Aerial Vehicles (UAVs), robots and driverless cars) that are worth a detailed review because of their popularity. Swarms are an extension of these systems, and Autonomous Internet of Things (AIoT) is a new concept yet to be explored. We believe in having studied the most applicable works available in this area of research.

3 HISTORICAL EVOLUTION OF AUTONOMY, APPROACHES, AND CURRENT TRENDS

3.1 Historical Evolution

In the last few decades, concepts and modeling of automation have evolved considerably. Fields such as HRI, Human Machine Teaming (HMT), AI, and Unmanned Systems (UMS) share the concepts of autonomy. As with many inconceivable technologies of the current era, the ideation of such systems can be dated back to religious myths (Origins 2013), poets (Homer n.d.; Yeats 1933), artists (Rosheim 2006), and storytellers (Wiener and Others 1964), thereby materializing into remote-controlled inventions (Turi 2014a, 2014b), movies (Wold and Staff 2015; ZDNet 2018), and science fiction literature (Newitz 2013). With the advancement in associated areas and state-of-the-art technologies like robot mechanics, sensors and actuators, processors, navigation and communication, the definition and levels of autonomy (LoA) have gone through multiple

revisions and modifications to be up-to-date with the other emerging and advancing technologies so that it can be adapted for more robust use.

The word "Robotics" was first invented by Isaac Asimov in the story "Liar" in 1941 while "Automation" was first coined by Dal Harder, a Ford executive, in 1947. As recounted in Sheridan and Verplank (1978), vehicles remotely controlled by human operators were called master-slave manipulators in the early history (1954) of robotics. In the 1950s, when industries like General Electric (GE) was working to build industrial robots such as "Yes Man" and "Handyman," the US Army was exploring the ideas of teleoperated rovers (MOBOT) and Project Horizon (Turi 2014a).

In 1978, Sheridan and Verplank (1978) discussed the idea of supervisory control and explained how it is different from teleoperators and manipulators, listing the 10-level scale of autonomy (LoA), which has been a background work for further research in this area till today (Farooqui and Niazi 2016; Goodrich et al. 2008; Navarro 2018; Parasuraman et al. 2000; van der Kleij et al. 2018). As more systems were gaining autonomy, operators' roles were getting reduced to a supervisor or passive monitor of these systems and performance problems on human out-of-the-loop emerged because of many failure incidents of these systems (Bainbridge 1983; Norman 1990; Wiener and Curry 1980). The authors realized the lack of feedback, poor communication interfaces, and lower levels of situation awareness (Norman 1990). A new approach to automation was a solution to these problems with new roles for automation, opting for adaptive automation, incorporating situational awareness in the design process, and revisiting the LoA (Endsley 1995). Endsley et al. (1987, 1988) focused their research on improving situational awareness. They worked on bringing human-in-the-loop (Endsley 1987), moving toward adaptive autonomy and enhancing the LoA (McDaniel 1988). Adaptive autonomy, proposed back in 1976 by Rouse, is an autonomous system in which the LoA changes, initiated by particular events in the task environment, physiological methods, task load, or by changes in operator performance (Parasuraman et al. 1992). An initial survey (Sheridan 1992) on telerobotic, supervisory control, and automation tried to address questions arising in those fields at that time; provided application history of such systems in the field of aircraft, nuclear power, and intelligent vehicle highway (IVH), brought forth the areas that were still immature and the prospects.

In Parasuraman et al. (1992), the authors took a step back and did extensive research on the issues related to adaptive autonomy and how it should be approached in design. They outlined what, when, and how the adaptation would be invoked. Would it be a measurement- or modeling-based adaptive system? What would be the logic of implementation? And so on. The idea was that adaptive automation would aid in solving human out-of-the-loop performance problems and provide a dynamic allocation of tasks between the operator and the system, as and when needed. It could increase the operator's performance thereby increasing management load, which would, in turn, affect the operator's situation awareness (Endsley 1995). As recounted in Beer et al. (2014), Endsley and Kaber (1999) proposed a revised 10-scale taxonomy based on input functions rather than fixed-task allocation, organized according to four generic functions of "monitoring displays," generating various courses of action or "strategies to meet goals," deciding on a course of action, and then implementing the selected one. A year later, Parasuraman et al. proposed an extension of their previous work (Parasuraman et al. 1992), suggesting a similar model to Endsley and Kaber (1999) and adopting a "four-stage view of human information processing (Information acquisition, Information analysis, Decision and action selection, Action implementation)" where automation can be applied to each of these stages to different degrees and levels (Parasuraman et al. 2000).

By the beginning of the 21st century, the Department of Defense (DoD) was actively employing UAVs on different "dull, dirty, and dangerous" missions and had long-term innovative programs for deploying these UAVs in various areas. One of the focus areas, along with the development of several other technological requirements for the enhancement of UAVs' reliability and

survivability was autonomy (DC 2001). Within the next decade, ongoing research and goals of the Air Force Research Laboratory (AFRL) were to demonstrate the autonomous capability of level 8 out of 10 based on autonomous capability level (ACL) metrics (Clough 2002). The National Institute of Standards and Technology (NIST) realized the need for some standard definitions for autonomous levels based on system specifications and performance measurements. They assembled an ad hoc group for the generic framework development of unmanned systems' autonomy level specification called Autonomy Levels for Unmanned Systems (ALFUS) (Huang et al. 2003a). The results of their various workshops include:

—a complete list of terminologies and definitions (Huang 2004),
—a set of metrics for ALFUS detailed model identifying "mission complexity, environmental difficulty, and HRI" as the combination of factors indicating LoA (Huang et al. 2003b, 2004a, 2004b),
—an executive model showing general trends in the transitions of levels of aforementioned factors (Huang et al. 2005), and
—illustrating applications of ALFUS in military, homeland security, and manufacturing (Huang 2007).

Meanwhile, research communities were moving toward "adjustable autonomy" where the human user, autonomous system, or another system itself can adjust the LoA during the operation. After the comeback from a severe "AI winter" (Cognilytica 2018), AI created a boom in intelligent and smart systems such as smartphones, smart home appliances, and assisted technologies. In AI research domain, these intelligent autonomous systems are referred to as "agents." Research in the areas of adaptive and advanced interfaces facilitated the easy deployment and operations of adjustable autonomous agents providing multiple channels of communication between the human user and the system such as gestures, voice, and touch. Social acceptability, trust, reliability, mutual situation awareness, coordination of tasks among users and agents, and transfer of control strategies formed the elements of the new set of concerns for the researchers along with safety and robustness. Efforts were made to include these variables in the LoA framework (Beer et al. 2014).

In summary, industrial and academic research on robotics and automation started in the 1950s. However, the progress was slow for more than a decade due to the lack of proper understanding and implementation of autonomy; trained operators that had good situational awareness in case of failures; and resources such as high-computing processors, cameras, and sensors. Supervisory control advanced to adaptive and adjustable autonomy. A summary of various taxonomy for LoA that various researchers proposed over the years, listed in Table 2, shows the work done to overcome the challenges raised by design approaches of autonomous systems. Research advancement in the areas of AI and HMT also paved the way for more trust and social acceptance toward these systems.

3.2 Approaches of Autonomy

The challenges in an autonomous system are how to implement the LoA and who would have the control to adjust it and in what scenarios. It would fundamentally mean what, when, who, and how the necessary actions need to be taken. Various works have been done to recognize the balance between the flexibility of control over the autonomy levels such that HMT outperforms either the human or machine working alone. Comparative studies were also done to test the efficiency, robustness, and workload in various modes of an autonomy spectrum (Heger and Singh 2006; Heger et al. 2005). A systematic literature review on adjustable autonomy has been done (Mostafa

Table 2. Level of Automation (LoA) Frameworks Summary

Level	LoA (Sheridan and Verplank 1978)	LoA (Endsley and Kaber 1999)	ACL (AFRL) (Clough 2002)	ALFUS (NIST) (Huang et al. 2005)
1 Low/ Remote Control	No assistance from system/Humans decide	Manual Control	Remotely guided	— High-level HRI — Low-level tactical Behaviour — Simple environment
2	System offers set of decision alternatives	Action Support	Real-time Health/Diagnosis	
3	Narrows selection down to few	Batch Processing	Adapt to failure and flight conditions	
4	Suggests one alternative	Shared Control	Onboard route replan	— Mid-level HRI — Mid complexity, multi-functional missions — Moderate environment
5	Executes the suggestion if human approves	Decision Support	Group Coordination	
6	Allows human restricted time to veto before automatic execution	Blended Decision Making	Group tactical replan	
7	Executes automatically, informs human	Rigid System	Group tactical goals	— Low-level HRI — Collaborative, high complexity missions — Difficult environment
8	Informs human if asked	Automated Decision Making	Distributed control	
9	Informs human if the system decides to	Supervisory Control	Group Strategic goals	
10 High/ Fully Autonomous	System acts autonomously, ignores human	Full Automation	Fully autonomous swarms	— Approaching 0 HRI — High complexity — Extreme environment

et al. 2019) that listed approaches to autonomy. We have an updated list here with additional references and a comparative study of different approaches in Table 3.

3.2.1 Supervisory Control/Task-based Approach. The user acts as a system supervisor who monitors the activities of the system and has the privilege to modify the system behavior dynamically without taking over complete control of the system, which could be necessary to avoid task failure (Reed 2005). In this approach, both the user and the system may have individual subtasks to perform in the entire mission, and the system passes control when it is done with its subtask. For example, mission and payload management in a UAV requires monitoring of sensors and making knowledge-based decisions to meet overall mission requirements (Cummings et al. 2007). In these situations, the human power of judgment, experience, and intuition exceeds intelligence algorithms while the system is better controlling the navigation and motion controls (Cummings 2014).

3.2.2 System-Initiative Approach. Some research has been done in the area where the autonomous robotic team requests for help from the human operator. The system only passes control when it is stuck and no longer can perform its assigned task and needs human intervention to take further action. The efficiency of such type of adjustable autonomy depends on how rapidly and accurately the human operator responds to the situation while engaged in different unrelated tasks (Sellner et al. 2006). For example, Roomba vacuum cleaner can serve as an excellent example of

Table 3. Comparison of Different Approaches of Autonomy

Approach	Authority	Pros	Cons	Situation Awareness (SA)	Goal Achievement	Representative Work
Supervisory Control/Task-based Approach	User	Easier to model and implement	User role reduced to a monitor causing boredom. Recognizing and responding to cyberattacks difficult.	Low SA for new or inattentive monitor/user	User skill/expertise level dependant	(Reed 2005) (Cummings et al. 2007) (Cummings 2014)
System-Initiative Approach	System	Relatively easier to model and implement.	Wait for the user to take actions that need user authorization	User distracted with unrelated tasks.	User skill/expertise level and response time dependant	(Sellner et al. 2006) (Dias et al. 2008) (Cummings 2014)
Mixed-Initiative/ Teamwork-centered Approach	Decision-making is shared between the user and the system	Reaction time would be less	Difficult to realize a certain level of autonomy in terms of task assignment. Smooth transfer of control is a challenge	Depends on the interface, which would remind the user of the system's state, time-off period, and user's expertise	User's skill-level and the system should complement each other	(Clough 2002) (Wray et al. 2016) (Moffitt et al. 2006) (De Brun et al. 2008) (Hardin and Goodrich 2009)
Sliding Scale Approach	User's control inversely proportional to the system	Autonomy levels between the pre-programmed levels could be achieved. Increases robustness and adaptability	Swiftly attaining situational awareness is a challenge for the user	Depends on the autonomy level the system is working on and how engaged the user is with the system	Combines the forte of user and autonomy: each does what they are good at.	(Lin et al. 2012) (Desai and Yanco 2005) (Goodrich and Schultz 2007) (Desai 2007) (Dias et al. 2008)
Hierarchical Approach	User/Highest level in the hierarchical architecture determines objectives and control criteria	Easier to manage and coordinate multiple systems. When lower level systems are compromised, higher levels can disable them until issue resolution	Higher levels rely on lower level outputs. When a higher level is compromised, the whole system would be down.	Single operator, multiple autonomous systems would increase workload and hence decrease situation awareness.	Group Coordination is necessary for the completion of the task	(Wakulicz-Deja and Przybyła-Kasperek 2007) (Cummings et al. 2007) (Proscevicius et al. 2011)
Policy-based Approach	User/Policies	Increased trust in the system as the user can set bounds	Making policies for all situations is a challenge.	On a policy-by-policy basis.	Completion of task depends on the possible actions a system can take defined by the policy	(Bradshaw et al. 2004b) (De Brun et al. 2008) (Scerri et al. 2003) (Bradshaw et al. 2005)
Goal-driven Approach	User/Goals	More self-sufficient	High degree of difficulty. Hackers can manipulate the goal itself.	Shouldn't require human intervention	Goal-driven AI algorithms should be interactive with the environment	(Weber et al. 2012) (Klenk et al. 2013) (Wilson et al. 2016)
Collaborative Approach	Multiple individual systems	Multiple systems serve toward completing a higher goal	Collaborating multiple systems without human intervention is a challenge	Shouldn't require human intervention	Individual systems must complete their respective goals to achieve a higher goal	(Dufrene 2005) (Lacerda et al. 2018)

such a system that would need human intervention when stuck in a corner (Zilberstein 2010). In peer-to-peer human-robot teams, maintaining coordination and learning from "interactions at different levels of granularity" would increase the situational awareness of the team and, in turn, increase the overall productivity (Dias et al. 2008).

3.2.3 Mixed-Initiative/Teamwork-centered Approach. In this approach, the user and the system smoothly exchange controls throughout the mission. The idea of such a system where human and robots complement each other and collaborate in a safe, productive, and cost-efficient environment is not novel. The aim of NASA's Astronaut-Rover (ASRO) project, first tested in 1999 (Clough 2002), is to bring together human and planetary rovers to work together seamlessly, communicating throughout the mission and be a scout, technical field assistant, infrastructure assistant, and much more to the crew (Fong et al. 2001), with adjustable LoA during system operation (Dorais et al. 1999). In such systems, the back-and-forth transfer of control between the system and the human should be smooth and quick, along with the guarantee that each entity would be able to handle its part competently (Wray et al. 2016). This approach would be able to address several challenges, including maintaining consistent and stable operation, user trust, and situation awareness during the transfer of control at different LoA (De Brun et al. 2008; Moffitt et al. 2006). Research in the area of urban search and rescue missions utilizing mixed-initiative control autonomy shows that a robot was able to make better navigation decisions (Bruemmer et al. 2002). It holds for a large-scale team of robots as well indicating that theoretical benefits of this approach could be met if system and operators have complementary abilities in such a way that the systems must be able to make progress without waiting for human intervention (Hardin and Goodrich 2009).

