Security of Wireless Communication For Mobile Robot Networks: A Survey

Christopher Archibald, John Grogan, Daniel Rayborn, and Maxwell Young

***Abstract*—**

***Index Terms*—**

Max: What is the structure of this paper? Scope seems to large to ever get done; need to narrow focus. The general scope of this survey is wireless security with a focus on attacks in robot networks that are (1) "harder" to defend against than in more-established network settings, and (ii) new and specific to this domain. The structure of this survey breaks down into the following sections:

1) Introduction with short story/hook, statement of scope, some relevant statistics, points to other closely-related surveys and highlights differences/our contributions, organization of manuscript; aim for 1 page. Section 1 is a good start.
2) Brief review of well-established security threats/adversary goals/known defenses/terminology. Most of this should be pointers to other surveys/textbooks; no more than 2 pages. Section 2 and parts of Section 4 provide a good start to this.
3) Old attacks made worse in a new setting; aim for 4 pages.
   - Jamming; mobility
   - Sybil; again, mobility
   - Physical compromise; by their nature as semi-autonomous devices, can be captured.
   - Sensor data manipulation
   - Resource concerns; energy for computation is still concern for encryption, spectrum crowded.
4) New attacks specific to robot networks; aim for 3 pages
   - Robbing host's home.
   - Data privacy in the home/hijacked robot
   - Psychological attacks? (in our paper)
   - Operating system ROS vulnerabilities
   - Physical/real-world and anonymous attacks, rather than attacks on a network.

I. Introduction

Max: start with a story of a security threat that actually happened involving a robot network?

The increasing presence of wireless robot networks in everyday society exacerbates many traditional security challenges and introduces several new ones. While there is a general sentiment among academics and practitioners that securing these emerging networks is critical, no consensus exists on the best way to achieve this. Coupled with this, the physical nature of robots creates new concerns or exacerbates common vulnerabilities, making many security concerns unique and traditional solutions inadequate.

Here, we survey the literature on (i) security threats that arise from the use of wireless communication among networks of mobile robots, and (ii) state-of-the-art approaches to mitigating these threats. We highlight why attacks that are stymied in more-established wireless systems stubbornly remain a threat in the context of robot networks, and we report on a range of new vulnerabilities. Our investigation of the literature points to a domain that is currently experiencing growing pains as researchers work to address issues of security critical to the success of this increasingly popular network paradigm.

Max: please insert the citation and give more specific numbers here ***Resource shows a growing trend and expected continued growth of robot development and usage.

A. What is Robot?

While there is no single agreed-upon definition for ***robot***, we adopt one given by Murphy [], "~~an intelligent robot is~~ a mechanical creature which can function autonomously". To expand on the components of this definition further:

The terminology "mechanical creature" refers generally to the use of mechanical components as the building blocks for the ***robot form*** in contrast to biological components. Given the many applications where robots must interface with humans, this form is important; for example, resemblance to the human form is useful in therapy bots [] and search-and-rescue [46].

To "function autonomously" pertains to a robot's ability to perform operations with little to no human supervision and/or user input. This distinguishes a robot from, for example, a 1980s automotive; the latter being mobile, but requiring significant human administration to accomplish a task. There is some debate on the difference between *autonomous* versus *intelligent* agents, and we refer the reader to [] for a more nuanced discussion. In this survey, we confine our terminology to the use of *autonomous*.

Finally, implicit to our definition is "mobility". That is, a robot may change its location over time. The actual rate of change varies over different application domains.

Given this definition, we concede that there is plenty of room to debate the inclusion of many, for example, self-driving cars [] or modern-day fighter jets [], and we suspect no definition is free of such a gray area.

However, this definition is a helpful heuristic for delineating between robots and many other computing devices. It captures the general notions of a robot's ability to interact with the world and effect change with little oversight or guidance. For instance, how does a robotic emergency medical technician

(EMT) [] differ from a desktop computer? Approximation of the human form and mobility are clear separators. Additionally, the autonomy of the robotic EMT allows it to use a desktop computer instead of the reverse.

