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 [53].

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 [43] 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 [14] 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 [32] 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 [44] 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 [18]. 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 [7].

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 [22], Aerohive Networks WiFi Planning Tool [2], TamoSoft Site Survey [56], and Netspot [45].

Other proposed solutions use a combination of optimization and measurement points [6], [11], [21], [31], [35], [36], [51], [51]. Additionally, genetic algorithms, simulated annealing, greedy heuristics have been proposed [28], [29], [34], [37], [49].

Sybil. Despite its introduction more than a decade-and-a-half ago, the Sybil attack [20] 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 one of the main approaches to security classifications utilized by cybersecurity experts and we will be using it for classification purposes. Fully enumerated CIAA stands for confidentiality, integrity, availability, and authentication. This classification system allows security concerns to be broken into four distinct categories to aid in security assessment and discussion.

1) C - Confidentiality: Maintaining the confidentiality of data and assets primarily refers to maintaining access control between data and users. Specifically, this idea has to do with ensuring that only select users can access data or assets that they should and is considered breached when non-authorized users can view or gain access. Data includes items such as network packets or other items of a digital nature that the system gather, process, and possibly save. Assets items include hardware and specific software structures that the system is using to process data and complete other tasks. For both of these items confidentiality is highly important as having unauthorized access to either or both creates the possibility for compromised systems and abuse.

2) I - Integrity: Integrity of data and assets means ensuring that the items maintain a level of ability to detect when modifications have been made and/or prevented. For many systems data integrity is the largest concern as the data that is being processed and having decisions made upon should be as correct as possible and that the system should be able to determine if the data appears to be altered though either

data corruption or by a malicious actor. For a robotic system concerns of asset integrity is necessary as well as physical access to the robot is possible in many cases and thus the robot must be able to detect and be confident in it's asset's ability to function within expectations.

3) A - Availability: Maintaining the availability of data and assets means that these resources are accessible to the authorized users when requested. This idea can be at odds with confidentiality because to make the items more available inherently reduces the items confidentiality. Thus it is important to maintain a balance between the two items as the proper users should be able to access the items otherwise the data or asset can be rendered useless.

4) A - Authentication: This [38] paper discusses this.

Authentication is the most recently added letter to the CIAA triad but for good reason. In the most broad sense authentication requires that a user prove that they have the proper credentials to access data or assets and can be used as one way to prevent breaches too confidentiality and ensure that the data is available to those that require access. For robots the idea of authentication can be incredibly important as physical access to the robot can be difficult to prevent and thus authentication methods have to be put in place to prevent tampering.

Along with authentication, some security theorists include non-repudiation. This is typically defined as any method which can be used to prove that an action was taken by a specific user. The most common implementation of this involves using digital signing, a form of asymmetric cryptography, but this can be computationally expensive. For robotic systems having some form of non-repudiation can be important depending on the tasks attempting to be accomplished but due to its more resource intensive nature, it can be difficult to justify adding it to systems where typically resources are limited.

It is important to note that these properties do not control system design, but rather, these are aspects of good system design. Any secure system will have all of these principles included in some form or another, however by simply being present it does not mean that a system is infallible. Many consideration will have to be made at many levels of a robotic network to build a secure system as many attacks will attempt to break at least one of major aspects of CIAA along a specific attack vector.

B. Goals of Adversary

The goals of an adversary to a computer system can be widely varied. On a philosophical level, it is to break one or more of the aspects of CIAA, but realistically speaking these goals are typically more practical and concrete. For a mobile robotic network these goals could include things such as intercepting and/or spoofing transmissions, attempting to remove a robot from the network either physically or through software, attempt to take control of a robot, etc. All of these goals are different in their end result, likely attack vectors, and motivations thus can be typically broken into three broad categories of controlling the system, impairment, and data access that will be covered in this paper.

1) Control of the System: If an adversary is able to gain control of a robotic system, they are capable of making any changes or view any of the data flowing through the network and typically breaks every aspect of CIAA. Due to the nature of this breach, if successful, the adversary gains full control over every aspect of the system or individual robot and create a large variety of consequences. Since robots are capable of interacting and possibly manipulating the physical environment around them, compromised robots can cause an innumerable number of effects. These can range from destruction of their local environment and possible even themselves but also the possible endangerment of human health and safety.