3.2.4 Sliding Scale Approach. In sliding scale autonomy, the intermediate LoA between the discrete modes: teleoperation, safe, shared, and fully autonomous, can be achieved. It is more of a continuous mode of autonomy where the autonomy of the system increases with the proportional decrease of user's control on the system. It is achieved by blending human and system's desired characteristics or variables. The user can guide the actions/operations of the autonomous systems in different modes or dimensions, which provides authority and flexibility to the user in managing the autonomous systems (Desai and Yanco 2005; Lin et al. 2012). In these works, variables that characterize the systems are provided on a sliding scale, which would influence the autonomy levels. In Goodrich and Schultz (2007) and Desai (2007), the authors designed a trust scale to adjust the autonomy level (Dias et al. 2008). Another work implements sliding autonomy to develop a coordinated team of robots to dock both ends of a suspended beam in assembling of structures. These robots interact with a human operator in case they need help if stuck or to improve efficiency.

3.2.5 Hierarchical Approach. It is comparatively easy for two systems or a human and a machine to cooperate and coordinate. As the number of systems or agents increases, coordination and management conflicts arise between them. In this approach, systems are structured in a hierarchy through which a global problem can be solved based on the knowledge of lower level systems (Wakulicz-Deja and Przybyła-Kasperek 2007). It helps to localize specific tasks to systems based on goals, control, duration of execution, the complexity of tasks, and the amount of interaction or supervision needed by the operator, hence, defining the autonomy levels. A group of researchers proposed a "hierarchical control loop" architecture for single user-multiple UAVs as three loops ("Motion control inner loop," "navigation," and "mission management outer loop") (Cummings et al. 2007). Their case studies conclude that an operator can control an increased number of UAVs if the automation is increased in the "control and navigation loops" with good user-system collaborative decision making in the mission management loop. Similarly, Proscevicius et al. (2011)

suggests a five-level control hierarchy for autonomous mobile robots to speed up communications and control in the hierarchy levels.

3.2.6 Policy-based Approach. Policies are a set of guidelines defined by the designer that an autonomous system must abide by in any given situation. They are permissions given to the autonomous system for the adjustment of autonomy in changing operational environment without changing the code. Such an approach increases the trust of the user in the system as he/she can set bounds on the system based on his competency level. Moreover, a policy-based approach provides re-usability, efficiency, extensibility, context-sensitivity, verifiability, protection from malware, poorly-designed or buggy agents, and reasoning about agent's behavior (Bradshaw et al. 2004b). One such work based on policies is the driving mission for the human-robot team (De Brun et al. 2008) in which one of the policies could be "if the road is slippery, the human should drive." Another example is the Electric Elves, a multi-agent system acting as a personal assistant to a group of researchers for their daily activities such as ordering, scheduling meetings, selecting presenters in the research group, and organizing lunch meetings. This system is based on policies to the strategic transfer of control (Scerri et al. 2003). The Knowledgeable Agent-oriented System (KAoS) is an example of platform-independent policy services (Bradshaw et al. 2003) used in areas like modeling human-machine team, military, and space applications (Bradshaw et al. 2004a), which enable users to define policies of autonomous systems or agents that govern the autonomy and adjust them dynamically so that the system could adapt to the changing situation (Bradshaw et al. 2005).

3.2.7 Goal-driven Approach. It is a conceptual model to build an autonomous agent that observes a set of expectations during the execution of a plan, detects discrepancies if they occur, details the reasons of failures, and creates new goals to pursue if the execution of a current plan fails (Weber et al. 2012). It incorporates a model for goal reasoning and has been applied in various domains such as responding to unexpected events in strategy simulations (Klenk et al. 2013), StarCraft game for strategic planning, and so on. A group of researchers demonstrated this conceptual framework through Autonomous Response to Unexpected Events (ARTUE) in a navy training simulation—Tactical Action Officer (TAO) Sandbox—and showed that it could perform well in a complex dynamic environment (Molineaux et al. 2010). Preliminary works by Wilson et al. (2016) show that a goal-driven autonomous underwater vehicle can successfully detect a potentially hostile surface vehicle when pursuing a different goal of surveying a bay area.

3.2.8 Collaborative Approach. In collaborative autonomy, multiple individual agents, each having their own specific individual task to complete, collaborate to serve toward completing a higher collective goal. The multiple individual agents form a complex system whose autonomy is decided based on the autonomous actions of the collective individual agents depending on sharing information and goals (Dufrene 2005). A conceptual example of this approach could be seen in the system design for Mars exploration with a UAV and a ground vehicle in collaboration. The goal is that UAV would have the capability to dock to a charging station on the ground rover without human intervention. The ground rover would serve as a mobile-base that would provide charging, communication, and docking capabilities to the UAV (Lacerda et al. 2018).

3.3 Current Trends

In recent years, the research focus has moved to implement adjustable autonomy in the real world, and other more challenging areas such as transfer-of-control, goal reasoning, deliberation, and collaboration with multiple heterogeneous agents and individuals. Companies like Google and Nissan are predicted to launch their self-driving cars by 2020, while GM's Cruise and Waymo are not behind. Although cars like Tesla, Navya, and others have advanced autonomous features, there

are still significant challenges to make them completely driverless. Automated path and motion planning with efficient computational paradigm and a well-planned execution model would facilitate a smooth transfer of control between the user and the system. As discussed in Zilberstein (2010), to build robust autonomous systems, a human action model, a user's state monitoring, intent recognition techniques, and efficient interfaces to facilitate collaboration between the user and the system are required. These emerging fields of AI and HMT are gaining momentum and works are being done in facial and emotion recognition (Corneanu et al. 2016; Mehta et al. 2018) that would be helpful in monitoring a user's state while augmented reality devices, gesture, and voice user interface would facilitate easy communication.

Autonomous systems operating in the complex dynamic environment need to make informed decisions promptly to react safely and reliably in complex dynamic situations based on an accurate perception of its surrounding. More than one sensor is employed in these systems to assess the surrounding environment accurately. The fusion of data from multiple sensors and multiple modalities has become crucial in the perception process of autonomous systems in various application fields and can be used in image registration (Giering et al. 2015) along with the detection and mapping of static and dynamic obstacles along the trajectory (Korthals et al. 2018). A recent survey discusses the current developments in the areas of perception, planning, coordination, and control of autonomous systems (Pendleton et al. 2017).

The fast pace of research advancements in autonomous systems require that different aspects of these systems have a benchmark and a proper metric designated for each of them. It would not only set a standard for the development of an autonomous system with a certain degree of autonomy but would be helpful as well to recognize appropriate systems for particular scenarios that require a certain level of autonomy (Hrabia et al. 2015). Some earlier works were done to establish a common metric for autonomous systems by government agencies (Clough 2002; Huang et al. 2004b). In the field of HRI, common metrics for autonomous systems concerning five categories of "navigation, perception, management, manipulation, and social" have been presented in Steinfeld et al. (2006), while another work addresses the benchmarking of socially assistive robots on aspects of robot technology, social interaction, and assistive technology (Feil-Seifer et al. 2007). A review of these works is presented in Damacharla et al. (2018) to identify common metrics and set a benchmark in the field of HMT. Most recent works reviewed autonomy measures to compare and contrast autonomy approaches and discussed the capabilities of autonomous systems (Bihl et al. 2018).

4 CYBERSECURITY OF AUTONOMOUS SYSTEMS

Autonomous systems can be broadly seen as a type of cyber-physical systems that has embedded computers and physical elements connected and controlled by sophisticated software, exhibiting distinct behaviors through multiple means of communication with the outside world. Most of these systems are deployed in critical areas such as nuclear power plants, automatic pilot avionic, and war zones. Some of these systems are highly vulnerable to cyberattacks; hence, the security of these systems poses significant concerns if they are entrusted with our lives. Complete failure of these systems through cyberattacks, failure to correctly respond to critical missions, or even a slight change in the desired output data can leave the operator in a confused or ignorant state. Some research work has been done on the comprehensive review of threats, vulnerabilities, attacks, and control on cyber-physical systems (Abdul-Ghani et al. 2018; Alguliyev et al. 2018; Ding et al. 2018; Huang et al. 2003a; Lin et al. 2016; Wu et al. 2016). Extrapolated from these works, we present a taxonomy of common attacks on autonomous systems in Figure 2 and a brief description of some of these attacks and their effects in Table 4. A comprehensive list of cyberattacks and its detailed survey on autonomous systems is beyond the scope of the article. In this section, we discuss some of the highly researched autonomous systems (Figure 3) and work done on their cybersecurity.

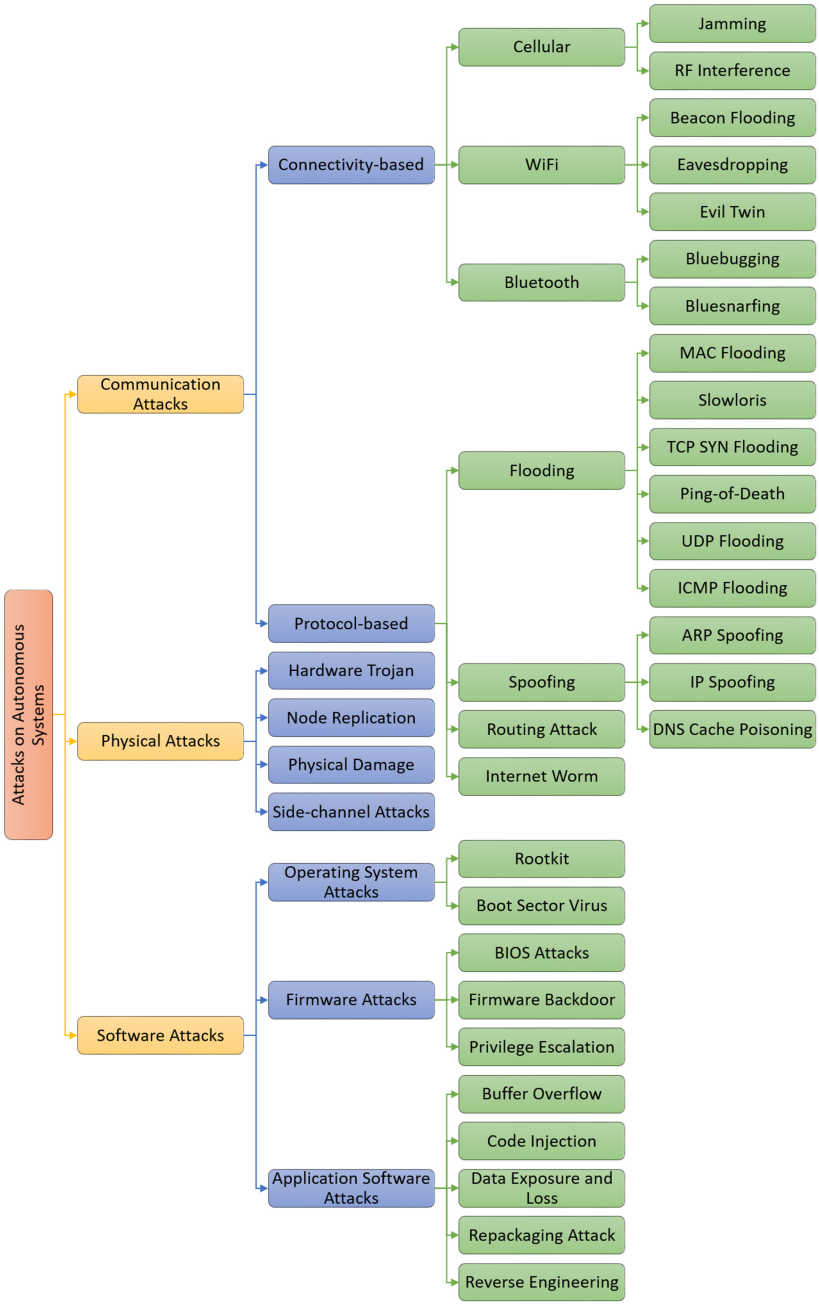

Fig. 2. Taxonomy of attacks on autonomous systems.

4.1 UXVs

The increasing popularity of unmanned systems (UAVs, Unmanned Ground Vehicles (UGVs), Unmanned Underwater Vehicles (UUVs)) in various mission-critical tasks have forced the researchers to work on their autonomy-level related to task complexity, human interaction, environmental difficulty, and so forth (Behzadan 2017; Goodrich and Schultz 2007; Huang 2007). Commercialization

Table 4. Effects of Cyberattacks on Autonomous Systems

Attack Types	Description	Effects on Autonomous Systems	Works
Jamming	Caused by intentional interference, e.g., GPS Jamming	Loss or corruption of packets disrupting communication	(Bhattacharya and Basar 2010; Javaid et al. 2015)
Spoofing	Masquerading as a legitimate source, e.g., GPS Spoofing	Gain access to the system, information, etc.	(Humphrey 2012; Javaid et al. 2017; Petit et al. 2015)
Flooding	Flooding of packets thereby overloading the host, e.g., DoS, DDoS	Loss of communication through network congestion	(Javaid et al. 2015; Vasconcelos et al. 2016)
Side-channel Attack	Attack based on the extra information gained by the physical analysis	Leakage of sensitive information without exploiting any flaw or weakness in the components	(Akram et al. 2016; Cornelius et al. 2017)
Stealthy Deception Attack	Tampering system component or data	Mislead the system to take undesirable action	(Kwon et al. 2013)
Sensor input spoofing	Manipulate environment to form implicit control channel	Exercise direct control over system's actions	(Davidson et al. 2016)

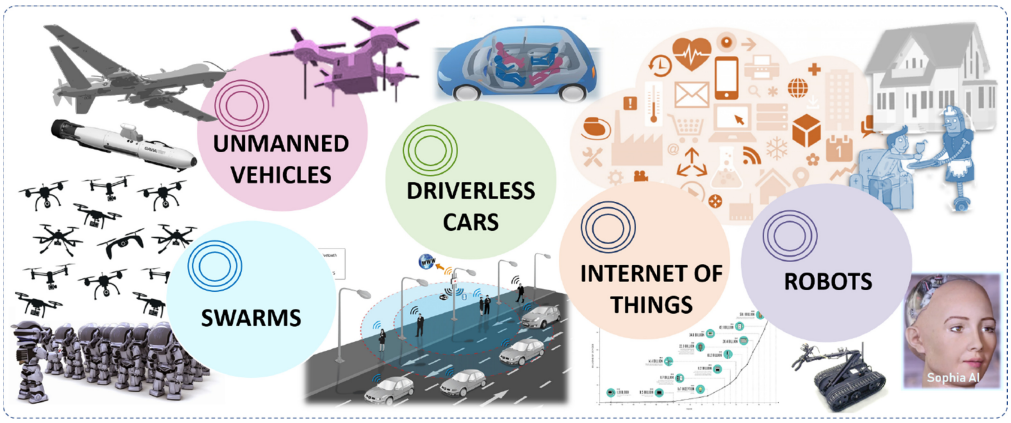

Fig. 3. Autonomous systems.

of UAVs, a.k.a drones, is gaining momentum as multiple industries are planning to use them for their business functions. Door-to-door delivery and hauling cargos as far as 300 miles with a weight of up to 200 pounds is not a distant dream. Industries like Bell Labs are working on prototypes that can use gas or electric power and convert to a plane during mid-flight, addressing some aerodynamic concerns (Joe Pappalardo 2018). These systems are at a higher risk of becoming targets of cyberattacks. One of the earliest works to identify vulnerabilities in a UAV auto-pilot system was done in Kim et al. (2012). A group of researchers analyzed system safety (Kwon et al. 2013) and developed a real-time safety assessment algorithm (Kwon et al. 2016) to investigate the performance of such systems against stealthy deception attacks.