B. Our Scope: Wireless Security & Robots

Wireless communication has moved from a commodity to a necessity in modern infrastructures as it offers a level of flexibility and accessibility that wired communication does not. This is evidenced by the near-ubiquity of IEEE 802.11 (WiFi) networks, and the rapid growth of the Internet of Things (IoT) Max: insert text on stats here where many IoT devices communicate wirelessly. Mobility typically goes hand-in-hand with wireless communication, and while stationary robot have their uses, robot networks are likely to roughly follow the overall trend towards employing wireless communication.

Many of the challenges that face contemporary wireless networks will be pertinent to robot networks, such as sharing of a limited spectrum [], backwards compatibility with legacy standards [], impact of physical-layer effects on throughput and quality-of-service [], and many others. Each of these is a vast research domain, and our survey does not focus on these issues.

Similarly, the topic of wireless security is vast. Well-known issues such as confidentiality, data integrity, authentication, etc. apply to mobile robot networks as much as they do to other network paradigms. However, in this survey we focus on highlighting threats that are especially pertinent to robot networks. That is, we are interested in threats that are unique to, or greatly exacerbated by, robotic networks. For example:

- What are the implications of unsecured robot communication in XYZ industry? ...This paper [37] is useful in the intro. It coins the term ”cryptobotics” and says what a lack of security in robotics could do to various industries. It doesn't really say what to do about it all, but it helps answer the question ”why?” for this paper.
- Do robot networks make us more prone to attacks that leverage human psychology or social engineering?...This paper [11] says we over trust robots and gives an example experiment for this. It's more about psychology, but it's useful for the ”why” of this paper, I guess. This paper [27] talks about what privacy concerns that people (not just tech people) have concerning robots. Again, it can help with the ”why?” of this paper.
- Does the interface between robot networks and other emerging systems, such as IoT, pose new vulnerabilities? ...This paper [38] is here because it can help link IoT and robotic security/communication challenges, which will be useful later in the paper.

C. Layout of Our Survey

Our survey is structured into XYZ primary sections:

In each of these, secondary sections are used to summarize the associated literature. Finally, each subsection ends with a discussion of future work...

D. More Related Work

Existing First-Responder Systems. A ***land mobile radio (LMR) system*** is a narrowband wireless communications system that services mission-critical operations at the state or local level for police, firefighters, and emergency medical services in the USA [14]. The more recent ***First Responder Network Authority (FirstNet)*** is a nationwide broadband network meant to deliver high-speed data/video services for use by first responders [6].

Wireless Network Planning. A related challenge is wireless network planning which addresses how wireless devices should be deployed to provide good performance. Predictive planning allows for network design without requiring access the intended area of deployment; a blueprint of the terrain is sufficient for many commercial products: Ekahau [17], Aerohive Networks WiFi Planning Tool [2], TamoSoft Site Survey [49], and Netspot [39].

Other proposed solutions use a combination of optimization and measurement points [5], [10], [16], [26], [30], [31], [44], [44]. Additionally, genetic algorithms, simulated annealing, greedy heuristics have been proposed [23], [24], [29], [32], [42].

Sybil. Despite its introduction more than a decade-and-a-half ago, the Sybil attack [15] remains a challenging threat to permissionless systems. Robot networks, and mobile networks more generally, are especially vulnerable given that

II. General Security

A. CIAA

CIAA is an initialism that includes the original CIA triad and adds an extra letter. Fully enumerated: Confidentiality, Integrity, Availability, and *Authentication*. CIAA breaks security concerns into four distinct categories to aid in security assessment and discussion.

1) C - Confidentiality: The confidentiality of data and assets primarily refers to access control between data and users. I.e. who or what can or cannot access data or assets. Specifically, if data/assets are confidential, only the people who should see/use them can. Confidentiality is breached when someone views data/assets that they are not allowed to see. It is obvious to see how data is or is not confidential. Assets are a little more subtle. Assets include hardware and software. So, who cares if someone knows that they have 4 hard drives on the network or are running an Apache web server? It is important to be able to control who knows the existence of assets because knowledge of assets can give an attacker a leg up.

