Sneakernet on Wheels: Trustworthy NFC-based Robot to Machine Communication

Thomas Ulz, Thomas Pieber, Christian Steger
Institute for Technical Informatics
Graz University of Technology
Graz, Austria
{thomas.ulz, thomas.pieber, steger}@tugraz.at

Sarah Haas, Rainer Matischek
Development Center Graz
Infineon Technologies Austria AG
Graz, Austria
{sarah.haas, rainer.matischek}@infineon.com

***Abstract*—Wireless communication technologies such as WiFi, ZigBee, or Bluetooth often suffer from interference due to many devices using the same, unregulated frequency spectrum. Also, wireless coverage can be insufficient in certain areas of a building. At the same time, eavesdropping a wireless communication outside a building might be easy due to the extended communication range of particular technologies. These issues affect mobile robots and especially industrial mobile robots since the production process relies on dependable and trustworthy communication. Therefore, we present an alternative communication approach that uses Near Field Communication (NFC) to transfer confidential data such as production-relevant information or configuration updates. Due to NFC lacking security mechanisms, we propose a secured communication framework that is supported by dedicated hardware-based secure elements. To show the feasibility of our approach, an Industry 4.0 inspired production process that uses our communication approach is evaluated in simulation.**

***Index Terms*—Near Field Communication; Industrial Robots; Industry 4.0; Configuration.**

I. Introduction

Having a trustworthy and dependable communication channel is essential in many scenarios, especially in industrial settings where the production process can be influenced negatively due to malfunctioning communication between involved devices. This applies in particular to so-called *smart factories* as envisioned in high-tech initiatives such as *Industry 4.0* [1]. Such smart factories are characterized by rapidly changing product demands, varying utilization of different production machinery, and usage of industrial autonomous mobile robots (IAMRs). Since IAMRs are involved in the production process, they need to transfer information between them and the involved production machinery. Although wired network technologies are usually preferred in industrial settings, wireless technologies are required in such Industry 4.0 setting due to the IAMRs not being stationary devices. Therefore, industrial wireless technologies are gaining popularity [2] although they generally suffer from the following three problems:

1) **Interference:** The $2.4\,\mathrm{GHz}$ frequency band that is used by communication technologies such as WiFi, Bluetooth or ZigBee is crowded due to all these technologies using the same spectrum. In addition, also devices such as cordless telephones, baby phones or other remote controlled accessories could potentially operate in the $2.4\,\mathrm{GHz}$ range [3]. The alternative $5\,\mathrm{GHz}$ range for WiFi is also already used by other devices such as cordless phones, radar, and digital satellites [4]. Due to many devices operating in the same frequency range, interference will occur and affect wireless communication.
2) **Insufficient Coverage:** Due to certain objects in buildings that dampen or even shield wireless communication (e.g. walls or large production machines) it is costly to provide good wireless coverage for every part of a certain area. For IAMRs this is a problem due to the non-deterministic behavior when navigating on a factory floor. For instance, avoiding a moving obstacle (e.g. humans) might require the IAMR to navigate to a certain part of the factory floor without sufficient wireless coverage.
3) **Eavesdropping:** The communication range of wireless technologies such as WiFi (and particularly sub-GHz ISM-band protocols) ranges up to several hundred meters. Due to this fact, eavesdropping ongoing communication could be possible outside an enclosed factory environment. This fact allows potential adversaries to eavesdrop and attack wireless communication without physical access to the smart factory, even if the communication is sufficiently secured against remote attacks.

In order to mitigate these problems, we propose to use Near Field Communication (NFC) in industrial settings due to the following three reasons. (i) NFC operates at a different frequency range than the most commonly used wireless technologies, thus reducing the risk of interference with other devices. (ii) NFC only supports peer-to-peer communication. Therefore, wireless coverage for a certain area is not required. Instead, each communication partner needs to be equipped with NFC capable devices. (iii) Due to the limited communication range of NFC, eavesdropping becomes more complicated for potential adversaries compared to other wireless communication technologies. To account for the previously discussed Industry 4.0 settings, NFC devices need to be mounted on any production machinery and IAMR that wants to communicate with other involved partners. We present a hardware extension that can be integrated into new

equipment as well as retrofit to existing legacy devices. In combination with security mechanisms that we are going to present in this paper, this NFC extension is capable of providing a dependable and trustworthy communication mechanism that does not suffer from the previously mentioned problems of other wireless communication technologies. Because a production machine A can not directly communicate with a second production machine B due to the limited communication range of NFC, the machines will rely on the IAMRs moving between them to transport information from A to B. This concept of communicating originates from the early days of IT, where network connections were not that common. In a so-called *sneakernet* [5], data was transported from A to B using mediums such as floppy disks or USB sticks. In our case, this sneakernet concept will therefore be introduced to (robotic) wheels.