A review of all recent major attacks on UAVs has been presented in Krishna and Murphy (2017). Global Positioning System (GPS) Jamming and Spoofing are the two most common attacks on UAVs' navigation. GPS jamming is a type of interference that specifically restricts GPS signals. In

Table 5. Driverless Car Technology Trend

Proposed	Launch	Manufacturer	Pilot Project	Features	Works
2005	2021	Ford	–	Level 4 Automation, no gas pedal, no steering wheel	(Chad Vander Veen 2015)
2009	2020	Google	Waymo	Fully self-driving, no steering wheel, no accelerator and brake pedal	(Chad Vander Veen 2015)
2014	2015	Tesla	Model S	Autopilot, 360 degree view, real-time traffic updates, automatic parking	(Fred Lambert 2018)
2014	2025	Mercedes-Benz	Future Truck 2025	Autonomous Driving	(Chad Vander Veen 2015)
2015	2021	Volvo	Drive Me	Level 4 Automation, IntelliSafe Auto Pilot lets user activate and deactivate autonomous mode	(Tom Huddleston Jr. 2018)
2015	2020	Nissan	ProPILOT	Automatic lane change on highways, autonomous driving on urban roads and intersections	(Chad Vander Veen 2015)
2016	2019	General Motors	Super Cruise	Hands-Off lane following, brake, and speed control	(Joe Williams 2018)
2014	2016	Induct Technology	Navya	Autonomous shuttle, deployed in specific loops, closed environment, and half-mile radius	(Navya 2018)
2016	2018	Drive.ai	–	Autonomous driving, remote monitoring, LED screens display car's next action to pedestrian	(Alex Davies 2018)
2016	2021	BMW-Intel-Mobileye	BMW iNEXT	Develop open standard platform for highly and fully automated driving	(Sarah Sloat 2016)

a GPS spoofing attack, a false GPS signal is transmitted to the GPS receiver of the autonomous system to introduce an unnoticeable error in the position, navigation, and time (PNT) calculation, which results in the deviation of the system from its original path toward a malicious destination. US Maritime Administration reported a recent incident of GPS spoofing where around 20 ships off the Russian port of Novorossiysk found themselves in the wrong spot—more than 32 kilometers inland, at Gelendzhik Airport (Hambling 2017). While the military GPS signals are encrypted, civilian GPS signals are publicly known. Hence, the GPS spoofing attack poses a significant threat to critical infrastructure and public lives in case spoofed systems are used maliciously. Some researchers have tried to demonstrate these attacks on a small, but sophisticated UAV (Humphrey 2012). Other researchers have simulated those attacks on academic testbeds (Jahan et al. 2015; Javaid et al. 2017, 2015).

4.2 Driverless Cars

Major car manufacturing companies like Google, Audi, BMW, Ford, GM, and Uber have envisioned a future of autonomous vehicles on the road. Table 5 lists some of the major autonomous car

manufacturers and their pilot projects. By the end of 2018, Waymo tested about 5 million miles nationwide while Cruise racked up second (David Welch, Keith Naughton 2019). The year 2019 may be the year of the driverless car as GM prepares to launch its fleet (Joe Williams 2018) while Waymo is already on the streets of Phoenix, Arizona opening initially to early-riders (Matthew DeBord 2018). Another startup, Drive.ai, launched its self-driving shuttle service around a geo-fenced area of Frisco, Texas (Alex Davies 2018). In the effort of envisioning a "smart city," Lake Nona, Florida would soon see AUTONOM, a self-driving bus deployed by Beep in partnership with the French company Navya (Joey Roulette 2019). Companies like Nissan are planning to put driverless cars on the streets of Tokyo by 2020 (Greenberg 2015). Today, many new cars already incorporate state-of-the-art driver-assistance features such as autopilot, self-parking, and summoning, blind spot, and lane-monitoring systems. Future autonomous vehicles need to be connected through sophisticated vehicular networks such as the Vehicular Ad hoc Network (VANET) so that they may exchange traffic and routine information such as speed, location, or notification of any traffic collision. It increases the potential for cyberattacks. In 2015, Wired documented a hacking experiment on Jeep Cherokee where an intruder took the car control from the driver on the highway. In the beginning, the hackers toyed with air conditioning, radio, and windshield wipers. It became scary for the driver when the accelerator stopped working on the long overpass with no shoulder to escape. It would have been a lot worse if the intruder had abruptly engaged the brakes or disabled them all together (Mejri et al. 2014).

The communication over VANET would help the vehicles to plan for better driving decisions and performance. However, a significant amount of confidential data would also be circulating on the network. A simple attack such as eavesdropping on a user's habit of commuting can reveal a lot of valuable information about the user to the attackers. Also, the next-level of cyberattacks such as ransomware attack could be executed in the middle of the commute. A secured network would throttle all the possible attacks at the point of entry. Many researchers have reviewed the contribution of others in this area by identifying and classifying the vulnerabilities and security challenges in VANETs (Al-Kahtani 2012; Azees et al. 2016; Bariah et al. 2015; Dhamgaye and Chavhan 2013; Elsadig and Fadlalla 2016; Gillani et al. 2013; La Vinh and Cavalli 2014; Mejri et al. 2014; Saini et al. 2015; Sumra et al. 2011). As these vehicles will communicate with nearby devices and infrastructure, it is important to explore the architecture and main characteristics of these systems, and analyze the corresponding countermeasures against the possible attacks (Hamida et al. 2015; Mejri and Hamdi 2015). Authenticating vehicles entering into VANET through dual authentication methods or highly secure mechanisms should be the first line of defense (Vijayakumar et al. 2015). Authors have dedicated their research to individual attack detection such as DoS (Lyamin et al. 2014; Mejri and Ben-Othman 2014a), jamming (Hamieh et al. 2009; Puñal et al. 2012), and greedy behavior (Mejri and Ben-Othman 2014b). Sending false congestion messages to the vehicles by exploiting congestion avoidance mechanisms (Bauza et al. 2010; Fontanelli et al. 2010) in VANET would be an easy way for attackers to re-route and position them in zones of interest (Garip et al. 2015).

4.3 Robotics

Robots are marking their place in our lives with the significant investments in robotics technology (Waters and Bradshaw 2016), advancement in cutting-edge technologies like 5G, Augmented Reality (AR), IoT (Fearn 2018), reduced cost of electronic devices, and people's need for assistance in mundane activities. Being an evolutionary industry, they are designed based on the environment they would be deployed in and work side-by-side with humans. Their reach varies from space to manufacturing, from home to war front. Surgical or industrial robots need to have an extremely high level of accuracy while rescue robots should be fast and efficient in locating survivors in

inaccessible areas. Home-assistive robots such as Care-O-Bot should be able to help in household tasks, be a mobility aid for the elderly and needy, and a medium for communication and social integration (Hans et al. 2002).

Several cybersecurity issues and vulnerabilities identified by researchers pose serious threats that can be easily exploited by malicious users. Industrial and academic researchers have demonstrated attacks on industrial robots that can be hacked and manipulated to introduce a few millimeters of a defect in a manufactured product, which could result in a catastrophic failure of that system (Quarta et al. 2017). They analyzed the standard architecture of an industry robot from a security point-of-view and developed an attack model based on the attacker's goal, an access level to the system, and their capabilities (Maggi et al. 2017). An independent security firm took the initiative to evaluate currently available robots in the market from different vendors. Their initial search report reflects several cybersecurity vulnerabilities in robot technology (Cerrudo and Apa 2017). Although some of these vulnerabilities are common cybersecurity problems, vendors should implement and address them from the very first phase of the software development process.

Surgical robots are the new trends in the medical industry, even in third world countries such as India, which reported 26 da Vinci systems in 2015 (Ians 2015). These robotic surgeries result in small incisions, minimal loss of blood, and faster recovery of patients with less post-operative pain. These robots work very closely with humans. It is essential to ensure the security and safety of robots that operate around people and animals in home and organizations alike. Various attacks were reported that compromised a potential entry point to get into the hospital network in the last few years (Snell 2015; Zetter 2014). Network vulnerabilities could easily be exploited to access surgical systems, bypassing intrusion detection systems and firewalls (Alemzadeh et al. 2016).

The same goes for household robots on a home network as well. Since such types of robots are near children and adults in the house, it is more likely that an onboard camera can be exploited to capture inappropriate audio/video streams (Denning et al. 2009) by pedophiles and online sexual offenders (Yong et al. 2011). Besides privacy issues, the home robot's sensors can be used to collect sensitive data that can be used to launch different types of cyber or physical environment attacks. For example, a home robot acting as a scheduler would know when the owners would be away from home, and a planned burglary could be attempted or a family member could be physically harmed in the worst-case scenario. A group of researchers investigated possible attacks on these service robots, analyzed the threat, and listed different available defense mechanisms against such attacks (Cornelius et al. 2017).

4.4 Internet of Autonomous Things (IoAT)/Autonomous Internet of Things (AIoT)

There are two future concepts that are more or less intertwined in researchers' opinions. One is the Internet of Autonomous Things (IoAT) where smart autonomous devices would be connected through the network and would be able to solve the problems or adapt themselves through information exchange with peers. The other concept is an AIoT connecting smart devices that would "actively manage data and decisions on behalf of users" (University of Nottingham-Mixed Reality Laboratory 2016). These two concepts overlap each other in the sense that smart devices would have some autonomous decision-making and would be connected through a network. The future is not so far away from where IoT devices will be information generators, and the edge devices will be consumers with cloud-based control. The statistics generated by Statista shown in Figure 4 predicts that the number of connected devices would be 75 billion by 2025 (Statista 2018). Most of these devices would be autonomous (or semi-autonomous). In Engineering (2016), Tom Keeley discussed the market of IoAT and how they will be able to solve newer problems through self-organization and team operation. Markets like personal security, home automation, and healthcare will lead the way with IoAT. Intelligent actuators will be the tools, arms, and hands for IoAT devices.

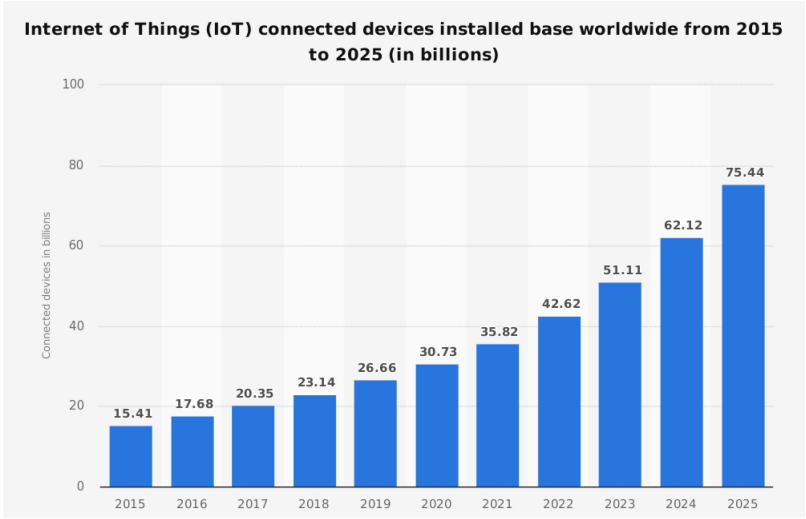

Fig. 4. Statistics of the number of devices connected worldwide from 2015 to 2025 (in billions) published in Statista, 2016 (Statista 2018). Note: Data is a forecast from 2017–2025.

As big data, machine learning, and Blockchain technologies advance alongside the innovation of IoT devices, it would be sooner than expected that these devices would achieve autonomy at the level of human actors (Industry 2017). Future IoT infrastructures should be able to support heterogeneous platforms, locations, and environments. For smart and reliable autonomous IoT infrastructures, it should be easily scalable via decentralized management mechanisms and self-adapting to the changes in the environmental context (Kyriazis and Varvarigou 2013). Moreover, it should support confidentiality and prevent personal information infringement, allowing the users to keep their confidential data "in-house." For example, an AIoT would range from the smart pantry for automatic inventory tracking or washing machines that would order detergent once the supply is about to finish (University of Nottingham-Mixed Reality Laboratory 2016). Again, since this area itself calls for further research, cybersecurity and privacy of data should be one of the primary goals in the architectural design of such a network. For sure, a list of cyberattacks that could be performed on IoT devices (Abdul-Ghani et al. 2018) would be applicable on AIoT devices as well.

4.5 Swarms

An emerging area of research is swarm robotics. It is directly inspired by nature where, for example, a swarm of insects or a flock of birds perform tasks beyond individual capabilities. It has found applications in varied areas (Sahin 2005) such as detecting lives in disaster rescue missions, an inspection of industrial machinery (Correll and Martinoli 2009), mapping agricultural fields (Albani et al. 2017), and monitoring for undesired environmental events. Swarm robotics is much researched for military applications as well. Since individual entities that make the swarm are dispensable and redundant, they can be applied in mining or places dangerous/inaccessible to humans. Also, swarms of robots can complete a particular task faster than an individual robot as they are self-organized and work in parallel with a distributed command and control structure of communication.