2) I - Integrity: Integrity of data and assets says that data/assets should be unmodified and assets should be functioning properly. Moreover, it also means that data should be correct and that assets take in and produce correct data (although this is outside of the scope of security). Integrity also determines who can modify data and assets. Obviously you only want certain people changing values in the database and pushing changes to your Git repository.

3) A - Availability: Availability of data and assets determines when said data/assets are ready to be seen/modified/used/etc. Data should be easily accessible by those who are allowed to see and hardware/software (such as web servers) need to also be available to people who are allowed to use it. For example, when I go to www.google.com, I expect to be able to search for anything via that service. If it unavailable, then I cannot use that service, rendering it useless. The same thing applies to data. If I cannot access my data, it is useless.

4) A - Authentication: This [33] paper discusses this.

Authentication is added to the original CIA triad for a variety of reasons. Generally, it allows a person to prove who they are. This is useful specifically for robot for reasons that will hopefully be clear later in this paper. It allows robots to verify that they are in fact a true user of the system that they are in and keeps the ones who are faking it out. This is very important because physical access to robots is almost impossible to prevent, making authentication essential.

Along with Authentication, some security theorists include non repudiation. This says that an action taken by an entity cannot be proved to not have happened. It is important to have with robots, although it is not usually considered. It is solved with digital signing, a form of asymmetric cryptography, which is computationally expensive. Since it is resource intensive, it is difficult to justify adding in to a robotic system, where resources are limited.

These properties do not control a system, rather, the system decides how to implement/control these aspects. For example, a system can implement digital signing to have non repudiation. However, if an entity is able to breach one of these aspects, that aspect is no longer present in the system and the system will need to be amended. Either way, these are important concepts to keep in mind throughout the paper, because all attacks break one or more of these aspects. How we prevent these attacks also goes back to this section.

B. Goals of Adversary

The goals of an adversary of a computer system can be widely varied. On a philosophical level, it is to break one or more of the previously mentioned aspects of security. Realistically speaking, the adversaries and attackers goal are more practical and concrete. This paper focuses on 3 broad categories: control of the system, impairment, and data access.

1) Control of the System: If an adversary is able to gain control of a system, s/he can do anything to it (e.g. change it, see all the information, shut it down, etc.). This is a total breach of the system and gives the adversary all the power over it. This breaks all aspects of CIAA. The large diversity of robotic system implementations creates a diverse outcome of impacts when a system is compromised. Robots ability to manipulate or interact with their physical surroundings makes compromised robots unique when compared to other systems. A robot may not only be a means for visual data compromise (by on board cameras) but the mobility of the robot as opposed to a stationary or fixed camera system makes data acquisition o

2) Impairment: An adversary is able to inhibit or prohibit parts or all of the system from functioning. This does not give the attacker as much power as control of the system, but s/he can control whether or not certain parts of the system are functioning. This mostly break availability, but can break integrity in certain situations.

3) Data Access: The adversary is able to see the data being transmitted through the system. This breaks confidentiality of the system. It is important to note that modern robots can contain data that traditional computers do not (such as a vacuum holding a rough layout of your house), making this very important for this paper.

Compromised robotic systems This paper has information on specific attacks possible against robotic networks. This section will be referred back to, saying which broad goal is accomplished by the breach.

C. Attack Vector

Not only is it important what is being attacked, it is important to look at what the attack is being used on (i.e., what its being carried out across). In terms of networking, this means we need to look at what layer the attack uses to carry out its mission. The network protocol stack has 5 layers (lowest to highest): physical, data link, network, transport, and application.

1) Physical Layer: The physical layer includes electricity on a wire or wave patterns in space. For wireless robotic networks, attacks carried out across the physical layer will involve cancelling out or overpowering wireless signals. It could technically include stealing robots from the field or accessing their physical ports, but that is out of the scope of this paper.