Contributions. Briefly, the contributions of this paper are: (i) We propose to use NFC as communication technology for industrial contexts that involve IAMRs to mitigate drawbacks of other wireless technologies. (ii) To provide a secured and reliable connection that can be used in new equipment as well as for legacy hardware, we present a hardware extension and the software components necessary for our approach. (iii) The feasibility of our presented approach is then shown in a simulation of an Industry 4.0 inspired use case.

Outline. The remainder of this paper is structured as follows. In Section II background information on the involved technologies as well as related work is discussed. The NFC-based communication approach for IAMRs is then presented in Section III. Section IV discusses and evaluates the feasibility of that approach for Industry 4.0 inspired settings. Future work and a conclusion are then given in Section V.

II. Background and Related Work

A. Industrial Robot Wireless Communication

Robot wireless communication has evolved from early technologies such as infrared towards radio frequency (RF) technologies such as Bluetooth and WiFi [6], [7]. Due to the emergence of Wireless Sensor Networks (WSNs) and the Internet of Things (IoT) in general, the mitigation of interference effects is a focus in research [8], [9], [10]. Many of the presented approaches try to minimize the effects of interference by modifying the lower layer protocols (e.g. MAC layer protocols). Although more robust solutions were proposed in research, in current practice WiFi is still seen as the de-facto standard in industrial communication due to factors such as low cost, ease of integration, and compatibility with almost any system. Therefore, special variants of wireless technologies suited for industrial use have been proposed [11].

The topic of robot wireless communication is also discussed concerning robotic inspired use cases such as the RoboCup that is seen as a testbed for future robotic solutions. Rooker and Birk [12] show that using wireless communication poses certain constraints that need to be considered in the respective robotic use case. Liu et al. [13] compare different communication technologies regarding their dependability and delay. The authors also note that wireless communication is especially critical in industrial settings. Santos et al. [14], [15] present measures on how to efficiently use a shared wireless communication channel in RoboCup competitions. In contrast to that, Birk et al. [16] propose to use cable-based communication for scenarios where reliable communication is of utmost importance such as for rescue robots. However, to the best knowledge of the authors, no satisfactory solution suited for robot to machine communication has been presented yet.

B. Near Field Communication (NFC)

NFC operates at an RF of $13.56\,\mathrm{MHz}$, typically at a range of $3\,\mathrm{cm}$-$10\,\mathrm{cm}$ and supports bit rates of 106, 212, 424, and $848\,\mathrm{kbps}$. The technology is based on several RFID standards and operates in a so-called contactless communication mode. The most common and well-known fields of application for NFC are mobile payment and access control systems [17]. NFC supports the following three standardized modes of operation: (i) *Card Emulation Mode:* The NFC device emulates a (smart) card; no RF field is generated by the device (passive mode). (ii) *Reader/Writer Mode:* The NFC device generates an RF field that is used to communicate with a passive device. The passive device also can be powered through the RF field emitted by the active device. (iii) *Peer to Peer Mode:* In this mode, a master/slave principle is used. The communication's initiator is defined as master. Independent on the chosen mode of operation, the device pairing principle of NFC is fundamentally different compared to other wireless technologies such as WiFi or Bluetooth. NFC devices are paired by bringing the two communicating devices in close proximity of each other [18]. Other than the so-called *security by proximity* principle, NFC provides no security mechanisms at the link layer; therefore, security needs to be provided by the application layer.

C. Authenticated Encryption (AE)

To provide data confidentiality, integrity, and authenticity AE comprises *symmetric cryptography* and *Message Authentication Codes (MAC)* [19]. Symmetric encryption (or private key encryption) requires both communicating partners to be in possession of the same shared secret that is then used for encryption and decryption of data. The most commonly used symmetric cryptographic algorithm is the *Advanced Encryption Standard (AES)* [20]. AES provides various modes of operation that provide different characteristics regarding execution speed or size of the implementation. Some of these modes such as AES-CCM or AES-GCM support the calculation of AE.