Currently, researchers mainly focus on modeling methods and algorithms of swarm robotics of flocking, foraging (Winfield and T. 2010), navigating, and searching applications (Haque et al. 2018; Tan, Ying and Zheng 2013). The papers of Higgins et al. (2009) and Sharma and Bagla (2009) are

early works on considering security challenges in swarm robotics and analyzing possible threats to the swarms. They also compare the specific characteristics of the swarms with other similar systems such as multi-robots, multi-agent systems, mobile sensor networks, and Mobile Ad hoc Network (MANET). This area of research is still raw, and not much work has been done related to individual attacks on the swarm robotic network.

5 MODELING SYSTEM, VULNERABILITIES, THREATS, AND ATTACKS

It is of utmost importance to have a clear picture of what an autonomous system can do, when it needs to send an alarm signal to the user, when it must transfer the control altogether, or when it is under attack. At the same time, the operator should also be aware of the cues the system is sending. Researchers have tried to model different aspects of the system using different techniques. From a security point of view, it is essential to analyze the system model to find the vulnerabilities and threats to each part of the system, which can be further utilized to create an attack model. These areas have been studied, and various theoretical and analytical models have been proposed. We have tried to capture these works concerning UAVs, robots, and driverless cars as these autonomous systems are widely being researched and incorporated into the real world.

5.1 System Modeling

System modeling describes an abstract view of a system, ignoring its details. It can be used to illustrate the functions, behavior, or architecture of the system without going into other details. It reflects how the system reacts at certain events or how it communicates with sub-parts and its environment.

5.1.1 Theoretical Model.

- **UAVs**: Significant parts of a UAV architecture, which make up the guidance, navigation, and control systems, have been described in Kim et al. (2012). Modeling a UAV from the communication network perspective has been discussed in Javaid et al. (2012), detailing communication among various modules. The model described in the paper has six modules starting from the data acquisition module, which collects data from the sensors and sends the required information to respective modules such as altitude data to the Altitude and Heading Reference System (AHRS) module, and camera data to the telemetry module. The navigation module provides PNT information while the control module sends speed and orientation control signals to actuators of the system. These systems also have a data logging module that logs flight details such as PNT data to keep track of the missions and for further analysis in case of failure. Another work proposed a hierarchical model for coordinated control of multiple UAVs and used differential game theory for collision avoidance and formation control as a pursuit-evasive game (Vachtsevanos and Reimann 2004).
- **Autonomous Vehicles**: DARPA Urban Challenge accelerated the research for full-sized autonomous vehicles. A team from MIT was one of them who completed the race. They discussed their autonomous vehicle architecture in Leonard et al. (2008) where the requirement was to perceive and navigate a road network segment in a GPS-denied and highly dynamic environment. Another team designed the autonomous vehicle based on the "Sense-Plan-Act" model of an autonomous system (Urmson et al. 2007). Based on these works, Guo et al. modeled a mobile robot system that consists of a robotic platform and a planner to detect sensor and actuator attacks. Sensors are the eyes and ears of an autonomous system to the outside world while actuators can be compared to the limbs that execute control commands transmitted by the sensors (Guo et al. 2017).

— **Robots**: Gage (1985) was the first work to present a generic model of an autonomous robot related to security modeling. Recently, some industrial researchers presented the architecture of an industrial robot for security and threat modeling. In this architecture, a programmer communicates with the robot controller over the network, which, in turn, sends the command signals to the sensors and actuators of the robot to accomplish the assigned task (Maggi et al. 2017).

5.1.2 Analytical Model. Each autonomous system has some unique system dynamics, and a generalized study of such systems could be limited to standard parts. Goppert et al. (2012) modeled the dynamics of a UAV system using JSBSim and Scios for the control, guidance, and navigation system of the UAV, which was used to simulate the response of the UAVs to several identified cyberattacks such as a fuzzing attack and digital update rate attack, where an increased sampling rate would make the system unstable. Some of the works describe a UAV as a linear transitional time-invariant dynamic system with zero-mean Gaussian white noise and a constant co-variance matrix (Kwon et al. 2016; Su et al. 2016). Authors have also used game theory to describe the kinematic model of a UAV using variables to express the 3-D coordinate frame (Bhattacharya and Basar 2010). Guo et al. (2017) modeled a mobile robot as a nonlinear discrete-time dynamic system where the robot states evolve from x_{k-1} to x_k after the robot actuators execute the command generated by the planner.

5.2 Threat Modeling

Threat modeling is a process of identifying and understanding the threats to a system and then defining countermeasures to mitigate the threats. Not only does it helps to visualize the system model through potential adversaries' eyes, but it also helps to evaluate security risks and countermeasures in the case of possible attacks (Oladimeji et al. 2006). Envisioning potential threats is a daunting task. Modeling strategies like STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) can help to analyze the data flow through the system (Madan et al. 2016). Another threat modeling approach is Persona Non-Grata that focuses on attackers, their motivations, and abilities (Shull 2016).

Analyzing each part of the system for a different aspect of security by following the CIA model (Confidentiality, Integrity, Availability) lays the foundation for researchers to identify certain attacks (Javaid et al. 2012). As technology advances, so do the attackers' strategies and attack vectors (Tomas Foltyn 2018). Based on the vulnerabilities of the UAV's auto-pilot, threats in different components and the effect on the proper functioning of the UAV were analyzed in Kim et al. (2012). These were preliminary works in this field that lacked identification of hardware vulnerabilities or insider threats to the system. Another group of researchers developed a threat model for smart device ground control station (a portable hand-held ground control stations for UAVs) that allows soldiers to pilot UAVs in the battlefield. The key components addressed in the model are attack motivation, vulnerabilities in these systems, cybersecurity threats, and mitigation steps in case of attacks on these devices (Mansfield et al. 2013). They presented a risk analysis summary of threats and their impact based on hardware, software, communication network, and human errors. Similar discussion based on policies to defend against CIA threats in the context of unmanned autonomous systems has been done in Madan et al. (2016) along with threat modeling and risk analysis using the STRIDE approach. Some software products like Microsoft Threat Modeling Tool and ThreatModeler automate threat modeling, with the latter offering more sophisticated features (Beyst 2016).

The study of cybersecurity issues in robotics is also gaining pace in academia and industries. Most preliminary work in the identification of direct and indirect threats to robotic systems could

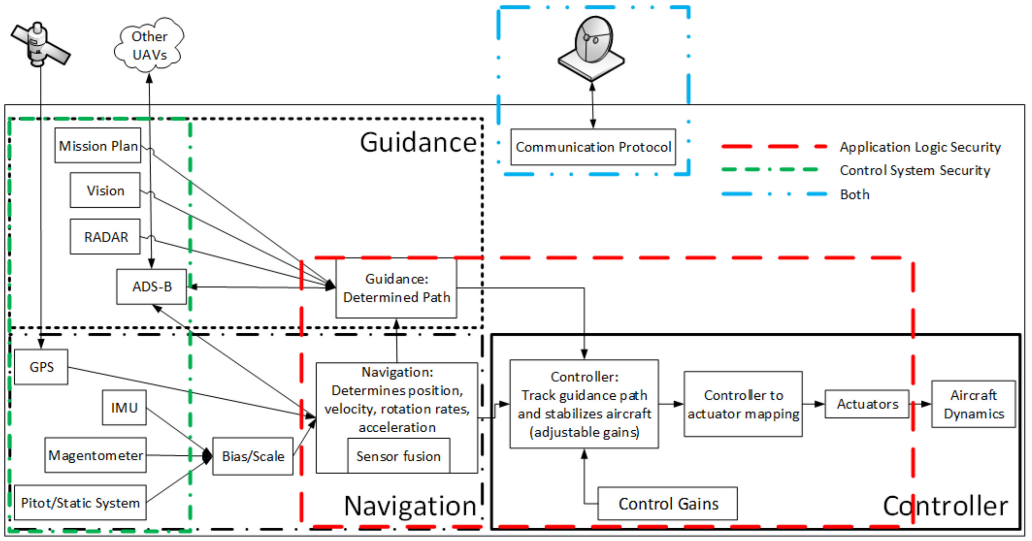

Fig. 5. Vulnerabilities of an autopilot system reproduced from Kim et al. (2012).

be found in Gage (1985). Gage discussed direct threats on the sensor, actuator, communication network, and processing elements along with some derived threats. Cornelius et al. (2017) identified four threat vectors in a mobile service robot: attacks on sensor data, hardware attacks, software attacks, and attacks on infrastructure. While Clark et al. (2017) discusses cyber threats to robots at "hardware, firmware/OS, and application levels," Lera et al. (2017) models cybersecurity threats, risks, and safety issues of using robots. They grouped the threats based on the origin of attack (natural, accidental, or intentional), the target (physical, cyber, or both), the impact on robot and external entities, and the risk associated with them. Threat scenarios based on the vulnerabilities found in the security analysis of an industrial robot have been discussed in Maggi et al. (2017). An attacker could alter the production outcome, introduce defects in the products, cause physical damage to the robot, or cause harm to coworkers. They can also be used as an entry point to extract company sensitive data or hacked to perform ransomware attacks.

5.3 Vulnerability Modeling

Kim et al. (2012) identified control system security and application logic security as the two vulnerabilities of an autopilot system in UAVs and categorized the identified threats under them, as shown in Figure 5. In control system vulnerability, the attackers exploit the vulnerabilities in the hardware or software programs such as buffer overflow attack and malware installation. Attacks in which manipulated input data are fed into the control systems exploit the application logic vulnerability such as GPS spoofing and automatic dependent surveillance-broadcast (ADS-B) attack. The mode of communication among UAVs or with ground control station is over wireless communication networks. It widens the grounds for cyber-physical attacks ranging from the disruption of communication links to the capture and use of one of the UAVs as an adversary. In Behzadan (2017), the author emphasized on the vulnerabilities of different layers (physical layer, link layer, network layer) of a communication network of UAVs. Krishna and Murphy (2017) reviewed the cyber vulnerabilities of UAVs based on recent real and simulated attacks.

There are more than 100 built-in or installed Electronic Control Units (ECUs) within a modern car, listed in Koscher et al. (2010), to control and regulate various functions of the vehicle.

These ECUs are connected through an in-vehicular network of sensors, processors, control systems, and communication applications along with a wireless gateway for external communications with other vehicles and infrastructure. Each system in the automated vehicle has some vulnerabilities. A group of researchers extensively reviewed the vulnerabilities in an autonomous vehicle. They highlighted the vulnerabilities based on sensors and control modules, behavioral and privacy aspects of humans, and connection infrastructure (Parkinson et al. 2017). An independent security firm evaluated the robots, currently available in the market from different vendors, to show how insecure robot technology is and reported nearly 50 cybersecurity vulnerabilities (Cerrudo and Apa 2017). Maggi et al. (2017) were able to identify several weaknesses of an industrial robot. Lack of mandatory user authentication, unsecured network, and naive cryptography are some of the vulnerabilities identified in the computer interface used to interact with the robot. An attacker could easily bypass or disable user authentication, tamper existing accounts, or exploit buffer overflow memory error.

5.4 Attack Modeling

With the increase in cyberattacks, it has become the need of the hour for government, organizations, and researchers to be ready with planning so that future attacks can be handled rapidly and efficiently. Attack modeling helps to realize the attacks before they happen and prepare the organization with mitigation steps that need to be taken if an attack happens. There are various attack modeling techniques to analyze the cyberattacks such as the attack graph or tree, the diamond model, attack vectors, and attack surfaces (Al-Mohannadi et al. 2016).

5.4.1 Theoretical Model. Guo et al. (2017) gave the attacker model for a mobile robot where the attacker can launch actuator or sensor attacks. Potential cyberattacks on automated vehicles have been discussed in Petit and Shladover (2015) in which the authors have identified attack surfaces and the possible attacks on automated and connected vehicles. They extend their research by performing real and effective blinding, jamming, relaying, and spoofing attacks on the camera and LiDAR sensors of automated vehicles (Petit et al. 2015). One of the works in this area classifies cyberattacks as passive and active attacks. A passive attack is to extract information from the system without affecting the system resources, like eavesdropping. An active attack objective is to harm the system in some ways like the DoS attack that compromises the availability of communication channel (Yağdereli et al. 2015). A taxonomy of attacks on autonomous vehicles has been presented in Thing and Wu (2016), which categorized the study based on attacker, attack vector, target, motive, and potential consequences. This taxonomy was modified to reflect attack taxonomy of a UAV in Krishna and Murphy (2017) with minor modifications such as the addition of a new subcategory of "communication stream" and listing references of actual instances of attacks.

As stated earlier, robots have already entered our lives and are making a place around humans. These robots assist us in our daily lives, including medical services in hospitals, battlefields or emergency response, factories, and homes. Lives could be put in danger if such robots are attacked. Various works have been done to analyze the possible cybersecurity attacks against them. In Bonaci et al. (2015), authors presented an attacker model of a teleoperated surgical robot. They identified possible attacks and classified them as intention modification, intention manipulation, and hijacking attacks. Robots are connected to a network through an interface used for operator interaction such as joystick or I/O diagnostic ports. An attacker model of an industrial robot discussed in Maggi et al. (2017) profiles an attacker based on access level, technical capabilities, access to equipment, an attacker's budget, and the type of attacks that could be performed.

5.4.2 Analytical Model. A kinematic model for sensor and actuator attacks has been presented in Guo et al. (2017) where sensor attacks result in wrong sensor readings that might generate

erroneous control commands, and actuator attacks could directly alter the control commands. Kwon et al. (2013) modeled the stealthy deception attack and analyzed the security of a cyber-physical system in case of a deception attack on sensors, actuators, or both, which causes an unbound estimation error without being detected by the monitoring system using a steady-state Kalman Filter. They extended their work to model a direct control acquisition attack and onboard navigation attack, which includes individual as well as combined stealthy deception attacks on Inertial Measurement Unit (IMU) and GPS. They further proposed a real-time safety assessment algorithm to verify the safety of the UAV subject to cyberattacks based on reachability analysis (Kwon et al. 2016). Su et al. (2016) define the UAV model under a GPS spoofing attack where falsified data could be injected into the navigation component either through a GPS signal simulator or by injecting a data level GPS spoofing attack in a hacked onboard navigation system. They formulated a real-time manipulation method for the UAV under the GPS spoofing attack to drive the UAV toward a malicious destination without triggering the fault detector, and computed the attainable location set of the UAV under such attacks.

Decision-making theories have also been used by many researchers to model attack strategies as games (Bhattacharya and Basar 2010; Merrick et al. 2016; Sanjab et al. 2017; Sourabh Bhattacharya and Tamer Basar 2012). Bhattacharya and Basar (2010) analyzed the coordination of multiple UAVs in case of a jamming attack on the communication channel by an aerial jammer and modeled this scenario as a zero-sum pursuit-evasive game. A zero-sum network interdiction game between a vendor of a delivery drone and attacker was modeled using the prospect theory (Sanjab et al. 2017). Here, the attacker's objective was to prevent the goods delivery drone from taking the optimal path from the warehouse to the customer's location chosen by the vendor.