2) Data Link Layer: The data link layer is were protocols enter the picture. Ethernet and 802.11 act at this layer. Attacks at this layer will involve spoofing other machines or a form of denial of service (DOS).

3) Network Layer: IP is the dominant protocol of the network layer. Attacks at this layer could be DOS, spoofing, rerouting, Some attacks at this layer (and higher layers) are not specific to robotic networks.

4) Transport Layer: TCP and UDP are the predominant protocols at this layer. Operating system level attacks occur at this layer. Usually, attacks at this layer occur because of poor or nonexistant key management/security.

5) Application Layer: Application layer attacks do not have a real place in this paper because they are not specific to robotic security, rather general computer security.

III. Random Cites

Mobile Service robots [20]

Swarm robot challenges [22]

General security things about robots [53]

This paper [38] talks about the 5 main points of security as well WSN security challenges.

IV. WSN Attacks in a Mobile Robot Networks

(**Survey On Issues In Wireless Sensor Networks: Attacks and Countermeasures**) has a list of attacks on WSNs. Look here for what could be applicable.
This is an overview of specific network attacks that can occur in Mobile Robot Networks. These are different attacks that are extended from WSNs into this area of MRNs.

A. Jamming/DoS

Denial of Service (DoS) attacks aim to deny resources of a system to other potential users or operations. These attacks could be focused on any resource in order to degrade the functionality of that system. These are typically broken down into jamming and physical attacks.
(**Jamming techniques a survey**) mentions many different types of jammers and resolutions to jamming attacks. A noticeable amount of these resolutions involve detecting the jammer and recreating the network around the jammer. However for a static jammer and a mobile node, it makes sense for the node to just move away from the jammer. This is also known as a spatial retreat. This paper (**secure communication for mobile agents** *fix later*) explains the situation of jamming in multi-agent systems and offers a solution.
(**Denial of Service Attacks in Wireless Sensor Networks**) talks about DoS attacks at all the layers of the IP stack. Go into more detail about that.

B. Physical Compromise

Physical attacks in WSNs occur because the nodes are not strong enough physically to protect against the environment or malicious attackers. This makes it relatively simple for an attacker to tamper with one of the nodes. This can be anywhere from uploading code, destroying the node, replacing with malicious nodes, etc (**Survey On Issues In Wireless Sensor Networks: Attacks and Countermeasures**). *Find how this an example in Mobile robot networks*

C. Eavesdropping

Eavesdropping is an attack where an attacker views the content of any data that passes through a network. This breaks the confidentiality aspect of security.

D. Sybil

Sybil attacks occur when an attacker places a malicious node that portrays itself as having multiple identities. This is an attack on the redundancy mechanism in the WSN.

E. Sensor Manipulation

F. Resources

Exhaustion attacks

V. Attacks on Mobile Robot Networks

This section is an overview on attacks that are new to Mobile Robot Networks that do not show up in Wireless Sensor Networks.

A. Host Attacks

Possibly doesn't need to be here.

B. Psychological Attacks

Possibly doesn't need to be here. These would exist in Archibald's paper.

C. ROS Vulnerabilities

Security for the Robot Operating System has most of the information needed for this section.

D. Other Non-network Attacks

VI. Mitigations

The need for cyber security in robotic systems has gained more awareness as robot usage has increased in the industrial and commercial environments. Security concerns are amplified by the physical environment that robots often operate in as well as safety and security concerns associated with human-robot interactions [20]. As robotic systems attain more trust and usage within networks, they become an increasingly desirable target for malicious actors [4], [20]. Research focused on analysing cyber security concerns in robotic systems, mitigation techniques, and safe development practices is on the rise [33].

A. Securing Communications

B. Encryption Techniques

Communicating over an open wireless channel is not new, nor are the problems that come with it (such as sending secrets over that open channel). In order to have secure communications, people use encryption. Encryption is also not a novel solution (it predates digital computers). The novel problem in robotic networks is the limited power and computational (find a paper and cite this shit). Secondary solutions have been proposed that make encryption possible with limited resources and power. Daniel: Key Generation and resource utilization, how does memristors work with this

Packet encryption [3]

1) Memristors: A memristor is a hardware component that allows for generating session keys at the hardware level (as opposed to the software/application level) [1]. This is much faster and less expensive than software level key generation and is proven secure with the Scyther test [1].

