Mobile Robots: An Overview of Data and Security

Esmeralda Kadena[1], Nguyen Huu Phuoc Dai[2] and Lourdes Ruiz[3]
Doctoral School on Safety and Security Sciences, Óbuda University, Budapest, Hungary

Keywords: Collection, Communication, Data, Mobile Robots, Security.

Abstract: The field of mobile robotics has become the focus of several types of research for many years. The revolutionary technology of Wireless Sensor Networks (WSNs) has provided many benefits for the process of data collection and communication. On the other hand, the network is facing challenges in supporting the traffic requirements to carry on the data flow generated by the nodes. Hence, the focus of this work is to give an overview of data processes in mobile robots based on the literature review. At first, we present the definitions and the most common types of mobile robots. Then, we emphasize the role of sensors and sensor nodes in WSNs for gathering and communicating the data. In the fourth section, we extend this work by introducing the main security issues posed to data in mobile robots. Our conclusions are drawn in the end. As this paper generally describes and points out the main problems related to data in mobile robots, further analysis is planned for future work.

1 INTRODUCTION TO MOBILE ROBOTS

Mobile robots are robots that can move from one place to another place automatically without any external human assistance. They can be classified as:

- Land-based: wheeled robot, tracked robot, legged robot, manipulator robot;
- Air-based: plane, helicopter, quadcopter, drones;
- Water-based: boat, submarine, hybrid, or stationary robot (arm/manipulator robot) (Rasam, 2016),
- Space-based: Robonaut 1&2, Valkyrie (Elizabeth Howell, 2017).

Mobile robots offer several benefits such as working 24/7, accuracy and consistency, working in harsh environments like in industrial, medical, and space environment, and job creation (Rachel, 2018). However, they also have some drawbacks like power supply, implementing, deploying, maintaining and repairing costs. They are not intelligent as a human, dependency on robots, unemployment, and human fears of robots (Heba Soffar, 2016). This paper briefly describes data processing and communication in mobile robots via a meta-analysis of literature reviews. Moreover, the role of the robot's sensors and sensor nodes in WSNs to collect information, challenges and solutions are emphasized and discussed. Furthermore, several security issues of robot's data transmission are also indicated to draw users' attention and increase their security awareness.

2 DATA COLLECTION

Data collection is the process of data gathering from one or more points for using them at more points (Weik, 2001). Data can be gathered from different network stations to process them on a computer or at a central location.

In the traditional form, data were collected manually. Such a process has been considered time-consuming, too long, and the generated data were limited as well (Swartz et al., 2012). Due to technological advancements, the process of data collection has made significant progress. The development, installation, and integration of wired and wireless sensors into different kinds of systems, has provided better results.

[1] https://orcid.org/0000-0002-3808-6909
[2] https://orcid.org/0000-0003-1523-0856
[3] https://orcid.org/0000-0002-3649-6226

Kadena, E., Huu Phuoc Dai, N. and Ruiz, L.
Mobile Robots: An Overview of Data and Security.
DOI: 10.5220/0010174602910299
In *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021)*, pages 291-299
ISBN: 978-989-758-491-6

Wireless Sensor Networks (WSNs) monitor and communicate the conditions and features of a physical environment (i.e., acoustic, visual, vibration, motion, radio, magnetic, heat, light, biological) (Canli & Khokhar, 2009). Data acquisition and dissemination protocols in WSNs aim to collect information from sensor nodes and to forward it then to the subscribing entities. As a result, the data rate is achieved while maximizing the lifetime of the overall network. The gathered information can be data raw or processed by using typical signal processing techniques (i.e., filtering, aggregation, event detection.). During the navigation of ambient data, a mobile robot follows the steps shown below (Figure 1):

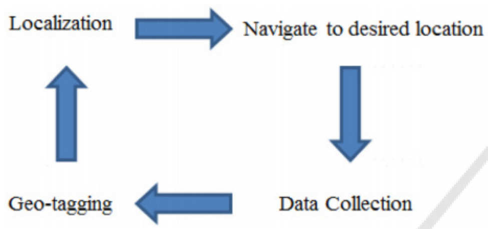

Figure 1: Steps for data collection in mobile robots (Mantha et al., 2018).

2.1 Sensors

As mobile robots are assigned for several types of applications, an essential element to achieve their primary purpose is sensor-guidance (Drunk, 1988). Sensors used in mobile robots are classified based on their tasks and working principles.

2.1.1 Navigation Sensors

Navigation is the process of determining and controlling the position, direction, and speed and movements of a robot from one point to another without considering the obstacles (Lobo et al., 2005). The sensors for navigation are categorized as internal and external. In external navigation, the most commonly used sensors are as below.

Laser Range Finders: a sensor used for determining the distance to an object by using a laser beam (Eric, 2020). Usually, this technique does not provide high precision measurements. Thus, it is replaced by triangulation and similar techniques.