6 DISCUSSION

The technological world is progressing from smart gadgets to smart homes, smart vehicles, and smart cities. There have been some real-world attacks exploiting the vulnerabilities of the current cyber-physical systems and network. With the advancement in technologies toward autonomous systems, the rate of attacks is bound to increase. It has become more important than ever before that the security challenges and concerns related to autonomous systems are addressed in the development phase itself.

In this article, we started with a glimpse into the historical evolution of autonomy and the progressive work done in this broad field. An idea of the background behind complex topics always clears the questions of how and when for new researchers, and gives a comprehensive understanding of the subject. The different approaches to implement autonomy in intelligent systems could be a good start to thinking about how the system's autonomy is going to work. A supervisory approach can very well be used for robots that would need supervision at some point through the task completion process. A goal-driven autonomy could be applied to driverless cars. Depending upon the traffic situation or roadblocks, it could alter its route to the destination. It could decide to pick up a fellow rider in a "Share-a-Ride" business model while on its way to drop off its customer and update its goal. The mixed-initiative approach is also one of the better approaches toward autonomy in a semi-autonomous car. The smooth transfer of control between the vehicle and the driver is a challenge and a topic of further research where each can take control if one feels that other is not in a situation to make a better decision. For example, if the driver is sleepy or in a drunken state, the car can take control of the driving. In a weather condition like heavy rain or a blizzard, it would be difficult to rely on optical sensors. In such a scenario, the car will not be in a good state to be driven autonomously, and the driver should take control of the vehicle to avoid mishaps. In the same scenario, an autonomous vehicle with sliding scale autonomy would lower its autonomy and give more control to the user, and as the weather clears, it could take back

Table 6. List of System, Vulnerabilities, Threat, and Attack Modeling Studies

Representative Works	Modeling				Description
UAV					
Vachtsevanos and Reimann (2004)	■				Presented hierarchical model control for multiple UAVs, game theory based pursuit-evasive game for collision avoidance and formation control
Bhattacharya and Basar (2010)	■			■	Kinematic model of a UAV using game theory in 3-D frame, attack strategies as zero-sum game
Kim et al. (2012)	■	■	■		Discussed architecture and vulnerabilities of UAV autopilot system
Javaid et al. (2012)	■		■		UAV Communication Network Threat assessment
Goppert et al. (2012)	■				Dynamics of UAV system—Control guidance and navigation
Kwon et al. (2013)				■	Modeled the attack and analyzed the security of the system in case of deception attack on sensors, actuators, or both
Mansfield et al. (2013)		■	■		Attack motivation, system vulnerabilities, threats, and mitigation steps
Yağdereli et al. (2015)				■	Classifies cyberattacks as passive attacks and active attacks.
Kwon et al. (2016)	■			■	Analytical safety-assessment algorithm for unmanned aircraft during stealthy cyberattacks
Su et al. (2016)	■			■	Defined the UAV model under GPS spoofing attack, formulated a real-time manipulation method and computed the attainable location set of the UAV under such attacks.
Madan et al. (2016)			■		Analyzed CIA threats of UXVs and risk assessment using STRIDE
Sanjab et al. (2017)				■	Modeled zero-sum game between a delivery drone vendor and attacker
Krishna and Murphy (2017)		■		■	Presented attack taxonomy of a UAV
Autonomous Vehicle					
Urmson et al. (2007)	■				Autonomous vehicle design based on "Sense-Plan-Act"
Leonard et al. (2008)	■				Autonomous vehicle architecture
Petit and Shladover (2015)				■	Attack Surfaces and potential cyberattacks on "autonomous automated vehicle" and "Cooperative automated vehicle"
Thing and Wu (2016)				■	Presented attack taxonomy of autonomous vehicles
Parkinson et al. (2017)		■			Highlighted vulnerabilities based on sensors and control modules, behavioral and privacy aspects of humans, and connection infrastructure
Robot					
Gage (1985)	■		■		Presented generic robot model, identified direct/indirect threats
Bonaci et al. (2015)				■	Presented teleoperated surgical robots' attacker model, possible attacks as intention modification, manipulation, and hijacking attacks
Guo et al. (2017)	■			■	Presented mobile robot's design, sensor, and actuator attacker model
Cerrudo and Apa (2017)		■			Identified Cybersecurity vulnerabilities
Cornelius et al. (2017)			■		Identified possible attacks, threat vectors, and defense mechanisms
Clark et al. (2017)			■		Discusses cyber threats at hardware, firmware/OS, and application levels
Lera et al. (2017)			■		Models cybersecurity threats, risks, and safety issues
Maggi et al. (2017)	■	■	■	■	Discussed industrial robot architecture, vulnerabilities, threats, and attacks

■ System Modeling ■ Vulnerability Modeling
■ Threat Modeling ■ Attack Modeling

the full control of the vehicle. We explored some of the trending areas in the development and enhancement of autonomous systems in the "current trends" section as well.

Our next discussion was on cybersecurity of autonomous systems where we threw some light on the work done in the industry as well as academia on some of the latest autonomous systems related to security listed in Table 6. We focused our work on the system, threats, vulnerabilities,

and attack modeling of a few widely researched autonomous systems, which show how much work has been done in these areas. Our insight into these discussions is that cybersecurity and modeling of individual autonomous systems are at a very early stage. As per our findings and to the best of our knowledge, UAV is the most active field of research concerning the system modeling and attack scenarios. System modeling of autonomous vehicles started with the DARPA challenge. While lots of work related to network security of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) VANET network has been done, the modeling of threat and attack vectors of autonomous vehicles needs lots of attention. Identification of vulnerabilities and threats on robot security started very recently, which can be inferred from Table 6, as most of the work on robot security was published in 2017. There is a vast scope of research and simulation/implementation in these areas. A generalized study on the cybersecurity of these individual systems could be an area of research. New modeling techniques like game theory and machine learning could be applied in these areas as well. Also, the autonomy approach should be taken into account while modeling threats and attack scenarios for these autonomous systems.

7 RESEARCH CHALLENGES AND FUTURE DIRECTIONS

To ensure and assure that these systems are safe and secure to be used by humans, a new approach toward cybersecurity and autonomy is needed. The research community in this area lacks algorithmic solutions to address:

- uncertainties in modeling
- security of autonomous systems from malicious attacks
- accomplishing higher goals through cooperation and collaboration

Autonomy is a dynamic property that needs to adapt to varying unknown situations, depending on the mission complexity. We need a resilient system that performs well over its lifetime. Rigorous mathematical modeling could provide a basis for a framework that would help in the early development study of various capabilities, factors, and tradeoffs between human interaction and machine automation. It could further be used in the development of an autonomy assessment tool, keeping factors like security in mind. Though we are moving ahead toward an autonomous future, there are many research challenges that researches have to face. We have tried to summarize a few of them as follows:

- **Building Human Trust:** After Uber's self-driving car crash in 2018, a survey performed by Statista shows that trust in self-driving cars dropped to 27% (Felix Richter 2018). This is the most intimidating challenge the developer of autonomous systems is about to face. While these systems promise a more comfortable and efficient life, safety and security measures need to be taken before deployment among the public. The world should be ready in legal, social, economic, and ethical context before these systems are incorporated in our lives, as failures of these systems are inevitable at some point in time, either through known or unknown causes. The trust in these systems could only be built by thorough analysis and testing. The service providers and manufacturers of these systems should be stringent when talking about security and be ready with countermeasures when it is compromised.
- **Diverse Training Dataset**: Autonomous systems need to be trained on a large, diverse, and complete dataset to be secure and safe. A simulated dataset is incomplete as it fails to capture critical conditions in the real world. Its relevancy and integrity are questionable as it lacks the human factor. Machine learning is an area that could be applied to enhance the cybersecurity of autonomous vehicles. As discussed in Causevic (2018), if a car's in-vehicular network logs are monitored and analyzed by a machine learning-based system,

it can detect malicious activity early and alert the driver or take some preventive measures to save itself from fatal accidents. With the collected data, machine learning algorithms can be used to detect malware activities, network attacks, or unusual commands. They can also be used to establish behavioral profiles of any potential attacker (Critchley 2018). It would also improve the effectiveness of the security algorithms as the data would be continuously updated and would be unbiased of any technical or human intentions.

— **Data Security**: A lot more research needs to be done in the area of security of communication data and over-the-air updates. Blockchain is an emerging technology that can be used to provide a more secure and robust solution for these autonomous systems. Blockchain, devised initially for digital currency (Bitcoin), is a chain of blocks linked through a cryptographic hash from the previous block with a timestamp and distributed over the network, which makes it resistant to modification of the data. Ferrer (2016) shows that Blockchain has the necessary capabilities for swarm robotics operations to be more secure, autonomous, and flexible. This technology would not only provide a private and reliable communication among swarm agents, but it would also overcome the vulnerabilities, potential threats, and attacks associated with them (Aggarwal 2017). The decentralized storage of Blockchain would guarantee the confidentiality and integrity of the driver's data with no downtime in network connectivity of autonomous vehicles. It would also ensure the accuracy of data in a V2V or V2I communication (Williamson 2018).

— **Computing Power and Network Management**: Current status of autonomous systems lacks the computational capability to perform computationally intensive tasks on large datasets such as encryption of collected data to be shared securely over the network. The end controller of these systems in many cases would be handheld devices such as mobile phones and controllers, which lack the computational power to run advanced security algorithms. One solution is to embed security into the hardware design. Another solution is to secure the network against cyberattacks by network softwarization such as Network Function Virtualization (NFV) and Software Defined Networking (SDN) (Shakhatreh et al. 2018). SDN provides efficient network management, programmability, and ease of reconfiguration (Zhang et al. 2017). It provides a flexible and dynamic environment with a view of the entire network topology, which helps to block specific attacks such as DDoS based on network's policy (Niyaz et al. 2016; Ydenberg et al. 2018). A group of researchers proposed a secure mobility model between UAVs and ground Wireless Sensor Network (WSN) nodes where communication would be through the SDN controller for authentication and coordination (Kumar et al. 2017). SDN provides a virtual, centralized, software-based control that allows easy integration of security-relevant functions into an SDN controller. Along with the holistic view of security, SDN provides an improved response in case of any security incidents, which would otherwise take a long time to respond to in a traditional network (Edward Amoroso 2019).

8 CONCLUSION

This article presents a survey on security modeling of autonomous systems. We looked at the history of automation and the various approaches of autonomy to get a deeper understanding of the scope of automation in these systems. We also highlighted significant research done toward the study of security in some widely researched systems both in the industry as well as academia, followed by identification of survey papers regarding the modeling of the systems and possible attacks. Finally, we provided an overall analysis of the surveyed papers and concluded with a discussion on future research directions and challenges to enhance the automation and security of these systems. Adoption of autonomous systems discussed above will usher a new era of

technological advances and economic growth. Driverless cars are expected to reduce road accidents, fuel consumption, traffic congestion, and air pollution (Darrell M. West 2017). Robots would be deployed in homes and various industrial sectors to provide assistance and efficiency in a routine as well as high-precision jobs. The question is, how secure and safe are these technologies to be adopted into society? With every new revolution in transportation, there are risk factors involved. These systems should not be immaturely deployed into the public. Researchers in industry and academia alike have to shoulder the responsibility of addressing the security flaws. The manufacturers have to ensure the safety of its users, considering even the remote scenarios of mishaps and attacks. Also, the government has to have proper legal policies and supporting infrastructure in place (Kaur and Rampersad 2018).

REFERENCES

Hezam Akram Abdul-Ghani, Dimitri Konstantas, and Mohammed Mahyoub. 2018. A comprehensive IoT attacks survey based on a building-blocked reference model. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* 9, 3 (2018).

Manuj Aggarwal. 2017. Blockchain in Robotics—A Sneak Peek into the Future. Retrieved July 18, 2018 from https://tinyurl.com/y5flry5n.

Raja Naeem Akram, Pierre-François Bonnefoi, Serge Chaumette, Konstantinos Markantonakis, and Damien Sauveron. 2016. Secure autonomous UAVs fleets by using new specific embedded secure elements. In *Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, 606–614.

Mohammed Saeed Al-Kahtani. 2012. Survey on security attacks in vehicular ad hoc networks (VANETs). In *Proceedings of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS'12)*. IEEE, 1–9.

Hamad Al-Mohannadi, Qublai Mirza, Anitta Namanya, Irfan Awan, Andrea Cullen, and Jules Disso. 2016. Cyber-attack modeling analysis techniques: An overview. In *Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. IEEE, 69–76.

Dario Albani, Joris I. Jsselmuiden, Ramon Haken, and Vito Trianni. 2017. Monitoring and mapping with robot swarms for agricultural applications. In *Proceedings of the 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. IEEE, 1–6.

Homa Alemzadeh, Daniel Chen, Xiao Li, Thenkurussi Kesavadas, Zbigniew T. Kalbarczyk, and Ravishankar K. Iyer. 2016. Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation. In *Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'16)*. IEEE, 395–406.

Rasim Alguliyev, Yadigar Imamverdiyev, and Lyudmila Sukhostat. 2018. Cyber-physical systems and their security issues. *Comput. Ind.* 100 (2018), 212–223.

Edward Amoroso. 2019. Security Advantages of Software Defined Networking (SDN). Retrieved February 26, 2019 from http://tinyurl.com/yynq6gpg.

Maria Azees, Pandi Vijayakumar, and Lazarus Jegatha Deborah. 2016. Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intel. Transport Syst.* 10, 6 (2016), 379–388.

Lisanne Bainbridge. 1983. Ironies of automation. In *Analysis, Design and Evaluation of Man–Machine Systems 1982*. Elsevier, 129–135.

Lina Bariah, Dina Shehada, Ehab Salahat, and Chan Yeob Yeun. 2015. Recent advances in VANET security: A survey. In *Proceedings of the 2015 IEEE 82nd Vehicular Technology Conference (VTC Fall)*. IEEE, 1–7.

Ramon Bauza, Javier Gozalvez, and Joaquin Sanchez-Soriano. 2010. Road traffic congestion detection through cooperative vehicle-to-vehicle communications. In *Proceedings of the 2010 IEEE 35th Conference Local Computer Networks (LCN)*. IEEE, Denver, CO. https://ieeexplore.ieee.org/abstract/document/5735780/.

Gordon D. Baxter, John Rooksby, Yuanzhi Wang, and Ali Khajeh-Hosseini. 2012. The ironies of automation: still going strong at 30? In *ECCE*. 65–71.