2) Key management: One technique used it a protocol that allows each node (robot) in the network to store a minimal number of keys [18]. Other technique has a simplified key distribution mechanism for session keys [43]. This techique uses JTAG numbers for encrypting messages (and not TLS/SSL) making it compact and secure [19].

C. Physical Layer

D. Data Link Layer

E. Network Link

1) Q-IPSec: Q-IPSec is the combination of QoS (quality of service) and IPSec (internet protocol security) [25]. It has been expiermentally proven to provide the normal security with IPSec as well as the QoS necessary for teleoperation [25]. This could also be used in robotic or IoT systems, theoretically.

F. Transport

G. Frameworks

Robotic frameworks help designers and coders by abstracting complexities into more readily accessible constructs. The framework offers a simpler format for designers to work with, enabling implementation of complex behaviors, simulation, and testing, and a standardized code base. The robotic operating system (ROS) framework has proven itself a reliable tool for implementing and simulating robot designs. Updates to ROS have focused on securing the framework and end results of systems built utilizing ROS as a framework.

ROS secure comms [12]

This paper [33] discusses quite a few frameworks, including ROS and compares them with and without security stuff enabled. Also discusses the hardware abstraction layer (HAL).

This paper [47] was written when ROS did not have authentication for TCP comms. Either way, it looks at ROS and YARP, and it introduces a new framework that the author created.

1) Protocols: Communication protocols are important not just for the operation of the network. They lay the groundwork on which security (as well as other applications) are built. An efficient, effective, and robust protocol allows for security to be added in easily (or provides it inherently).

This paper [13] has information about many wireless standards, such as 802.11, Zigbee, Bluetooth, RFID, 2/3G, as well as others. The security discussion is in the context of IoT networks, which could be useful. However, I think the true value in the paper lies in the outlining of these protocols.

This paper [9] describes 802.11 and how to attack it. It also provides a checklist of things to do in order to test basic security of your robot network (though it does not provide a security framework for use).

This paper [51] provides a Robotic Wireless Mesh Protocol (RWMP) for an 802.11 robotic network (although it doesn't follow the IEEE 802.11 routing standards and whatnot). Using NS3, they ran experiments (simulating deployed robots, not just stationary nodes) and claim that their protocol outperforms the conventional protocol.

This paper [35] talks about using directional antennas (off the shelf) for long range reliable comms. It's not exactly security, but it is robotic communication. Maybe this should be placed elsewhere.

This paper [50] introduces a multihop routing algorithm based on RT-WMP but with better bandwidth guarantees and lower power comsumption. They actually set it up (in ROS, I believe) and ran expirements in the real world. Also, in their abstract, they claim that centralized routing is a no-go in robot networks. They say that most of time, the upper levels of the protocol stack are relied upon, and these don't handle robot networks well.

H. Attack Detection

Instead of simply preventing every attack, another way to protect a system is to detect on going attacks and taking action to mitigate or stop said attack. This section will cover a few methods for detecting attacks.

1) Physical Wireless Signals: The Sybil attack is carried out by one robot spoofing the identities of multiple robots (i.e. it's pretending to be more than one robot). One way to prevent this is to use the physics of wireless signals to detect whether or not a single robot is pretending to be multiple robots (this can be used for replay attacks as well) [21].

2) Decision Tree IDS: An internal detection system (IDS) is used for detecting attacks in an internal network. Generally, this is too resource intensive for a robotic network. One way to fix this is to simplify it by making a simple decision tree based IDS [52]. This has been experimentally proven to be able to detect DoS and command injection attacks [52].