GPS (Global Positioning System): provides information about latitude, longitude, and altitude (Xu & Xu, 2016). GPS can be used for static, kinematic, relative, and multi-receiver positioning. Some authors have found some problems related to the use of GPS in mobile robots such as the signal can be blocked periodically because of foliage and steep terrain, multi-path interference, and insufficient position accuracy (Hofmann-Wellenhof et al., 2001). Therefore, GPS should be combined with other information.

MMWR (Millimeter-Wave Radars): determine the range and bearing to a set of beacons that are set up at known locations (Durrant-Whyte, 1996). Such radars aim to detect and avoid obstacles. These radars have full control of the beacons (number and precise location). Thus, they can be considered more reliable.

Ultrasonic Sensors: range sensors for map building and collision detection (Kanayama et al., 1984). Their working principle is based on the wavelength (Pagac et al., 1996). Such sensors can offer valuable and useful data when the sound speed is precisely known. However, there are some disadvantages: the used wavelengths, when the target is mirror-like objects, and when the angle between the normal to the object surface and the sensor direction is more than 10 degrees. In such conditions, there is not any significant reflected signal.

Internal navigation is associated with sensors mounted inside of the robot. This navigation is not related to environmental features or marks. The most common types of sensors are as follows.

Encoders: are digital optical devices that convert motion into digital pulses' sequence (robotiksistem, 2019). They are used for determining the velocity, acceleration, or position of a vehicle.

Gyroscopes: are devices that measure the inertial state of vehicles (Scheding et al., 1997). Due to their features (non-radiating, non-jammable, and fast), these sensors provide many advantages, especially for harsh environmental conditions. They can also compensate for errors that occur in the odometry based positioning method. Recently, fiber optic gyros provide better accuracy, and they have been an essential solution for navigation in mobile robots (Pao, 2018).

Potentiometer: is a rotary analog device used in several electrical and electronic circuits, and that operates mechanically as a three-terminal (Electronics Tutorials, 2020). They do not need to have a power supply or additive circuitry to perform their position (linear or rotary) function. Due to their variety, they provide simplification for controlling and adjusting voltage, current or the biasing, and for controlling the circuits to obtain a zero condition.

Electronic Compasses: devices that indicate the yaw heading to an object when they measure the earth's magnetic field (Skvortzov et al., 2007). When the compass is mounted into a vehicle, it shows only the direction of where the vehicle is headed. In human-made indoor environments, it can be found a considerable source of magnetic interference like reinforced concrete floor and walls, pipes, wiring, built-in cabling, different metals, and magnetic objects. The compass can experience magnetic interference from floor fields when the height of the compass on the floor is low (Qin et al., 2012).

2.1.2 Sensors for Environment Perception

Environmental perception is a complicated and complex task of mobile robots (Drunk, 1988). An important method used for environment perception is collision sensing (Leng et al., 2016). Robots sense collision points and direction to avoid collision again, and then the compliment control comes true. Some of the most commonly used sensors for environment perception are presented in the following paragraphs.

Vision Systems: complex systems mounted on mobile robots. See for more, the system represented by Eugenio et al. (Eugenio et al., 2007). These systems primarily aim to capture a very high number of points in the environment.

Laser-based Range Finding 2D and 3D: scanner devices that produce a precise image of the environment (Drunk, 1988). Due to the relatively high price of 3D lasers, 2D ones have been applied in many mobile robots, even though they might provide limited information related to the robot environment. For instance, a laser ranger at first was designed for the safety of dangerous areas and as an electronic for industrial autonomous guided vehicles (SICK AG, 2004). It works based on the time-of-flight principle and has a single moving part-the the rotating mirror (Demim et al., 2018). On the other hand, 3D sensors have more extended capabilities (Generation Robots, 2018). It means that more data are gathered in multiple dimensions that result in higher measurement accuracy.

2.2 Sensor Nodes

There are hundreds of thousands of sensor nodes included in a WSN (Matin & Islam, 2012). Sensor nodes use radio signals to communicate. A wireless sensor node is comprised of sensing and computing devices, radio transceivers, and power components. They depend on processing speed, storage capacity, and communication bandwidth level.

After sensor nodes are deployed, their responsibility is related to organizing by itself an adequate network infrastructure, usually with multi-hop communication. Then, the needed information starts to be collected by onboard sensors. Besides, sensor devices reply to queries that control sites send for performing instructions or providing sensing samples. GPSs and local positioning algorithms can be used to obtain information regarding location and position. Actuators can be set into wireless sensor devices so they can act under specific conditions. Akkaya and Younis refer more specifically to such networks by defining and describing them as Wireless Sensor and Actuator Networks (Akkaya & Younis, 2005).