Jenay M. Beer, Arthur D. Fisk, and Wendy A. Rogers. 2014. Toward a framework for levels of robot autonomy in human-robot interaction. *J. Human-Robot Interact.* 3, 2 (2014), 74–99. DOI: https://doi.org/10.5898/JHRI.3.2.Beer arxiv:15334406

Vahid Behzadan. 2017. Cyber-physical attacks on UAS networks—Challenges and open research problems. arxiv:1702.01251 http://arxiv.org/abs/1702.01251.

Brian Beyst. 2016. Comparing ThreatModeler to Microsoft Threat Modeling Tool (TMT). Retrieved May 26, 2018 from https://tinyurl.com/y379hnrb.

Sourabh Bhattacharya and Tamer. Basar. 2010. Game-theoretic analysis of an aerial jamming attack on a UAV communication network. In *Proceedings of the American Control Conference (ACC)*. IEEE, 818–823. DOI: https://doi.org/978-1-4244-7427-1

Sourabh Bhattacharya and Tamer Basar. 2012. Multi-layer hierarchical approach to double sided jamming games among teams of mobile agents. In *Proceedings of the IEEE Conference on Decision and Control* (2012). 5774–5779. DOI: https://doi.org/10.1109/CDC.2012.6426411

Trevor J. Bihl, Chad Cox, and Todd Jenkins. 2018. Finding common ground by unifying autonomy indices to understand needed capabilities. In *Sensors and Systems for Space Applications XI*, Vol. 10641. International Society for Optics and Photonics, 106410G.

Tamara Bonaci, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. 2015. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. *arXiv preprint arXiv:1504.04339* (2015).

Jeffery Bradshaw, Andrzej Uszok, Renia Jeffers, Niranjan Suri, Patric Hayes, Mark Burstein, Alessandro Acquisti, Brett Benyo, M. Breedy, Marco Carvalho, et al. 2003. Representation and reasoning for DAML-based policy and domain services in KAoS and Nomads. In *Proceedings of the 2nd International Joint Conference on Autonomous Agents and Multiagent Systems*. ACM, 835–842.

Jeffrey M. Bradshaw, Alessandro Acquisti, James Allen, Maggie R. Breedy, Larry Bunch, Nate Chambers, Paul Feltovich, Lucian Galescu, Michael A. Goodrich, Renia Jeffers, et al. 2004a. Teamwork-centered autonomy for extended human-agent interaction in space applications. In *Proceedings of the AAAI 2004 Spring Symposium*. 22–24.

Jeffrey M. Bradshaw, Patrick Beautement, Maggie R. Breedy, Larry Bunch, Sergey V. Drakunov, Paul J. Feltovich, Robert R. Hoffman, Renia Jeffers, Matthew Johnson, Shriniwas Kulkarni, et al. 2004b. Making agents acceptable to people. In *Intelligent Technologies for Information Analysis*. Springer, 361–406.

Jeffrey M. Bradshaw, Hyuckchul Jung, Shri Kulkarni, Matthew Johnson, Paul Feltovich, James Allen, Larry Bunch, Nathanael Chambers, Lucian Galescu, Renia Jeffers, et al. 2005. Kaa: Policy-based explorations of a richer model for adjustable autonomy. In *Proceedings of the 4th International Joint Conference on Autonomous Agents and Multiagent Systems*. ACM, 214–221.

David J. Bruemmer, Donald D. Dudenhoeffer, and Julie L. Marble. 2002. Dynamic-autonomy for urban search and rescue. In *AAAI Mobile Robot Competition*. 33–37.

Patrick Caughill. 2017. An Artificial Intelligence Has Officially Been Granted Residency. Retrieved May 26, 2018 from http://tinyurl.com/y9q3zpz4.

Dino Causevic. 2018. How Machine Learning Can Enhance Cybersecurity for Autonomous Cars. Retrieved October 1, 2018 from http://tinyurl.com/yyrhhsg7.

CCW. 2018. Five Years of Campaigning, CCW Continues. Retrieved June 09, 2018 from https://www.stopkillerrobots.org/2018/03/fiveyears/.

Cesar Cerrudo and Lucas Apa. 2017. Hacking robots before skynet. *IOActive Website* 2017 (2017), 1–17.

George W. Clark, Michael V. Doran, and Todd R. Andel. 2017. Cybersecurity issues in robotics. In *IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA'17)*. IEEE, 1–5.

Bruce T. Clough. 2002. *Metrics, Schmetrics! How the Heck Do You Determine a UAV's Autonomy Anyway?* Technical Report 990. Air Force Research Lab, Wright-Patterson AFB OH. 313–319 pages. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA515926.

Cognilytica. 2018. Will There Be Another AI Winter? Retrieved June 26, 2018 from https://www.cognilytica.com/2018/02/22/will-another-ai-winter/.

Ciprian Adrian Corneanu, Marc Oliu Simón, Jeffrey F. Cohn, and Sergio Escalera Guerrero. 2016. Survey on rgb, 3D, thermal, and multimodal approaches for facial expression recognition: History, trends, and affect-related applications. *IEEE Trans. Pattern Anal. Mach. Intell.* 38, 8 (2016), 1548–1568.

Gary Cornelius, Patrice Caire, Nico Hochgeschwender, Miguel A. Olivares-Mendez, Paulo Esteves-Verissimo, Marcus Völp, and Holger Voos. 2017. A perspective of security for mobile service robots. In *Proceedings of ROBOT 2017: 3rd Iberian Robotics Conference*. 88–100. DOI: https://doi.org/10.1007/978-3-319-70833-1_8

Nikolaus Correll and Alcherio Martinoli. 2009. Multirobot inspection of industrial machinery. *IEEE Rob. Autom. Mag.* 16, 1 (2009), 103–112. https://ieeexplore.ieee.org/abstract/document/4799452/.

Liam Critchley. 2018. How Machine-Based Learning Will Protect Automobiles from Cyber Attacks. Retrieved October 1, 2018 from https://www.azom.com/article.aspx?ArticleID=15659.

Mary L. Cummings, Sylvain Bruni, S. Mercier, and P. J. Mitchell. 2007. *Automation Architecture for Single Operator, Multiple UAV Command and Control*. Technical Report. Massachusetts Inst. of Tech Cambridge.

Mary Missy Cummings. 2014. Man versus machine or man+ machine?*IEEE Intell. Syst.* 29, 5 (2014), 62–69.

Praveen Damacharla, Ahmad Y. Javaid, Jennie J. Gallimore, and Vijay K. Devabhaktuni. 2018. Common metrics to benchmark human-machine teams (HMT): A review. *IEEE Access* 6 (2018), 38637–38655.

Drew Davidson, Hao Wu, Robert Jellinek, Thomas Ristenpart, and Vikas Singh. 2016. Controlling UAVs with sensor input spoofing attacks. In *Proceedings of the 10th USENIX Conference on Offensive Technologies (WOOT'16)*. 221–231.

Alex Davies. 2018. The Self-Driving Startup Teaching Cars to Talk. Retrieved February 26, 2019 from https://www.wired.com/story/driveai-self-driving-design-frisco-texas/.

Office of the Secretary of Defense, Washington D.C. 2001. *Unmanned Aerial Vehicles Roadmap 2000-2025*. Technical Report. Defense Pentagon, Washington, D.C.

Meghann Lomas De Brun, Vera Zaychik Moffitt, Jerry L. Franke, Dimitri Yiantsios, Trevor Housten, Adria Hughes, Shannon Fouse, and Drew Housten. 2008. Mixed-initiative adjustable autonomy for human/unmanned system teaming. In *AUVSI Unmanned Systems North America Conference*.

Matthew DeBord. 2018. Waymo Has Launched Its Commercial Self-driving Service in Phoenix and It's Called "Waymo One". Retrieved February 26, 2019 from http://tinyurl.com/y25d4g9x.

Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua R. Smith, and Tadayoshi Kohno. 2009. A spotlight on security and privacy risks with future household robots. In *Proceedings of the 11th International Conference on Ubiquitous Computing - Ubicomp'09*. ACM, 105. DOI: https://doi.org/10.1145/1620545.1620564

Munjal Desai. 2007. *Sliding Scale Autonomy and Trust in Human-robot Interaction*. Master's thesis. 1442064.

Munjal Desai and Holly A. Yanco. 2005. Blending human and robot inputs for sliding scale autonomy. In *Proceedings of the IEEE International Workshop on Robot and Human Interactive Communication (ROMAN'05)*. IEEE, 537–542.

A. Dhamgaye and N. Chavhan. 2013. Survey on security challenges in VANET. *Int. J. Comput. Sci. Network* 2, 1 (2013), 1. DOI: https://doi.org/10.1109/COMST.2015.2453114

M. Bernardine Dias, Balajee Kannan, Brett Browning, E. Gil Jones, Brenna Argall, M. Freddie Dias, Marc Zinck, Manuela M. Veloso, and Anthony J. Stentz. 2008. Sliding autonomy for peer-to-peer human-robot teams. *Intell. Auton. Syst. 10, IAS 2008* (2008), 332–341. DOI: https://doi.org/10.3233/978-1-58603-887-8-332

Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, and Xian-Ming Zhang. 2018. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomput.* 275 (2018), 1674–1683.

Gregory A. Dorais, R. Peter Bonasso, David Kortenkamp, Barney Pell, and Debra Schreckenghost. 1999. Adjustable autonomy for human-centered autonomous systems. In *Proceedings of the 16th International Joint Conference on Artificial Intelligence Workshop on Adjustable Autonomy Systems*. 16–35.

Luke Dormehl. 2017. MiRo Is the Robot Dog that Promises to Be a Geek's Best Friend. Retrieved May 20, 2019 from https://tinyurl.com/yxz74w93.

Warren R. Dufrene. 2005. An approach for autonomy: A collaborative communication framework for multi-agent systems. In *Workshop on Radical Agent Concepts*. Springer, 147–159.

Muawia Abdelmagid Elsadig and Yahia A. Fadlalla. 2016. VANETs security issues and challenges: A survey. *Indian J. Sci. Technol.* 9, 28 (2016).

Mica R. Endsley. 1987. The application of human factors to the development of expert systems for advanced cockpits. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 31. SAGE Publications Sage CA, Los Angeles, CA, 1388–1392.

Mica R. Endsley. 1988. Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors Society Annual Meeting*, Vol. 32. SAGE Publications Sage CA: Los Angeles, CA, 97–101.

Mica R. Endsley. 1995. Towards a new paradigm for automation: Designing for situation awareness. *IFAC Proceedings Volumes* 28, 15 (1995), 365–370. DOI: https://doi.org/10.1016/S1474-6670(17)45259-1

Mica R. Endsley and David B. Kaber. 1999. Level of automation effects on performance, situation awareness and workload in a dynamic control task. *Ergon.* 42, 3 (1999), 462–492.

Control Engineering. 2016. IoT to IoAT: Internet of Autonomous Things Devices Provides Solutions. Retrieved June 18, 2018 from https://tinyurl.com/y5nlonp8.

Aisha D. Farooqui and Muaz A. Niazi. 2016. *Game Theory Models for Communication between Agents: A Review*. Vol. 4. 13 pages. DOI: https://doi.org/10.1186/s40294-016-0026-7 arxiv:1708.01636.

Nicholas Fearn. 2018. The Cutting-Edge Tech Set to Define 2018. Retrieved from http://www.techx365.com/author.asp?section_id=686&doc_id=739321.

David Feil-Seifer, Kristine Skinner, and Maja J. Matarić. 2007. Benchmarks for evaluating socially assistive robotics. *Interact. Stud.* 8, 3 (2007), 423–439.

Eduardo Castelló Ferrer. 2016. The blockchain: A new framework for robotic swarm systems. *arXiv preprint arXiv:1608.00695* (2016).

Tomas Foltyn. 2018. Cybersecurity Trends 2019: Privacy and Intrusion in the Global Village. *Check Point Research*. Retrieved from http://tinyurl.com/yxeph2cb.

T. Fong, N. Cabrol, C. Thorpe, and C. Baur. 2001. A personal user interface for collaborative human-robot exploration. In *6th International Symposium on Artificial Intelligence, Robotics, and Automation in Space (iSAIRAS'01)*.

Stefano Fontanelli, Enrico Bini, and Paolo Santi. 2010. Dynamic route planning in vehicular networks based on future travel estimation. In *Proceedings of the 2010 Vehicular Networking Conference (VNC)*. IEEE, Jersey City, NJ. https://ieeexplore.ieee.org/abstract/document/5698247/.

Douglas M. Gage. 1985. Security considerations for autonomous robots. In *1985 IEEE Symposium on Security and Privacy*. IEEE, 224–224.

Dom Galeon. 2017. World's First AI Citizen in Saudi Arabia is Now Calling for Women's Rights. Retrieved May 26, 2018 from http://tinyurl.com/yyqcksxq.

Mevlut Turker Garip, Mehmet Emre Gursoy, Peter Reiher, and Mario Gerla. 2015. Congestion attacks to autonomous cars using vehicular botnets. In *NDSS Workshop on Security of Emerging Networking Technologies (SENT), San Diego, CA*.

Michael Giering, Vivek Venugopalan, and Kishore Reddy. 2015. Multi-modal sensor registration for vehicle perception via deep neural networks. In *Proceedings of the 2015 High Performance Extreme Computing Conference (HPEC)*. IEEE, 1–6.

Saira Gillani, Farrukh Shahzad, Amir Qayyum, and Rashid Mehmood. 2013. A survey on security in vehicular ad hoc networks. In *International Workshop on Communication Technologies for Vehicles*. Springer, 59–74.

Michael A. Goodrich, Alan C. Schultz, et al. 2008. Human—robot interaction: a survey. *Foundations and TrendsR in Human—Computer Interaction* 1, 3 (2008), 203–275.

James Goppert, Weiyi Liu, Andrew Shull, Vincent Sciandra, Inseok Hwang, and Hal Aldridge. 2012. Numerical analysis of cyberattacks on unmanned aerial systems. *AIAA Infotech at Aerospace Conference and Exhibit 2012*. DOI: https://doi.org/10.2514/6.2012-2437

Andy Greenberg. 2015. Hackers Remotely Kill a Jeep on the Highway—With Me In It. Retrieved May 26, 2018 from http://tinyurl.com/o9coyn4.

Pinyao Guo, Hunmin Kim, Nurali Virani, Jun Xu, Minghui Zhu, and Peng Liu. 2017. Exploiting physical dynamics to detect actuator and sensor attacks in mobile robots. *CoRR* abs/1708.01834 (2017).