3) Sybil/DDoS detection: This paper [8] discussed a way to detect Sybil and DDoS attacks in a mobile robot network. It does not describe how to prevent or mitigate these attacks, but is does say that looking at violations in the network logic is key to detecting them. It also says that the protocol used is irrelevant because it looks at network logic. Also, it claims that attacks on robot networks need not be distributed, rather "rapid and intensive." This is because a distributed attack takes a lot of time and energy (I believe is what its saying, read the conclusion, 2nd bullet point) and robot networks operate for a limited amount of time.

VII. Random Cites

Packet encryption [3]
ROS secure comms [12]
2 factor auth [34]
Straight mitigation [41]
WSN threat detection (mothon) [28]
Controllable communication frequencies as an attack mitigation [40]
Mobile robot control group security protocol [7]

This paper talks about a non coordinated attack on a WSN anchor nodes. Most people will "prune the nods from the network, but this paper is saying dont do that. Really its saying dont let it get to that point. I'm trying to figure out where to put this [36]

antenna selection algorithm that is divided intro subproblems. Talks too much about cellular stuff. [45]

This paper [48] discusses using blockchain to verify the correctness of data/communications, whatever. They did not implement it in the real world, and don't know what would happen if the network sucked. Also, they noted blockchain packet use a whole lot more data (160 bytes vs 4 bytes) than

a classical approach that they examined. This could a useful example of going overboard, maybe?

VIII. Introduction

IX. Conclusion

Acknowledgment

References

[1] H. Abunahla, D. Shehada, C. Y. Yeun, B. Mohammad, and T. Stouraitis. A novel secure conference communication in iot devices based on memristors. In *2017 24th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, pages 58–61, Dec 2017.

[2] Aerohive. Wi-Fi planning tool, 2018. www.aerohive.com/planner/.

[3] Saad Al-Azzam, Ahmad Sharieh, Azzam Sleit, and Nedaa Al-Azzam. Securing robot communication using packet encryption distribution. *Network Security*, 2018(2):8 – 14, 2018.

[4] Christopher Archibald, Luke Schwalm, and John E. Ball. A survey of security in robotic systems: Vulnerabilities, attacks, and solutions. *I. J. Robotics and Automation*, 32, 2017.

[5] Leena Arya, S.C. Sharma, and Millie Pant. Performance analysis of indoor positioning system. *International Journal of Advanced Computer Science and Applications*, 1(4), 2010.

[6] First Responder Network Authority. Firstnet:, 2018. https://firstnet.gov/.

[7] Alexander Basan, Elena Basan, and Oleg Makarevich. Analysis of ways to secure group control for autonomous mobile robots. In *Proceedings of the 10th International Conference on Security of Information and Networks*, SIN '17, pages 134–139, New York, NY, USA, 2017. ACM.

[8] E. Basan, A. Basan, and O. Makarevich. Evaluating and detecting internal attacks in a mobile robotic network. In *2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pages 516–5168, Oct 2018.

[9] Elena Basan, Oleg Makarevich, and Andrew Stepenkin. Development of the methodology for testing the security of group management system for mobile robots. In *Proceedings of the 11th International Conference on Security of Information and Networks*, SIN '18, pages 27:1–27:2, New York, NY, USA, 2018. ACM.

[10] Roberto Battiti, Mauro Brunato, and Andrea Delai. Optimal wireless access point placement for location-dependent services. 2003.

[11] Serena Booth, James Tompkin, Hanspeter Pfister, Jim Waldo, Krzysztof Gajos, and Radhika Nagpal. Piggybacking robots: Human-robot overtrust in university dormitory security. In *Proceedings of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*, HRI '17, pages 426–434, New York, NY, USA, 2017. ACM.

[12] Benjamin Breiling, Bernhard Dieber, and Peter Schartner. Secure communication for the robot operating system. 04 2017.

[13] A. Burg, A. Chattopadhyay, and K. Lam. Wireless communication and security issues for cyberphysical systems and the internet-of-things. *Proceedings of the IEEE*, 106(1):38–60, Jan 2018.