Due to the improvements in information accuracy, the significance of WSNs has been increased (Chong & Kumar, 2003). The tasks of sensor nodes are to monitor the events that are happening within their sensing region, to collect the data to a sink node or base station, and to give meaning to the available information into the sink node. Then, users can get the data provided into the sink node and monitor the sensing regions' status. The use of WSNs can be found in many applications like surveillance, health monitoring, and investigations related to harsh physical environments (Mainwaring et al., 2002), (Galstyan et al., 2004).

2.2.1 Structure

The components of a sensor node are sensing, processing, transceiver, and power unit (Akyildiz et al., 2002).

Mobile sensor nodes can change the position autonomously and are subject to mission requirements. The benefits of them are related to the dynamic way they adjust network topology and to the promotion of sensor networks performance. The areas in which sensor nodes operate are typical disaster ones or harsh, remote environments where people face difficulties (Ssu et al., 2005):

Also, mobile sensors have the auto-refresh ability that helps to troubles and issues within a sensor network (Mora Vargas et al., 2006). Tanaka et al. proposed a dispersed algorithm to contribute to such confronts (Tanaka et al., 2012).

2.2.2 Data Collection from Mobile Nodes

To collect data, a mobile collector can go very close to a node. Thus, the node does not need a powerful transceiver to communicate with the mobile collector but only to wait until the collector goes close enough (Zheng et al., 2017). Data collection in WSNs with a mobile sink node consists of the following steps (R.Wankhade & Morris, 2013):

- Discovery: mobility independent and knowledge base;

- Data Transfer: joint discovery and transfer of data;
- Routing: flat and proxy-based;
- Motion Control: trajectory, static, dynamic, speed, and hybrid.

Since the nodes communicate only with the mobile collector and not with the other nodes, they do not need to have connectivity in the whole network (Zhang et al., 2015), (Nguyen & Teague, 2015).

Other authors have worked on mobile elements for reducing and set of scales in WSNs, but yet the compilation of data can elevate (Liang He et al., 2011). Hence, concerns related to mobile elements such as the way they navigate during the detected field and when they gather data from the sensors, have had attention and consideration from the researchers (Z. Wang et al., 2011). Ping et al. suggest that if the mobile antennas that meet data in short-range transportations will be used to gather data in WSNs, considerable improvement can be achieved (Ping et al., 2009).

2.3 Challenges

Some of the challenges related to data collection in mobile robots are listed as follows.

High Costs: The costs depend on the surface of buildings and, as a consequence on the number of places that must be monitored. Thus, the material and installation process can require a considerable amount of money (Demirbas, 2005).

Complex Design Requirements: Disturbances in indoor environments should be taken into consideration. They have a significant impact on the process design of the networks (F. Wang et al., 2010).

Supervision: Usually, sensors are installed in several locations, and there are several. Because of their number, they might need continuous monitoring against the threats they are posed from outsiders (F. Wang et al., 2010).

Maintenance: The calibration and maintenance process of the wireless sensors should be intense.

Limited Coverage: Because of the high costs involved, the space that can be monitored is relatively limited (Demirbas, 2005).

Other Challenges: WSs face issues from power consumption, scalability, and storage capacities. These influence the amount and quality of the data that can be collected (Raftery et al., 2011). Moreover, the terrain or the place where the sensors are placed plays a significant role. For instance, if the sensors are placed in heritage buildings, they can have a damaging impact on the underlying surface as the historical value of the place can be affected (Raffler et al., 2015).

3 DATA COMMUNICATION

Data communication is defined as the transmission of digital data such as numeric data, text, voice, video, photos between a source and a receiver (Techopedia, 2017). Its purpose is not the generation of data nor the outcome of the data transmitted but the transfer method and the data preservation during the transmission process (*Data Communication - Computer Networking Concepts*, 2019).

3.1 Types of Communication in Mobile Robots

Communication plays an important role to fulfill tasks in real-life processes. Mobile robots can use communications in the following situations presented below (Gage, 1997):

Robot and User Control Station: For example, in surveillance systems, the data collected comprises alarms or alerts, which are the result of the information acquired by the sensors. As a result, these alarms indicate a threat. Thus, the robot sends additional information such as images, audio, or videos in order to assess the problem.

Robots and Multi-robot System: Communication between robots and a multi-robot system is used for tasks such as supporting sensor data fusion, cueing from sensor to sensor, collaboration, and coordination of actions between robots and letting a robot act as a communications relay among other robots or user stations.

Robot System and External clients: Communication between robots and external sources serve for transferring sensor or processed data from the robot to an external client such as military officers.

Robot and Developer: The communication between the robot and a system developer is necessary for decreasing technical risks, boost productivity at the implementation phase by deploying software downloads and debugging tools to validate hardware and software. The communication will be able to allow developers to design, deploy, and integrate the software with the robot remotely.

Consequently, mobile robot communication can be envisioned for several applications, as showed in Figure 2. Robots can be teleoperated by a human or software which sends commands to the robot and receives data. Hence, low latency communication via the Internet is needed. Robots can work in a multi-robot system where low-power and long-range wireless communication is required. Remote sensing robots also need long-range wireless communication.