David Hambling. 2017. Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon. Retrieved July 18, 2018 from http://tinyurl.com/ycuzl3pz.

Elyes Ben Hamida, Hassan Noura, and Wassim Znaidi. 2015. Security of cooperative intelligent transport systems: Standards, threats analysis, and cryptographic countermeasures. *Electron.* 4, 3 (2015), 380–423.

Ali Hamieh, Jalel Ben-Othman, and Lynda Mokdad. 2009. Detection of radio interference attacks in VANET. In *Proceedings of the Global Telecommunications Conference, 2009 (GLOBECOM)*. IEEE, Honolulu, HI. DOI: https://doi.org/10.1109/GLOCOM.2009.5425381

M. Hans, B. Graf, and R. D. Schraft. 2002. Robotic home assistant care-o-bot: Past-present-future. In *Proceedings of the 11th IEEE International Workshop on Robot and Human Interactive Communication, 2002*. 380–385.

Musad Haque, Electa Baker, Christopher Ren, Douglas Kirkpatrick, and Julie A. Adams. 2018. Analysis of biologically inspired swarm communication models. In *Advances in Hybridization of Intelligent Methods*. Springer, 17–38.

Benjamin Hardin and Michael A. Goodrich. 2009. On using mixed-initiative control: A perspective for managing large-scale robotic teams. In *Proceedings of the 4th ACM/IEEE International Conference on Human Robot Interaction*. ACM, 165–172.

F. W. Heger and S. Singh. 2006. Sliding autonomy for complex coordinated multi-robot tasks: Analysis & experiments. In *Proceedings, Robotics: Systems and Science, Philadelphia*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.148.9892&rep=rep1&type=pdf.

Frederik W. Heger, Laura M. Hiatt, Brennan Sellner, Reid Simmons, and Sanjiv Singh. 2005. Results in sliding autonomy for multi-robot spatial assembly. *European Space Agency, (Special Publication) ESA SP*603 (2005), 489–496.

Fiona Higgins, Allan Tomlinson, and Keith M. Martin. 2009. Threats to the swarm: Security considerations for swarm robotics. *Int. J. Adv. Secur.* 2, 2&3 (2009), 288–297.

Kashmir Hill. 2016. Security robot accidentally attacks child. Retrieved April 03, 2018 from https://tinyurl.com/yynv5se3.

Homer. [n.d.]. The Iliad. In *Vol. Book XVIII*. circa.

Christopher-Eyk Hrabia, Nils Masuch, and Sahin Albayrak. 2015. A metrics framework for quantifying autonomy in complex systems. In *German Conference on Multiagent System Technologies*. Springer, 22–41.

H. M. Huang. 2004. Autonomy levels for unmanned systems (ALFUS) framework Volume I : Terminology version 2.0. Technical Report.

Hui-Min Huang. 2007. Autonomy levels for unmanned systems (ALFUS) framework: Safety and application issues. In *Proceedings of 2007 Workshop on Performance Metrics for Intelligent Systems (PerMIS'07)*. 48–53. DOI: https://doi.org/10.1145/1660877.1660883

Hui-Min Huang, James S. Albus, Elena R. Messina, Robert L. Wade, and R. W. English. 2004a. Specifying autonomy levels for unmanned systems: Interim report. In *Proceedings of SPIE Defense and Security Symposium 2004*. 386–397. DOI: https://doi.org/10.1117/12.552074

Hui-Min Huang, Elena Messina, and James Albus. 2003b. Autonomy level specification for intelligent autonomous vehicles: Interim progress report. In *2003 Performance Metrics for Intelligent Systems (PerMIS)* September (2003). 1–7.

Hui-Min Huang, Elena Messina, and James Albus. 2003a. *Toward a Generic Model for Autonomy Levels for Unmanned Systems (ALFUS)*. Technical Report. National Institute of Standards and Technology, Gaithersburg, MD.

Hui-Min Huang, Elena Messina, Robert Wade, Ralph English, Brian Novak, and James Albus. 2004b. Autonomy measures for robots. In *ASME 2004 International Mechanical Engineering Congress and Exposition*. American Society of Mechanical Engineers, 1241–1247.

Hui-Min Huang, Kerry Pavek, James Albus, and Elena Messina. 2005. Autonomy levels for unmanned systems (ALFUS) framework: An update. *Proc. SPIE* 5804, June (2005), 439–448. DOI: https://doi.org/10.1117/12.603725

Tom Huddleston Jr. 2018. Move Over Tesla, This Self-driving Car Will Let You Sleep or Watch a Movie during Your Highway Commute. Retrieved February 26, 2019 from http://tinyurl.com/yad58cgj.

Todd Humphrey. 2012. Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV. Retrieved July 18, 2018 from http://tinyurl.com/yydz75x5.

Ians. 2015. Surgical Robots to Become Ubiquitous in Indian Hospitals. Retrieved September 13, 2018 from http://tinyurl.com/y2rfp2es.

Smart Industry. 2017. Blockchain Makes IoT Devices Autonomous. Retrieved 2018-06-19 from https://tinyurl.com/y5w784re.

Farha Jahan, Ahmad Y. Javaid, Weiqing Sun, and Mansoor Alam. 2015. GNSSim: An open source GNSS/GPS framework for unmanned aerial vehicular network simulation. *EAI Endorsed Trans. Mobile Commun. Appl.* 2, 6 (2015), 1–13.

Ahmad Y. Javaid, Farha Jahan, and Weiqing Sun. 2017. Analysis of global positioning system-based attacks and a novel global positioning system spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation. *Simul.* 93, 5 (2017), 427–441.

Ahmad Y. Javaid, Weiqing Sun, and Mansoor Alam. 2015. Single and multiple UAV cyber-attack simulation and performance evaluation. *EAI Endorsed Trans. Scalable Inf. Syst.* 2, 4 (2015), 1–11.

Ahmad Y. Javaid, Weiqing Sun, Vijay K. Devabhaktuni, and Mansoor Alam. 2012. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*. IEEE, 585–590.

Kanwaldeep Kaur and Giselle Rampersad. 2018. Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars. *J. Eng. Tech. Manage.* 48 (2018), 87–96.

Alan Kim, Brandon Wampler, James Goppert, Inseok Hwang, and Hal Aldridge. 2012. Cyber attack vulnerabilities analysis for unmanned aerial vehicles. *Infotech@Aerospace 2012* (2012), 1–30. DOI: https://doi.org/10.2514/6.2012-2438

Matthew Klenk, Matt Molineaux, and David W. Aha. 2013. Goal-driven autonomy for responding to unexpected events in strategy simulations. *Comput. Intell.* 29, 2 (2013), 187–206.

Timo Korthals, Mikkel Kragh, Peter Christiansen, Henrik Karstoft, Rasmus N. Jørgensen, and Ulrich Rückert. 2018. Multimodal detection and mapping of static and dynamic obstacles in agriculture for process evaluation. *Front. Rob. AI* 5 (2018), 28.

Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. 2010. Experimental security analysis of a modern automobile. In *Proceedings of the IEEE Symposium on Security and Privacy (SP'10)*. IEEE, 447–462.

C. G. Leela Krishna and Robin R. Murphy. 2017. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In *Proceedings of the IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR'17)*. IEEE, 194–199.

Rajesh Kumar, Mohd Abuzar Sayeed, Vishal Sharma, and Ilsun You. 2017. An SDN-based secure mobility model for UAV-ground communications. In *Proceedings of the International Symposium on Mobile Internet Security*. Springer, 169–179.

Cheolhyeon Kwon, Weiyi Liu, and Inseok Hwang. 2013. Security analysis for cyber-physical systems against stealthy deception attacks. In *Proceedings of the 2013 American Control Conference (ACC)*. IEEE, 3344–3349.

Cheolhyeon Kwon, Scott Yantek, and Inseok Hwang. 2016. Real-time safety assessment of unmanned aircraft systems against stealthy cyber attacks. *J. Aerosp. Inf. Syst.* 13, 1 (2016), 27–45. DOI: https://doi.org/10.2514/1.I010388

Dimosthenis Kyriazis and Theodora Varvarigou. 2013. Smart, autonomous and reliable Internet of Things. *Procedia Comput. Sci.* 21 (2013), 442–448.

Hoa La Vinh and Ana Rosa Cavalli. 2014. Security attacks and solutions in vehicular ad hoc networks: A survey. *Int. J. Ad Hoc Networking Syst. (IJANS)* 4, 2 (2014), 1–20.

Michel Lacerda, Dongjin Park, Srujal Patel, and Daniel Schrage. 2018. A Mars exploration concept systems design with an innovative unmanned autonomous vehicle and "carrier" ground rover configuration. Part I: System design. In *Proceedings of the 2018 Aviation Technology, Integration, and Operations Conference*. 3262.

Fred Lambert. 2018. Watch What Tesla Autopilot Can See in Incredible 360º Video. Retrieved 2018-11-26 from https://electrek.co/2018/11/26/tesla-autopilot-360-video/.

John Leonard, Jonathan How, Seth Teller, Mitch Berger, Stefan Campbell, Gaston Fiore, Luke Fletcher, Emilio Frazzoli, Albert Huang, Sertac Karaman, et al. 2008. A perception-driven autonomous urban vehicle. *J. Field Rob.* 25, 10 (2008), 727–774.

Francisco J. Rodríguez Lera, Camino Fernández Llamas, Ángel Manuel Guerrero, and Vicente Matellán Olivera. 2017. Cybersecurity of robotics and autonomous systems: Privacy and safety. In *Robotics-Legal, Ethical and Socioeconomic Impacts*. InTech. DOI: https://doi.org/10.5772/46845

Hui Lin, Homa Alemzadeh, Daniel Chen, Zbigniew Kalbarczyk, and Ravishankar K. Iyer. 2016. Safety-critical cyber-physical attacks: Analysis, detection, and mitigation. In *Proceedings of the Symposium and Bootcamp on the Science of Security*. ACM, 82–89.

Lanny Lin, Michael A. Goodrich, and Spencer Clark. 2012. Sliding autonomy for UAV path planning: Adding new dimensions to autonomy management. *J. Hum.-Rob. Interact.* 1, 1 (2012), 78–95. DOI: https://doi.org/10.5898/JHRI.1.1.Tanaka

Nikita Lyamin, Alexey Vinel, Magnus Jonsson, and Jonathan Loo. 2014. Real-time detection of denial-of-service attacks in IEEE 802.11 p vehicular networks. *IEEE Commun. Lett.* 18, 1 (2014), 110–113.

Bharat B. Madan, Manoj Banik, and Doina Bein. 2019. Securing unmanned autonomous systems from cyber threats. *J. Defense Model. Simul.* 16, 2 (2019), 119–136.

Federico Maggi, Davide Quarta, Marcello Pogliani, Mario Polino, Andrea M. Zanchettin, and Stefano Zanero. 2017. *Rogue Robots: Testing the Limits of an Industrial Robot's Security*. Technical Report. Trend Micro, Politecnico di Milano.

Katrina Mansfield, Timothy Eveleigh, Thomas H. Holzer, and Shahryar Sarkani. 2013. Unmanned aerial vehicle smart device ground control station cyber security threat model. In *IEEE International Conference on Technologies for Homeland Security (HST'13)*. IEEE, 722–728.

Stephen McBride. 2018. The Driverless Car Revolution Has Begun—Here's How To Profit. Retrieved from http://tinyurl.com/ydzby4yr.

Joe W. McDaniel. 1988. Rules for fighter cockpit automation. In *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference (NAECON'88)*. IEEE, 831–838.

Dhwani Mehta, Mohammad Faridul Haque Siddiqui, and Ahmad Y. Javaid. 2018. Facial emotion recognition: A survey and real-world user experiences in mixed reality. *Sens.* 18, 2 (2018), 416.

Mohamed Nidhal Mejri and Jalel Ben-Othman. 2014b. Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks. In *Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM)*. IEEE, Austin, TX. DOI: https://doi.org/10.1109/GLOCOM.2014.7037603

Mohamed Nidhal Mejri and Jalel Ben-Othman. 2014a. Entropy as a new metric for denial of service attack detection in vehicular ad-hoc networks. In *Proceedings of the 17th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. ACM, 73–79.

Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. 2014. Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* 1, 2 (2014), 53–66.

Mohamed Nidhal Mejri and Mohamed Hamdi. 2015. Recent advances in cryptographic solutions for vehicular networks. In *International Symposium Networks, Computers and Communications (ISNCC'15)*. IEEE. DOI: https://doi.org/10.1109/ISNCC.2015.7238573

Kathryn Merrick, Medria Hardhienata, Kamran Shafi, and Jiankun Hu. 2016. A survey of game theoretic approaches to modelling decision-making in information warfare scenarios. *Future Internet* 8, 3 (2016), 34.

Vera Zaychik Moffitt, Jerry L. Franke, and Meghann Lomas. 2006. Mixed-initiative adjustable autonomy in multi-vehicle operations. In *Proceedings of AUVSI, Orlando, Florida* (2006).

Matthew Molineaux, Matthew Klenk, and David W. Aha. 2010. Goal-driven autonomy in a navy strategy simulation. In *AAAI*. 1548–1554.

Salama A. Mostafa, Mohd Sharifuddin Ahmad, and Aida Mustapha. 2017. Adjustable autonomy: A systematic literature review. *Artif. Intell. Rev.* (2017), 1–38. DOI: https://doi.org/10.1007/s10462-017-9560-8

Salama A. Mostafa, Mohd Sharifuddin Ahmad, and Aida Mustapha. 2019. Adjustable autonomy: A systematic literature review. *Artif. Intell. Rev.* 51, 2 (2019), 149–186.

Jordan Navarro. 2018. A state of science on highly automated driving. *Theoretical Issues in Ergonomics Science* 20, 3 (2019), 366–396.

Navya. 2018. Navya History. Retrieved March 2, 2019 from https://www.navya-corp.com/index.php/fr/navya/histoire.

Annalee Newitz. 2013. 15 Books That Will Change the Way You Look at Robots. Retrieved March 03, 2018 from http://tinyurl.com/yy2mkkwg.

Quamar Niyaz, Weiqing Sun, and Ahmad Y. Javaid. 2016. A deep learning based DDoS detection system in software-defined networking (SDN). *arXiv preprint arXiv:1611.07400* (2016).

Donald A. Norman. 1990. The problem with automation: Inappropriate feedback and interaction, not over-automation. *Phil. Trans. R. Soc. Lond. B* 327, 1241 (1990), 585–593.

University of Nottingham–Mixed Reality Laboratory. 2016. Future Everyday Interaction with the Autonomous Internet of Things (A-IoT). Retrieved June 19, 2018 from https://tinyurl.com/yylnuarh.