[14] Federal Communications Commission. Private land mobile radio services, 2018. https://www.fcc.gov/wireless/bureau-divisions/mobility-division/private-land-mobile-radio-services.

[15] John Douceur. The Sybil Attack. In *Proceedings of the Second International Peer-to-Peer Symposium (IPTPS)*, pages 251–260, 2002.

[16] A. Eisenblatter, H.-F. Geerdes, and I. Siomina. Integrated access point placement and channel assignment for wireless LANs in an indoor office environment. In *2007 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WOWMOM*, number 2007 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WOWMOM, 2007.

[17] Ekahau. Wireless design, 2018. www.ekahau.com.

[18] W. Elgenaidi, T. Newe, E. O'Connell, D. Toal, G. Dooly, and J. Coleman. Memory storage administration of security encryption keys for line topology in maritime wireless sensor networks. In *2016 10th International Conference on Sensing Technology (ICST)*, pages 1–4, Nov 2016.

[19] Ahmad Fayed Evangelos A. Yfantis. Authentication and secure robot communication. 06 2015.

[20] Nico Hochgeschwender Miguel A. Olivares-Mendez Paulo Esteves-Verissimo Marcus Volp Holger Voos Gary Cornelius, Patrice Caire. A perspective of security for mobile service robots. 2017.

[21] Stephanie Gil, Swarun Kumar, Mark Mazumder, Dina Katabi, and Daniela Rus. Guaranteeing spoof-resilient multi-robot networks. *Auton. Robots*, 41:1383–1400, 2017.

[22] Fiona Higgins, Allan Tomlinson, and Keith M. Martin. Survey on security challenges for swarm robotics. *2009 Fifth International Conference on Autonomic and Autonomous Systems*, pages 307–312, 2009.

[23] Árpád Huszák, Győző Gódor, and Károly Farkas. Investigation of WLAN access point placement for indoor positioning. In Róbert Szabó and Attila Vidács, editors, *Information and Communication Technologies*, pages 350–361, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[24] Zhong Ji, T. K. Sarkar, and Bin-Hong Li. Methods for optimizing the location of base stations for indoor wireless communications. *IEEE Transactions on Antennas and Propagation*, 50(10):1481–1483, 2002.

[25] Anas Abou El Kalam, Antoine Ferreira, and Frédéric Kratz. Bilateral teleoperation system using qos and secure communication networks for telemedicine applications. *IEEE Systems Journal*, 10:709–720, 2016.

[26] M. Kamenetsky and M. Unbehaun. Coverage Planning for outdoor wireless LAN systems. In *INTERNATIONAL ZURICH SEMINAR ON BROADBAND COMMUNICATIONS*, page 49, 2002.

[27] M. M. Krupp, M. Rueben, C. M. Grimm, and W. D. Smart. A focus group study of privacy concerns about telepresence robots. In *2017 26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)*, pages 1451–1458, Aug 2017.

[28] K. Lasota, P. Bazydo, and A. Kozakiewicz. Mobile platform for threat monitoring in wireless sensor networks. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 106–110, Dec 2016.

[29] Seungseob Lee, SuKyoung Lee, Kyungsoo Kim, and Yoon Hyuk Kim. Base station placement algorithm for large-scale lte heterogeneous networks. *PLOS ONE*, 10:1–19, 10 2015.

[30] Y. Lin, W. Yu, and Y. Lostanlen. Optimization of wireless access point placement in realistic urban heterogeneous networks. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 4963–4968, 2012.

[31] Y. Lin, W. Yu, and Y. Lostanlen. Optimization of wireless access point placement in realistic urban heterogeneous networks. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 4963–4968, 2012.

[32] K. Maksuriwong, V. Varavithya, and N. Chaiyaratana. Wireless LAN access point placement using a multi-objective genetic algorithm. In *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, volume 2, pages 1944–1949, 2003.

[33] Francisco Martn, Enrique Soriano-Salvador, and Jos Plaza. Quantitative analysis of security in distributed robotic frameworks. *Robotics and Autonomous Systems*, 100, 11 2017.