Moreover, robots' access to the Internet via a reliable communication link can enable uploading their processing tasks to the cloud, which can upgrade their computing and physical capabilities.

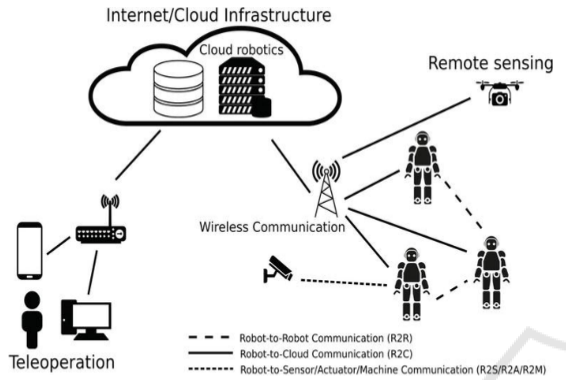

Figure 2: Mobile Robot Applications (Barriquello et al., 2018).

3.2 Communication Process

Three elements compose data communication within the mobile robot and its surroundings (Barriquello et al., 2018): awareness, processing and cognition, and action.

Awareness involves the data acquisition of the environment, the robot, and the relation between the robot and the surroundings. The information acquired is processed and sent to the actuators, which are in charge of the robot's motion. Once the data, such as the direction, destination, and purpose of the robot are established, the robot's cognition needs to arrange a plan on how the robot will achieve its purpose.

The cognition and control system responsible for the decision making and the deployment the robot uses in order to attain its goals. Additionally, the control system integrates the input data and the robot's movements. Cognitive models are necessary for a mobile robot. They are expected to represent the robot, the environment, and the interaction between them. Different areas work in a cognitive model. For example, computer vision and pattern identification are useful for keeping track of objects; and map algorithms are utilized to create maps of the surroundings.

Artificial intelligence algorithms, such as motion planning, are employed to manage the robot's interactions. Furthermore, it is anticipated that in the coming years, artificial intelligence will be mainly used for managing the information collected by the robot and the task given to it.

3.3 Internet Data Communication

The Internet as a communication channel has non-deterministic characteristics, depending on the network load. It is a non-expensive and readily available communication tool. However, it has significant limitations for robotic systems due to the restricted bandwidth, transmission delays, and data loss that impact the robots and system performance.

The connection performance depends on the speed and reliability of the transmitted data over that connection. In the case of the Internet, speed and reliability cannot be measured (Khamis et al., 2003).

Moreover, the upcoming 5G telecommunications will open up a variety of opportunities regarding mobile robotic applications in numerous fields such as education, ecology, medicine, agriculture, manufacturing, and more industries (Durmus & Gunes, 2019). These applications require remote interaction in which the human and the robot are physically separated but are connected by telematics

3.4 Challenges

Frequency communication is used for rescue and relief purposes (Greer et al., 2002). These robots use Industrial, Scientific, and Medical (ISM) bands, which are unlicensed frequencies and present some disadvantages. Communication can fail due to interferences since the bands are not licensed. The output power in the device and the control unit can be restricted, preventing signals from other units.

Efficiency in the transmission is affected when higher frequencies are used. Higher frequencies can penetrate more dense materials, such as in buildings. However, small elements such as dust resonate at high frequencies absorbing the signal. It is suggested to use a frequency in the middle of the two extremes that optimize communication. UHF frequencies are recommended since they need low power output and have excellent signal penetration characteristics.

Mobile robots controlled over the Internet pose several challenges such as internet transmission delays, delay jitter, and a non- guaranteed bandwidth in contrast with other communication systems in which there are constant delays and a limited but guaranteed bandwidth. These issues can lead to system performance degradation and can impact on the stability if they are not taken into consideration during the design and deployment of the system (Alves et al., 2000).

As a solution is suggested to eliminate human operators from the control loop, implement high local intelligence and reactive behavior into the robots. Hence, mobile robots will autonomously manage real-world uncertainty and network delays. Furthermore, an intuitive user interface is needed for facilitating non trained staff in the remote control of the robot. The whole system should be reliable so that the users can access it at any time without the necessity of human interaction (Hu et al., n.d.).

TCP and UDP are the transport protocols used for data communication among Internet-based robots. In this case, the exchange of information between the operator and the robot must not have delays. TCP is utilized for reliable static data communication such as emails and files in low- bandwidth. It guarantees the retransmission of a lost packet, which causes significant delays and efficiency reduction. UDP reduces delays, but it is not able to cope with extra bandwidth and network congestion.

Consequently, TCP and UDP are not suggested for teleoperation (Kazala et al., 2015). As a solution, a trinomial protocol for robotic internet systems is proposed. It is a source-based protocol that displays a similar performance to UDP concerning delays, delay jitter, and packet loss rate. Its steady-state and the transmission rate are better than TCP. It quickly adapts to network bandwidth variation (Xiaoping Liu et al., 2003), (Schiøler et al., 2012).