2) Impairment: Another possible goal is just to inhibit or prohibit parts or all of the system from functioning. This is different from control over the system as the attacker may only be able to prevent one specific subsystem from functioning as expected instead of being able to change the expected behavior. In terms of the CIAA this typically breaks the availability and possibly integrity aspect.

3) Data Access: The last area of possible adversarial goals is to gain the ability to intercept and read data being sent through the system. While this is an issue across any computing system, robotic systems in particular carry a larger operational risk in being susceptible to this kind of goal as they have the potential to hold more at-risk data. Examples of this include items such as maps of buildings, operational meta-data about a user's schedule, and other data about the physical environment that can be useful to a malicious user.

C. Attack Vector

With the goals established, it is also important to examine the various methods an attack will be carried out on. For the purpose of this paper attack vectors will be broken into two categories, networking attacks and non-networking attacks. For networking attacks the network protocol stack can be used to broadly classify attacks across the five layers which include the physical, data link, network, transport, and application layer. The non-networking attacks will include the categories of physical tampering and system-level exploits.

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 canceling out or overpowering wireless signals.

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, a form of denial of service (DOS), or jamming by taking advantage of the 802.11 protocol's faults.

3) Network Layer: The Internet Protocol (IP) is the dominant protocol of the network layer. Some examples of this attack at this layer could be DOS, spoofing, or malicious rerouting. Typically attacks at this layer and the following are not specific to robotic networks, but still stand as a threat to them.

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 nonexistent key management/security.

5) Application Layer: While this is a layer on the network protocol stack most attacks focused on this layer are covered under system-level exploits. This is because while a majority of these attacks are carried out over a network the actual fault being exploited is typically within the application itself.

III. Specific Attacks

A. DoS/Jamming

how did you run your code

Denial of Service

1) Physical: A Denial of Service attack (DoS) can be implemented via numerous methods depending on the platform of attack and affects accessibility via interruption. At the physical layer filling the communication medium with transmissions can be enough to negatively affect or even inhibit communication. Wireless systems do not utilize a physically conductive medium and often rely on broadcasting messages [17]. This property makes the physical layer wireless systems particularly susceptible to DoS attacks. where a physical cable forces one to have direct access to it in order implement an attack, the broadcast nature of wireless alleviates this problem for potential attackers [47]. Wireless DoS attacks generally can often be accomplished with simple equipment and little effort [47]. Physical layer DoS attacks are hard to prevent or handle without assistance from applications or users outside of the network infrastructure. An intrusion detection system may notice a Dos attack is occurring but there are little automated solutions to stop an in progress attack. For wireless DoS attacks triangulation may be used to pinpoint the source of malicious signals. Primary mitigation often occurs with designing robots to handle situations in which signal is lost or in other words to fail gracefully.

Because this attack affects the hardware or physical layer that Robots utilize for communication, proven successful attacks or proof of concepts that work on the specified hardware can be expected to be effective against the robots reliant on this hardware and be as or more detrimental in outcome. The same holds true for many of the attacks discussed in this paper.

802.11-Queensland attack The Queensland attack exploits the requirement of networks utilizing 802.11b to have a clear channel assessment before sending or receiving data. This function tests the wireless medium in order to determine if it is already in use so as to prevent sending a signal over another machine. the Queensland attack also known as the clear channel assessment attack achieves a DoS of 802.11b wireless networks by spoofing a constant signal that informs machines inquiring about clear channel assessment that the network currently being used. Because the machines will not communicate until given the all clear this effectively stops communication on the network.

2) Data Link: Layered model against encryption

3) Network: Fraggle Ping Flood Ping flood works by exploiting the natural function of ICMP echo requests to fill the bandwidth of a machine with request packets that will respond back to the address of the targeted machine. The subsequent ”flood” of reply packets can be quite effective at consuming enough bandwidth to DoS the desired client. The Ping command itself is not malicious and is generally included in most networked applications/systems in order to test connectivity and gather data on round trip time of requests. The response nature of ping makes the function exploitable in a pseudo bot-net fashion, turning the power of the collected systems of a network against an individual targeted machine in order to overwhelm its communication limits. An IP address of the target or some specific name that resolves to the target is required as well as a system that has multiple machines that use ping or a similar program with similar functionality in order to launch a successful attack. Smurf

Fraggle and Smurf attacks work on the same principal as ping floods.