Ebenezer A. Oladimeji, Sam Supakkul, and Lawrence Chung. 2006. Security threat modeling and analysis: A goal-oriented approach. In *Proceedings of the 10th IASTED International Conference on Software Engineering and Applications (SEA'06)*. Citeseer, 13–15.

Ancient Origins. 2013. Talos Crete. Retrieved March 05, 2018 from http://www.ancient-origins.net/myths-legends/talos-crete-00157.

Joe Pappalardo. 2018. The Dream of Drone Delivery Just Became Much More Real. Retrieved February 26, 2019 from http://tinyurl.com/yylzkvqs.

Raja Parasuraman, Toufik Bahri, John E. Deaton, Jeffrey G. Morrison, and Michael Barnes. 1992. *Theory and Design of Adaptive Automation in Aviation Systems*. Technical Report. Catholic Univ of America, Washington D.C., Cognitive Science Lab. http://books.google.com.my/books?id=DEtSOwAACAAJ.

R. Parasuraman, T. B. Sheridan, and C. D. Wickens. 2000. A model for types and levels of human interaction with automation. *IEEE Trans. Syst. Man Cybern. Part A Syst. Humans* 30, 3 (May 2000), 286–297. DOI: https://doi.org/10.1109/3468.844354

Simon Parkinson, Paul Ward, Kyle Wilson, and Jonathan Miller. 2017. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Trans. Intell. Transp. Syst.* 18, 11 (2017), 2898–2915.

Scott Drew Pendleton, Hans Andersen, Xinxin Du, Xiaotong Shen, Malika Meghjani, You Hong Eng, Daniela Rus, and Marcelo H. Ang. 2017. Perception, planning, control, and coordination for autonomous vehicles. *Machines* 5, 1 (2017), 6.

Jonathan Petit and Steven E. Shladover. 2015. Potential cyberattacks on automated vehicles. *IEEE Trans. Intell. Transp. Syst.* 16, 2 (2015), 546–556. DOI: https://doi.org/10.1109/TITS.2014.2342271

Jonathan Petit, Bas Stottelaar, Michael Feiri, and Frank Kargl. 2015. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Europe* 11 (2015), 2015.

T. Proscevicius, A. Bukis, V. Raudonis, and M. Eidukeviciute. 2011. Hierarchical control approach for autonomous mobile robots. *Elektronika ir Elektrotechnika* 110, 4 (2011), 101–104.

Oscar Puñal, Ana Aguiar, and James Gross. 2012. In VANETs we trust?: Characterizing RF jamming in vehicular networks. In *Proceedings of the 9th ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications*. ACM, 83–92.

Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea Maria Zanchettin, and Stefano Zanero. 2017. An experimental security analysis of an industrial robot controller. In *2017 38th IEEE Symposium on Security and Privacy (SP)*. IEEE, 268–286.

Nancy E. Reed. 2005. A user controlled approach to adjustable autonomy. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*. 295b–295b. DOI: https://doi.org/10.1109/HICSS.2005.61

Felix Richter. 2018. Fatal Accidents Damage Trust in Autonomous Driving. Retrieved May 26, 2018 from https://tinyurl.com/y3lbkx8a.

M. E. Rosheim. 2006. Leonardo's Lost Robot. Springer Verlag, Berlin.

Joey Roulette. 2019. Self-driving Buses Roll into Orlando's Lake Nona, a Growing Testbed for "Smart City" Technology. Retrieved February 26, 2019 from http://tinyurl.com/yy3kc8kh.

William B. Rouse. 1976. Adaptive allocation of decision making responsibility between supervisor and computer. In *Monitoring Behavior and Supervisory Control*. Springer, 295–306.

Erol Sahin. 2005. Swarm robotics: From sources of inspiration to domains of application. In *Swarm Robotics*, Erol \cSahin and William M. Spears (Eds.). Springer, Berlin, 10–20.

Mukesh Saini, Abdulhameed Alelaiwi, and Abdulmotaleb El Saddik. 2015. How close are we to realizing a pragmatic VANET solution? A meta-survey. *ACM Comput. Surv. (CSUR)* 48, 2 (2015), 29.

Anibal Sanjab, Walid Saad, and Tamer Başar. 2017. Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game. In *2017 IEEE International Conference on Communications (ICC'17)*. IEEE, 1–6.

Sarah Sloat. 2016. BMW, Intel, Mobileye Link Up in Self-Driving Tech Alliance. Retrieved February 26, 2019 from http://tinyurl.com/y56bwcd2.

Paul Scerri, David V. Pynadath, and Milind Tambe. 2003. Adjustable autonomy for the real world. In *Agent Autonomy*. Springer, 211–241.

Brennan P. Sellner, Laura M. Hiatt, Reid Simmons, and Sanjiv Singh. 2006. Attaining situational awareness for sliding autonomy. In *Proceedings of the 1st ACM SIGCHI/SIGART Conference on Human-Robot Interaction*. ACM, 80–87.

Shervin Shahrdar, Luiza Menezes, and Mehrdad Nojoumian. 2017. A survey on trust in autonomous systems. In *Intelligent Computing*.

Hazim Shakhatreh, Ahmad Sawalmeh, Ala Al-Fuqaha, Zuochao Dou, Eyad Almaita, Issa Khalil, Noor Shamsiah Othman, Abdallah Khreishah, and Mohsen Guizani. 2018. Unmanned aerial vehicles: A survey on civil applications and key research challenges. *arXiv preprint arXiv:1805.00881* (2018).

Yogesh Kumar Sharma and Ashish Bagla. 2009. Security challenges for swarm robotics. *SECURITY CHALLENGES* 2, 1 (2009), 45–48.

Thomas B. Sheridan. 1992. *Telerobotics, Automation, and Human Supervisory Control.* MIT Press, Cambridge, MA.

Thomas B. Sheridan and William L. Verplank. 1978. Human and computer control of undersea teleoperators. Technical Report. Massachusetts Inst. of Tech. Cambridge Man-Machine Systems Lab.

Forrest Shull. 2016. Cyber Threat Modeling: An Evaluation of Three Methods. Retrieved May 26, 2018 from https://tinyurl.com/y3j56guz.

Elizabeth Snell. 2015. Phishing Attack Affects 3,300 Partners HealthCare Patients. Retrieved June 08, 2018 from http://tinyurl.com/y3v8on9f.

Statista. 2018. Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions). Retrieved June 18, 2018 from http://tinyurl.com/j3t9t2w.

Aaron Steinfeld, Terrence Fong, David Kaber, Michael Lewis, Jean Scholtz, Alan Schultz, and Michael Goodrich. 2006. Common metrics for human-robot interaction. In *Proceedings of the 1st ACM SIGCHI/SIGART Conference on Human-Robot Interaction.* ACM, 33–40.

Jie Su, Jianping He, Peng Cheng, and Jiming Chen. 2016. A stealthy GPS spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle. *IFAC-PapersOnLine* 49, 22 (2016), 291–296.

Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, and Jamalul-lail bin Ab Manan. 2011. Classes of attacks in VANET. In *Proceedings of the Saudi International Electronics, Communications and Photonics Conference (SIECPC'11).* IEEE, Riyadh, Saudi Arabia. DOI: https://doi.org/10.1109/SIECPC.2011.5876939

Zhong-yang Tan, Ying, and Zheng. 2013. Research advance in swarm robotics. *Defence Technol.* 9, 1 (2013), 18–39. https://www.sciencedirect.com/science/article/pii/S221491471300024X.

Vrizlynn L. L. Thing and Jiaxi Wu. 2016. Autonomous vehicle security: A taxonomy of attacks and defences. In *Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).* IEEE, 164–170.

Jon Turi. 2014a. GE's Bringing Good Things, and Massive Robots, to Life. Retrieved March 03, 2018 from https://www.engadget.com/2014/01/26/ge-man-amplifying-robots/.

Jon Turi. 2014b. Tesla's Toy Boat: A Drone before Its Time. Retrieved March 03, 2018 from https://www.engadget.com/2014/01/19/nikola-teslas-remote-control-boat/.

Chris Urmson, Joshua Anhalt, Drew Bagnell, Christopher Baker, Robert Bittner, John Dolan, Dave Duggins, Dave Ferguson, Tugrul Galatali, Chris Geyer, Michele Gittleman, Sam Harbaugh, Martial Hebert, Tom Howard, Alonzo Kelly, David Kohanbash, Maxim Likhachev, Nick Miller, Kevin Peterson, Raj Rajkumar, Paul Rybski, Bryan Salesky, Sebastian Scherer, Young Woo-seo, Reid Simmons, Sanjiv Singh, Jarrod Snider, Anthony Stentz, William Red Whittaker, Jason Ziglar, Joshua Struble, and Michael Taylor. 2007. Tartan racing: A multi-modal approach to the DARPA urban challenge. *Defense* 94, 4 (2007), 386–387. DOI: https://doi.org/10.1002/rob.20251

George Vachtsevanos and Johan Reimann. 2004. An intelligent approach to coordinated control of multiple unmanned aerial vehicles. In *Proceedings of the American Helicopter Society 60th Annual Forum, Baltimore, MD.*

Rick van der Kleij, Tom Hueting, and Jan Maarten Schraagen. 2018. Change detection support for supervisory controllers of highly automated systems: Effects on performance, mental workload, and recovery of situation awareness following interruptions. *Int. J. Ind. Ergon.* 66 (2018), 75–84.

Gabriel Vasconcelos, Gabriel Carrijo, Rodrigo Miani, Jefferson Souza, and Vitor Guizilini. 2016. The impact of DoS attacks on the AR. Drone 2.0. In *Proceedings of the 2016 13th Latin American Robotics Symposium and 4th Brazilian Robotics Symposium (LARS/SBR).* IEEE, 127–132.

Chad Vander Veen. 2015. 10 Years, 10 Milestones for Driverless Cars. Retrieved February 26, 2019 from https://tinyurl.com/y4wb3qwt.

Pandi Vijayakumar, Maria Azees, and Arputharaj Kannan. 2015. Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* 17, 4 (2015), 1015–1028. DOI: https://doi.org/10.1109/TITS.2015.2492981

Daisuke Wakabayashi. 2018. Uber's Self-Driving Cars Were Struggling Before Arizona Crash. Retrieved September 13, 2018 from http://tinyurl.com/y83sc39o.

Alicja Wakulicz-Deja and Małgorzata Przybyła-Kasperek. 2007. Hierarchical multi-agent system. *Stud. Inf.* 28, 4 (2007), 63–80.

Richard Waters and Tim Bradshaw. 2016. Rise of the Robots Is Sparking an Investment Boom. Retrieved May 26, 2018 from http://tinyurl.com/yymnbxrt.

Ben George Weber, Michael Mateas, and Arnav Jhala. 2012. Learning from demonstration for goal-driven autonomy. In *AAAI.*

David Welch and Keith Naughton. 2019. GM Falls Millions of Miles Short on Cruise Driving Projection. Retrieved February 26, 2019 from http://tinyurl.com/y5w4zpm7.

Darrell M. West. 2017. Securing the Future of Driverless Cars. Retrieved February 26, 2019 from https://www.brookings.edu/research/securing-the-future-of-driverless-cars/.

Earl L. Wiener and Renwick E. Curry. 1980. Flight-deck automation: Promises and problems. *Ergon.* 23, 10 (1980), 995–1011.
Norbert Wiener and Others. 1964. *God and Golem, Inc.*
Joe Williams. 2018. 2019 May Be Year of the Driverless Car: Here's Where Top Automakers Stand. Retrieved February 26, 2019 from http://tinyurl.com/yxgjhhrh.
Sadie Williamson. 2018. Blockchain May Be the Answer to Making Self Driving Cars Safer. Retrieved October 1, 2018 from http://tinyurl.com/y3xv467u.
Mark A. Wilson, James McMahon, Artur Wolek, David W. Aha, and Brian H. Houston. 2016. Toward goal reasoning for autonomous underwater vehicles: Responding to unexpected agents. In *Proceedings of Goal Reasoning: Papers from the IJCAI Workshop.*
Wenguo Liu Winfield and Alan F. T. 2010. Modeling and optimization of adaptive foraging in swarm robotic systems. *Int. J. Rob. Res.* 29, 14 (2010), 1743–1760. https://doi.org/10.1177/0278364910375139
Scott Wold and Paste Staff. 2015. The 100 Greatest Movie Robots of All Time. Retrieved March 04, 2018 from http://tinyurl.com/y3zbsxyk.
Kyle Hollins Wray, Luis Pineda, and Sholo Zilberstein. 2016. Hierarchical approach to transfer control in semi-autonomous systems. In *Proceedings of the 25th International Joint Conference on Artificial Intelligence.* 517–523. http://www.ijcai.org/Proceedings/16/Papers/080.pdf.
Guangyu Wu, Jian Sun, and Jie Chen. 2016. A survey on the security of cyber-physical systems. *Control Theory Technol.* 14, 1 (2016), 2–10.
Eray Yağdereli, Cemal Gemci, and A. Ziya Aktaş. 2015. A study on cyber-security of autonomous and unmanned vehicles. *J. Defense Model. Simul.* 12, 4 (2015), 369–381.
Andrew Ydenberg, Navtej Heir, and Bob Gill. 2018. Security, SDN, and VANET technology of driver-less cars. In *Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC).* IEEE, 313–316.
W. B. Yeats. 1933. The winding stairs and other poems. Reprinted by Kessinger Publishing.
Siew Yong, Dale Lindskog, Ron Ruhl, and Pavol Zavarsky. 2011. Risk mitigation strategies for mobile Wi-Fi robot toys from online pedophiles. In *2011 IEEE 3rd International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE 3rd International Conference on Social Computing (SocialCom).* IEEE, 1220–1223.
ZDNet. 2018. 15 of the Best Movies About AI, Ranked. Retrieved March 03, 2018 from https://tinyurl.com/yculsjxp.
Kim Zetter. 2014. Hospital Networks Are Leaking Data, Leaving Critical Devices Vulnerable. *WIRED.* Retrieved from http://tinyurl.com/y5kxsfol.
Ning Zhang, Shan Zhang, Peng Yang, Omar Alhussein, Weihua Zhuang, and Xuemin Sherman Shen. 2017. Software defined space-air-ground integrated vehicular networks: Challenges and solutions. *IEEE Commun. Mag.* 55, 7 (2017), 101–109.
Shlomo Zilberstein. 2010. Building strong semi-autonomous systems. Chaffins 2008 (2010), 1–20.

Received November 2018; revised April 2019; accepted May 2019