4 SECURITY ISSUES

4.1 Security Threats

Data transmission between robots and base stations via the network needs to go through computers and routers such as wireless hotspots. Due to this reason, it can be targeted by a third party or a hacker. Several threats in the network traffic include:

Computer Viruses: small software can disable the security settings, corrupt, and steal data from the computer, including personal information like passwords, or deleting everything on the hard drive (Team, 2018).

Rogue Security Software: a malicious software that can mislead users to think that there are some computer antivirus scanners (Cova et al., 2009) on their computer or their systems and the security firewall or antivirus software are not up to date.

Trojan Horse: malware or malicious code, which trick users into running it by opening an attachment in the email or clicking on false advertisement. When a trojan horse is inside the system, it can save passwords by using keystroke logging or hacking webcam and stealing sensitive data on the computer/system.

Eavesdropping: information remains flawless, but its privacy is compromised. Someone could capture sensitive conversation or intercept classified information during transmission.

Tampering: information during transferring is changed or replaced and then sent to the recipient.

Impersonation: information passes to a person who poses as the intended recipient. Impersonation can take two forms: spoofing (a person can pretend to have the email address of another person, or a computer can identify itself as another website when it is not) and misrepresentation (a person or an organization can misrepresent itself).

Adware or Spyware: recognized as any software that is designed to track users' data surfing habits. Adware aims to collect consent data. Spyware is similar to adware, but it is installed on a computer without notice. It may include keyloggers to take personal information, including email addresses, passwords, and credit card numbers (Team, 2018).

Phishing: a social engineering method aiming to get sensitive data such as passwords, usernames, credit card numbers (Figure 3). There are several types of phishing attacks, such as spear phishing, clone phishing, and whaling (Cloudflare, 2020).

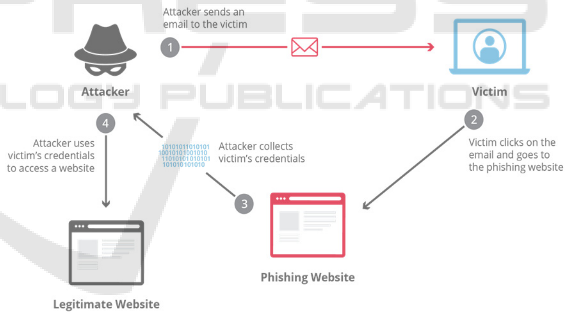

Figure 3: Phishing attack (Cloudflare, 2020).

DDOS Attack: the attackers break online devices networks (i.e., computers or other IoT devices), make them as bots or zombies, and gain control over a target. When a botnet has been set up, the adversaries are able to directly send updated instructions to each bot through a method of remote control. As a result, the victims' network will overflow its capacity and lead to the servers' or networks' denial of service.

4.2 Security Attacks

External Attacks: They occur by outside network attackers when they do not have any information about the network system. Also, it is related to several layers of the OSI model, such as the physical layer, data link layer, network layer, and transport layer (Puthal, 2012).

Internal Attacks: They can take place due to the flaws in networking protocols or weaknesses in software that integrate networking protocols. These intrusions focus on the network and transport layer of the OSI layer (Kamal & Issac, 2007).

Man in the Middle Attack: It happens when an attacker uses some techniques to put someone in the middle of a conversation between a user and an application to eavesdrop or capture the information (Imperva, 2020). The main goal of this attack is to steal personal information, for example, identity theft, passwords to target Advanced Persistent Threat (APT) (Figure 4).

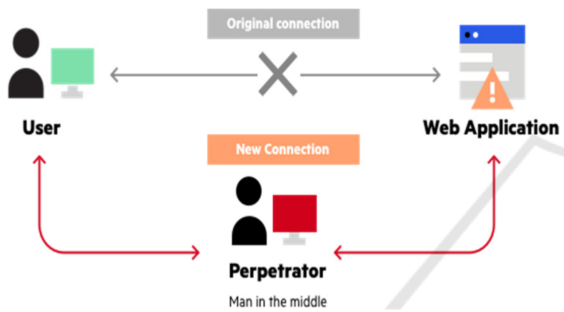

Figure 4: Man in the middle attack (Imperva, 2020).

Furthermore, MITM aims to steal the session through packet sniffer to gain control in some layers, such as Application, Presentation, Transport, and Datalink in the OSI model. MITM has two major distinct stages: interception (Ip spoofing, ARP spoofing, and DNS spoofing) and decryption (HTTPS spoofing, SSL beast, SSL hijacking, and SSL stripping).