[34] D. Miglani and A. Hensman. Vision for secure home robots: Implementation of two-factor authentication. In *2015 IEEE International Symposium on Technology and Society (ISTAS)*, pages 1–4, Nov 2015.

[35] B. Min, E. T. Matson, and B. Khaday. Design of a networked robotic system capable of enhancing wireless communication capabilities. In *2013 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)*, pages 1–8, Oct 2013.

[36] M. Mofarreh-Bonab, M. Mofarreh-Bonab, and S. A. Ghorashi. The effect of pruning stage in secure localization in wireless sensor networks. In *6th International Symposium on Telecommunications (IST)*, pages 455–458, Nov 2012.

[37] Santiago Morante, Juan G. Victores, and Carlos Balaguer. Cryptobotics: Why robots need cyber safety. *Front. Robotics and AI*, 2015, 2015.

[38] B. Mostefa and G. Abdelkader. A survey of wireless sensor network security in the context of internet of things. In *2017 4th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, pages 1–8, Dec 2017.

[39] NetSpot. Wi-fi site surveys, analysis, troubleshooting, 2018. www.netspotapp.com.

[40] S. Park, S. Kim, D. D. Cho, S. Jang, J. sung, and S. Kim. Multi-robot path finding testbed in wireless networks against malicious attacks. In *2018 18th International Conference on Control, Automation and Systems (ICCAS)*, pages 120–123, Oct 2018.

[41] Ishaani Priyadarshini. *Detecting and Mitigating Robotic Cyber Security Risks*, pages 333–. 03 2017.

[42] N. F. Puspitasari, H. A. Fatta, and F. W. Wibowo. Implementation of greedy and simulated annealing algorithms for wireless access point placement. In *2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS)*, pages 165–170, 2015.

[43] Yunchuan Qin and Qi Xiao. Polynomial-based key management scheme for robotic system. In *Proceedings of the 8th International Conference on Computer Modeling and Simulation*, ICCMS '17, pages 105–108, New York, NY, USA, 2017. ACM.

[44] S. Sendra, J. Lloret, C. Turro, and J.M. Aguiar. IEEE 802.11a/b/g/n short-scale indoor wireless sensor placement. *International Journal of Ad Hoc and Ubiquitous Computing*, 15(1-3):68–82, 2014.

[45] S. Sheikhzadeh, M. R. Javan, and N. Mokari. Antenna selection for secure robust communication in miso-ofdma based heterogeneous cellular networks. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, April 2018.

[46] S. Shin, D. Yoon, H. Song, B. Kim, and J. Han. Communication system of a segmented rescue robot utilizing socket programming and ros. In *2017 14th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*, pages 565–569, June 2017.

[47] Oleksandr Shyvakov. Developing a security framework for robots. 08 2017.

[48] Volker Strobel, Eduardo Castelló Ferrer, and Marco Dorigo. Managing byzantine robots via blockchain technology in a swarm robotics collective decision making scenario. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, AAMAS '18, pages 541–549, Richland, SC, 2018. International Foundation for Autonomous Agents and Multiagent Systems.

[49] Tamosoft. Tamograph site survey, 2018. www.tamos.com/products/wifi-site-survey/.

[50] D. Tardioli. A wireless communication protocol for distributed robotics applications. In *2014 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC)*, pages 253–260, May 2014.

[51] Nikita Trivedi, Bighnaraj Panigrahi, Hemant Kumar Rath, and Arpan Pal. Wireless mesh routing for indoor robotic communications. In *Proceedings of the 1st International Workshop on Internet of People, Assistive Robots and Things*, IoPARTS'18, pages 25–30, New York, NY, USA, 2018. ACM.

[52] T. P. Vuong, G. Loukas, D. Gan, and A. Bezemskij. Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. In *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6, Nov 2015.

[53] Khalil M. Ahmad Yousef, Anas AlMajali, Salah Abu Ghalyon, Waleed Dweik, and Bassam Jamil Mohd. Analyzing cyber-physical threats on robotic platforms . In *Sensors*, 2018.