The paper [60] has a bit of information of DoS attacks on different levels, mostly with regards to the PeopleBot. Specifically, it mentions the de auth attack and the IPv6 Router Advertisement (RA) attack. They both accomplish a DoS.

B. Eavesdropping

Eavesdropping like DoS is made simpler for attackers by the medium of wireless communication. Unless signals are beamed or formed the attacker can position themselves within the radius of the broadcast signal. This problem becomes compounded when individual robots acts as relays or communication nodes as the wireless network coverage area becomes larger. The primary goal of eavesdropping is to gain access to communications, with a secondary goal of doing so without being detected. Even if collected transmissions are encrypted details about the network or information being sent may still be available and useful in setting up other malicious behaviors.

C. Man in the Middle

Man in the Middle (MitM) attacks focus on gaining or spoofing a level of trust on a network in order act as a ”middle” man between communicating nodes. The MitM client acts a sort of proxy for communication giving it access to communication often even if encrypted. Furthermore MitM clients can inject and send malicious transmissions that appear to come from legitimate sources. MitM often starts with sniffing for network communication or eavesdropping for a communication system to compromise. After successfully compromising a network, MitM attacks often give attackers the ability to sniff for more traffic, access connected networks, manipulate transmission content (including sending malicious traffic), hijack sessions, and view encrypted transmissions. Wireless systems (specifically those with mobile or roaming nodes) are at an increased susceptibility due to range limitations. Often the MitM client will have to compete with the original signal, but if two nodes are out of range of each other the MitM client may be situated within range of them both preventing the need to compete with the original signal. Robots are often designed

to inherently trust communication and malicious actors my move without notice.

This paper [12] breaks down MitM stuff a bit and mentions the Raven II as an example of a MitM attack.

This paper [61] lists pseudocode for a MitM attack. It also talks about various other attacks, which could be useful to back up other specific attacks.

D. Sybil

[26] "In a Sybil attack a malicious agent generates (or spoofs) a large number of false identities to gain a disproportionate influence in the network. These attacks are notoriously easy to implement (Sheng et al. 2008) and can be detrimental to multi-robot networks." "This is because many characteristics unique to robotic networks make security more challenging; for example, traditional key passing or cryptographic authentication is difficult to maintain due to the highly dynamic and distributed nature of multi-robot teams where clients often enter and exit the network."

Sybil attacks specifically target multiple agent/node systems or networks, by spoofing multiple fake clients. A single malicious client may fake a large number of fake clients in order to gain various control or influence of the targeted network. "Douceur proves several results showing that without a centralized authority, Sybil attacks are always possible for any practical distributed network."

The vulnerabilities of multi-node systems to Sybil attacks is compounded when the mobility of robots is accounted for.

demonstrates a successful proof of concept of Sybil attacks against a mobile robot cluster.

This paper [8] also mentions Sybil, amongst other attacks. This paper [9] (different from the previous paper mentioned) mentions Sybil and DDoS on mobile robot networks.

E. Encryption Cracking

Limited resources may force robots (especially older systems or budget devices) to utilize less secure cryptographic methods. The mobile nature and inherent need for trust required of many robot implementations make it difficult to effectively implement defenses or mitigations implemented in static configurations

F. Unauthenticated TCP Port

This paper, [40], makes the point that if a TCP port doesn't require authentication (eg, SSH), then commands can be remotely executed on a robot.

G. Raven II

The Raven II is a teleoperated surgical robot. Bonaci et al. performed manipulation, modification, and hijacking attacks on this machine with the intent to expose the lack of security in robotics [13]. They were successful in breaching security; however they claimed it would be extremely easy to prevent the attacks the performed (both easy to implement and computationally easy) [13].