5 CONCLUSIONS

This paper presented an overview of mobile robots by emphasizing the importance of data collection, communication, and security. It was shown that the most significant devices are sensors assigned for different kinds of applications. Also, it was shed light on the significance of WSNs and sensor nodes. Then, we explained and highlighted the data communication procedures as an essential element for fulfilling the tasks in the real-life. Communication between users and robots or within robot systems is critical to assure the effectiveness and the correct fulfilment of the robot's task. It plays a crucial role in the mobile robot's performance. In the last part, we described the security threats and issues concerning data collection and communication.

The scientific data collected in this work suggests that due to the complexity and different environments where mobile robots operate, careful attention must be paid in reducing (if not eliminating) the challenges of data collection and communication. Also, we propose that future research should be taken in the area of security risks of data transmission. We believe that our research will serve as a baseline for further investigations in the field of mobile robots.

ACKNOWLEDGEMENTS

This article is supported by national grant "VKE-2017-00031" on High Precision Surface Control Robot Prototype.

REFERENCES

Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless sensor networks. *Elsevier Journal of Ad Hoc Networks*, *3*(2), 325–349. https://doi.org/10.1016/j.adhoc.2003.09.010

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks*, *38*(4), 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4

Alves, R. L., Vassallo, R. F., Freire, E. O., & Bastos-Filho, T. F. (2000). Teleoperation of a mobile robot through the Internet. *Midwest Symposium on Circuits and Systems*, *2*, 930–933. https://doi.org/10.1109/mwscas.2000.952906

Barriquello, C. H., Silva, F. E. S. e, Bernardon, D. P., Canha, L. N., Ramos, M. J. D. S., & Porto, D. S. (2018). Fundamentals of Wireless Communication Link Design for Networked Robotics. In *Service Robots*. InTech. https://doi.org/10.5772/intechopen.69873

Canli, T., & Khokhar, A. (2009). *Data Acquisition and Dissemination in Sensor Networks BT - Encyclopedia of Database Systems* (L. LIU & M. T. ÖZSU (Eds.); pp. 548–552). Springer US. https://doi.org/10.1007/978-0-387-39940-9_92

Chong, C.-Y., & Kumar, S. P. (2003). Sensor Networks: Evolution, Opportunities, and Challenges. *Proceedings of the IEEE, Vol 91*, 1247–1256. https://doi.org/10.1109/JPROC.2003.814918

Cloudflare. (2020). *What is a phishing attack?*

Cova, M., Leita, C., Thonnard, O., Keromytis, A., & Dacier, M. (2009). Gone rogue: An analysis of rogue security software campaigns. *EC2ND 2009 - European Conference on Computer Network Defense*, *February 2014*, 1–3. https://doi.org/10.1109/EC2ND.2009.8

Data Communication - Computer Networking concepts.

(2019). http://mucins.weebly.com/1-data-communication.html

Demim, F., NEMRA, A., Louadj, K., & Hamerlain, M. (2018). Simultaneous localization, mapping, and path planning for unmanned vehicle using optimal control. *Advances in Mechanical Engineering*, *10*, 168781401773665. https://doi.org/10.1177/1687814017736653

Demirbas, M. (2005). *Wireless Sensor Networks for Monitoring of Large Public Buildings*.

Drunk, G. (1988). Sensors for mobile robots. In P. Dario & C. E. (Eds. . Piaggio (Eds.), *Sensors and Sensory Systems for Advanced Robots* (pp. 463–492). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-83410-3

Durmus, H., & Gunes, E. O. (2019). Integration of the mobile robot and Internet of things to collect data from the agricultural fields. *2019 8th International Conference on Agro-Geoinformatics, Agro-Geoinformatics 2019*, 1–5. https://doi.org/10.1109/Agro-Geoinformatics.2019.8820578

Durrant-Whyte, H. F. (1996). An autonomous guided vehicle for cargo handling applications. *International Journal of Robotics Research*, *15*(5), 407–440. https://doi.org/10.1177/027836499601500501

Electronics Tutorials. (2020). *Potentiometer, Preset Potentiometers and Rheostats*.

Elizabeth Howell. (2017). *Real-Life "Replicants": 6 Humanoid Robots Used for Space Exploration*.

Eric. (2020). *The Best Rangefinder - Everything you Need to Know About Rangefinders 2019*.

Eugenio, A., Garcia-Silvente, M., González-Muñoz, A., Paúl, R., & Rafael, M. (2007). A Fuzzy System for Detection of Interaction Demanding and Nodding Assent Based on Stereo Vision. *Journal of Physical Agents*.

Gage, D. W. (1997). *Network Protocols for Mobile Robot Systems*.

Galstyan, A., Krishnamachari, B., Lerman, K., & Pattem, S. (2004). Distributed online localization in sensor networks using a moving target. *Third International Symposium on Information Processing in Sensor Networks, IPSN 2004*, 61–70. https://doi.org/10.1145/984622.984632

Generation Robots. (2018). *RoboSense RS-LiDAR-32 3D Laser Range Finder*.

Greer, D., Kerrow, P. M., & Abrantes, J. (2002). Robots in Urban Search and Rescue Operations. In *Citeseer*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.5977&rep=rep1&type=pdf

Heba Soffar. (2016). *Advantages and disadvantages of using robots in our life*.

Hofmann-Wellenhof, B., Lichtenegger, H., & Collins, J. (2001). 2. Overview of GPS. In *Global Positioning System. Theory and practice.* (Fifth edit, pp. 11–23). Springer-Verlag Wien.

Hu, H., Yu, L., Tsui, P. W., & Zhou, Q. (n.d.). Internet-based Robotic Systems for Teleoperation. *Journal of Assembly Automation*, *21*(2), 1–10.

Imperva. (2020). *Man in the middle (MITM) attack*.

Kamal, S., & Issac, B. (2007). Analysis of network communication attacks. *2007 5th Student Conference on Research and Development, SCORED*, *December*. https://doi.org/10.1109/SCORED.2007.4451370

Kanayama, Y., Yuta, S., & Kubotera, Y. (1984). Sonic Range Finding Module for Mobile Robots. *Proceedings - 14th International Symposium on Industrial Robots, 7th International Conference on Industrial Robot Technology.*, 643–652.

Kazala, R., Taneva, A., Petrov, M., & Penkov, S. (2015). *Wireless Network for Mobile Robot Applications*. https://doi.org/10.1016/j.ifacol.2015.12.088

Khamis, A. M., Rodríguez, F. J., & Salichs, M. A. (2003). Remote Interaction with Mobile Robots. *Autonomous Robots*, *15*(3), 267–281. https://doi.org/10.1023/A:1026268504593

Leng, Y.-Q., Chen, Z.-C., He, X., Zhang, Y., & Zhang, W. (2016). Collision Sensing Using Force/Torque Sensor. *Journal of Sensors*, *2016*, 6291216. https://doi.org/10.1155/2016/6291216

Liang He, Pan, J., & Jingdong Xu. (2011). Reducing data collection latency in Wireless sensor networks with mobile elements. *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 572–577. https://doi.org/10.1109/INFCOMW.2011.5928878

Lobo, J., Marques, L., Dias, J., Nunes, U., & de Almeida, A. T. (2005). Sensors for mobile robot navigation. *Autonomous Robotic Systems. Lecture Notes in Control and Information Sciences*, *236*, 50–81. https://doi.org/10.1007/bfb0030799

Mainwaring, A., Culler, D., Polastre, J., Szewczyk, R., & Anderson, J. (2002). Wireless sensor networks for habitat monitoring. *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications - WSNA '02*, 88–97. https://doi.org/10.1145/570738.570751

Mantha, B. R. K., Menassa, C. C., & Kamat, V. R. (2018). Robotic data collection and simulation for evaluation of building retrofit performance. *Automation in Construction*, *92*, 88–102. https://doi.org/10.1016/j.autcon.2018.03.026

Matin, M., & Islam, M. (2012). Overview of Wireless Sensor Network. In *Wireless Sensor Networks – Technology and Protocols*. InTech. https://doi.org/http://dx.doi.org/10.5772/57353

Mora Vargas, A. E., Mizuuchi, K., Endo, D., Rohmer, E., Nagatani, K., & Yoshida, K. (2006). Development of a Networked Robotic System for Disaster Mitigation, -Navigation System based on 3D Geometry Acquisition. *2006 IEEE/RSJ International Conference on Intelligent Robots and Systems*, 4821–4826. https://doi.org/10.1109/IROS.2006.282357

Nguyen, M. T., & Teague, K. A. (2015). Random sampling in collaborative and distributed mobile sensor networks utilizing compressive sensing for scalar field mapping. *2015 10th System of Systems Engineering Conference (SoSE)*, 1–6. https://doi.org/10.1109/SYSOSE.2015.7151962

Pagac, D., Nebot, E. M., & Durrant-Whyte, H. (1996). An evidential approach to probabilistic map-building. *Proceedings of the 1996 IEEE International Conference on Robotics and Automation*, 164–170. https://doi.org/10.1007/BFb0013958

Pao, C. (2018). *Exploring the Application of Gyroscopes*.

Ping, S., Kejie, L., Xiaobing, H., & Guangping, Q. (2009). Formation and obstacle-avoidance control for mobile swarm robots based on artificial potential field. *2009 IEEE International Conference on Robotics and Biomimetics (ROBIO)*, 2273–2277. https://doi.org/ 10.1109/ ROBIO.2009.5420385

Puthal, D. (2012). *Secure Data Collection and Critical Data Transmission Technique in Mobile Sink Wireless Sensor Networks*.