H. Mobile Service Robots

The paper, [25], is interesting because it outlines the security issues with mobile service robot (ie, robots that are used in the home and move around). The attackers motive are broken down into 2 categories: data theft (specifically sensor data, which is unique to robots) and destruction of environment. The attack vectors are broken down into 4 categories, each with specific kinds of attacks: attacks on sensor data, hardware, software, and infrastructure.

This paper, [19], is a little older but has interesting things. It mentions robotic vandalism, spying with robots (specifically with a Rovio robot), and even psychological attacks. Spying is important to talk about because robots are used differently than standard computers and therfore have different data.

I. Deauthentication

This paper describes IJam, a death tool that they created [3]. It was created for WiFi networks, but could be used for robot networks that use WiFi as they medium of communication.

IV. Random Cites

Sybil and spoof resilience [26]

Does have a section describing different attacks (maybe better in gen security) [30]

This paper lists attacks on IoT WSNs [44]. It also has counter measure for various attacks, useful in mitigations (though not there yet).

V. 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 [25]. As robotic systems attain more trust and usage within networks, they become an increasingly desirable target for malicious actors [5], [25]. Research focused on analysing cyber security concerns in robotic systems, mitigation techniques, and safe development practices is on the rise [38].

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 [4]

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 [23]. Other technique has a simplified key distribution mechanism for session keys [50]. This techique uses JTAG numbers for encrypting messages (and not TLS/SSL) making it compact and secure [24].

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) [30]. It has been expirementally proven to provide the normal security with IPSec as well as the QoS necessary for teleoperation [30]. 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 [15]

This paper [38] 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 [54] 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 [16] 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 [10] 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 [58] 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 [41] 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 [57] 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) [26].

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 [59]. This has been experimentally proven to be able to detect DoS and command injection attacks [59].

3) Sybil/DDoS detection: This paper [9] 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.

VI. Random Cites

Packet encryption [4]
ROS secure comms [15]
2 factor auth [39]
Straight mitigation [48]
WSN threat detection (mothon) [33]
Controllable communication frequencies as an attack mitigation [46]

Mobile robot control group security protocol [8]

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 [42]

antenna selection algorithm that is divided intro subproblems. Talks too much about cellular stuff. [52]

This paper [55] 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?

VII. Introduction

VIII. 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] Haitham Al-Ani and Ahmed Al-Zubidy. Introducing ijam wireless deauthentication attack tool. In *Proceedings of the SouthEast Conference*, ACM SE '17, pages 199–202, New York, NY, USA, 2017. ACM.

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] 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.

[10] 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.

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

[12] T. Bonaci and H. J. Chizeck. On potential security threats against rescue robotic systems. In *2012 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)*, pages 1–2, Nov 2012.

[13] Tamara Bonaci, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. *CoRR*, abs/1504.04339, 2015.

[14] 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.

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

[16] 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.

[17] zge Cepheli and Gunes Karabulut Kurt. Physical layer security in wireless communication networks. pages 61–81, 01 2013.

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

[19] Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua R. Smith, and Tadayoshi Kohno. A spotlight on security and privacy risks with future household robots: Attacks and lessons. In *Proceedings of the 11th International Conference on Ubiquitous Computing*, UbiComp '09, pages 105–114, New York, NY, USA, 2009. ACM.

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

[21] 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.

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

[23] 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.

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

[25] 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.

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

[27] 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.

[28] 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.

[29] 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.

[30] 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.

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

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

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

[39] 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.

[40] Justin Miller, Andrew B. Williams, and Debbie Perouli. A case study on the cybersecurity of social robots. In *Companion of the 2018 ACM/IEEE International Conference on Human-Robot Interaction*, HRI '18, pages 195–196, New York, NY, USA, 2018. ACM.

[41] 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.

[42] 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.

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

[44] 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.

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

[46] 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.

[47] Konstantinos Pelechrinis, Marios Iliofotou, and Srikanth V. Krishnamurthy. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *To appear in IEEE Communications Surveys & Tutorials*, 2011.

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

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

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

[55] 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.

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

[57] 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.

[58] 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.

[59] 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.

[60] K. M. A. Yousef, A. AlMajali, R. Hasan, W. Dweik, and B. Mohd. Security risk assessment of the peoplebot mobile robot research platform. In *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, pages 1–5, Nov 2017.

[61] 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.