Qin, J., Guo, Y., & Zhou, M. (2012). Data acquisition and processing of electronic compass for mobile robot autonomous navigation. *Proceedings of the 2012 National Conference on Information Technology and Computer Science, CITCS 2012*, 773–775. https://doi.org/10.2991/citcs.2012.17

R.Wankhade, S., & Morris, N. (2013). A Review on Data Collection Method with Sink Node in Wireless Sensor Network. *International Journal of Distributed and Parallel Systems*, *4*, 67–74. https://doi.org/10.5121/ ijdps.2013.4106

Rachel. (2018). *7 Advantages of Robots in the Workplace*.

Raffler, S., Bichlmair, S., & Kilian, R. (2015). Mounting of sensors on surfaces in historic buildings. *Energy and Buildings*, *95*, 92–97. https://doi.org/https://doi.org/ 10.1016/j.enbuild.2014.11.054

Raftery, P., Keane, M., & Costa, A. (2011). Calibrating whole building energy models: Detailed case study using hourly measured data. *Energy and Buildings*, *43*(12), 3666–3679. https://doi.org/https://doi.org/ 10.1016/j.enbuild.2011.09.039

Rasam, H. R. (2016). Review on Land-Based Wheeled Robots. *MATEC Web of Conferences*, *53*, 1–9. https://doi.org/10.1051/matecconf/20165301058

robotiksistem. (2019). *Mobile Robot Sensors*.

Scheding, S., Nebot, E. M., Stevens, M., Durrant-Whyte, H., Roberts, J., Corke, P., Cunningham, J., & Cook, B. (1997). Experiments in autonomous underground guidance. *Proceedings - IEEE International Conference on Robotics and Automation*, *3*, 1898–1903. https://doi.org/10.1109/robot.1997.619065

Schiøler, H., Thomas, ·, & Toftegaard, S. (2012). Wireless Communication in Mobile Robotics a Case for Standardization. *Wireless Pers Commun*, *64*, 583–596. https://doi.org/10.1007/s11277-012-0602-x

SICK AG. (2004). *Proximity Laser Scanner PLS 10 X- 317*.

Skvortzov, V. Y., Lee, H. K., Bang, S. W., & Lee, Y. B. (2007). Application of electronic compass for mobile robot in an indoor environment. *Proceedings - IEEE International Conference on Robotics and Automation*, 2963–2970. https://doi.org/10.1109/ROBOT.2007.363922

Ssu, K. F., Ou, C. H., & Jiau, H. C. (2005). Localization with mobile anchor points in wireless sensor networks. *IEEE Transactions on Vehicular Technology*, *54*(3), 1187–1197. https://doi.org/10.1109/TVT.2005.844642

Swartz, R. A., Zimmerman, A. T., Lynch, J. P., Rosario, J., Brady, T., Salvino, L., & Law, K. H. (2012). Hybrid wireless hull monitoring system for naval combat vessels. *Structure and Infrastructure Engineering*, *8*(7), 621–638. https://doi.org/10.1080/15732479.2010.4953 98

Tanaka, K., Ohtake, H., Tanaka, M., & Wang, H. O. (2012). Wireless Vision-Based Stabilization of Indoor Microhelicopter. *IEEE/ASME Transactions on Mechatronics*, *17*(3), 519–524. https://doi.org/10.1109/ TMECH.2011.2181532

Team, S. (2018). *Top 10 Common Network Security Threats Explained*.

Techopedia. (2017). *What is Data Communications (DC)?* Techopedia. https://www.techopedia.com/definition/ 6765/data-communications-dc

Wang, F., Liu, J., & Sun, L. (2010). Ambient Data Collection with Wireless Sensor Networks. *EURASIP Journal on Wireless Communications and Networking*, *2010*, 1–10. https://doi.org/10.1155/2010/698951

Wang, Z., Zhang, H., & Jiang, B. (2011). LMI-Based Approach for Global Asymptotic Stability Analysis of Recurrent Neural Networks with Various Delays and Structures. *IEEE Transactions on Neural Networks*, *22*(7), 1032–1045. https://doi.org/10.1109/TNN.2011. 2131679

Weik, M. H. (2001). *data collection BT - Computer Science and Communications Dictionary* (M. H. Weik (Ed.); p. 342). Springer US. https://doi.org/10.1007/1-4020-0613-6_4219

Xiaoping Liu, P., Q-h Meng, M., & Yang, S. X. (2003). Data Communications for Internet Robots. In *Autonomous Robots* (Vol. 15).

Xu, G., & Xu, Y. (2016). GPS: Theory, algorithms and applications, third edition. In *GPS: Theory, Algorithms and Applications, Third Edition*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-50367-6

Zhang, H., Zhu, Y., & Tan, J. (2015). Adaptive sampling and sensing approach with mobile sensor networks. *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 654–660. https://doi.org/10.1109/ CYBER.2015.7288018

Zheng, H., Li, J., Feng, X., Guo, W., Chen, Z., & Xiong, N. (2017). Spatial-Temporal Data Collection with Compressive Sensing in Mobile Sensor Networks. *Sensors*, *17*, 2575. https://doi.org/10.3390/s17112575.