D. One-Time Ticket (OTT)

OTTs are similar to one-time passwords [21] in that they are used to authorize an entity to access a certain service exactly

once. An OTT is issued to a certain entity and might be valid only for a given time. If the ticket holder tries to use the ticket after it has expired, access to the service is rejected. The concept of using tickets to access services is applied in widely used protocols such as *Kerberos* [22].

E. Security Controller (SC)

SCs are dedicated hardware-based secure elements that are capable of providing a secured execution environment for security-critical code as well as secured data and application storage. These functionalities can be offered by SCs due to their *tamper resistance* [23]. An SC that provides tamper resistance uses appropriate countermeasures to mitigate *physical attacks*. These kind of attacks are different to *remote attacks* as physical attacks are performed by adversaries who have physical access to the system under attack. Physical attacks are not a focus of research in robotics yet; however, the necessity to have some instance that provides reliable execution of software components in mobile robots was already proposed by Tomatis et al. [24]. Although the authors implemented their SC in software, its correct functionality is validated by a dedicated processor to improve the safety and security of the presented mobile robot platform.

III. NFC-based Communication

To enable production machinery as well as IAMRs to communicate using NFC technology, these devices need to be equipped with appropriate NFC-capable hardware. Additionally, a secured communication protocol needs to be applied to provide a trustworthy and dependable data channel. Therefore, we present NFC enhancement hardware for production machinery and IAMRs as well as a communication protocol fitted to the presented hardware. The feasibility of our approach will be evaluated int the context of the *RoboCup Logistics League's (RCLL)*. Since the RCLL's goal is to provide a factory automation testbed that resembles an Industry 4.0 motivated scenario including IAMRs [25], we consider this league as an ideal setting to evaluate our proposed approach.

A. NFC Enhancement Components

NFC communication supports different communication modes; however, all of these communication modes require an *active (master)* and a *passive (slave)* device in order to establish a connection and transfer data. In an Industry 4.0 inspired use case that involves production machinery and IAMRs, we propose to implement the IAMRs as active devices while the production machinery will be implemented as passive device. This allocation of roles would allow the IAMRs to communicate with production machinery independent of the machines current (power) state. Therefore, an approaching IAMR could, for example, turn on or activate the respective production machine, without the passive machine having to poll or wait for incoming connections. Both, the active and passive NFC enhancements are shown in Fig. 1 where the proposed hardware components are applied to an Industry 4.0 inspired simulation that was adapted from the RCLL's official simulation environment [26].

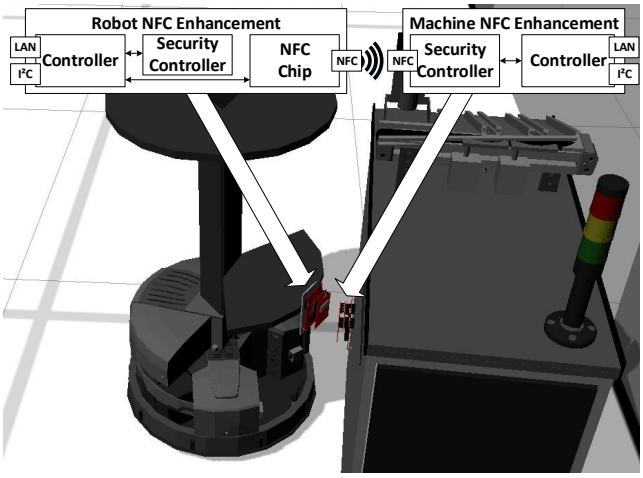


Fig. 1: Concept of NFC-based robot to machine communication applied to RCLL game simulation in Gazebo.

B. Robot (Active NFC Device)

The *Robot NFC Enhancement* component that is the active NFC device is shown on the left-hand side of Fig. 1 and comprises the following three components:

1) The *NFC Chip* provides the necessary interface to initiate and execute NFC communication. Due to the component being active, the NFC chip always needs to be powered by a power source provided by the IAMR.
2) The *SC* executes security related code that is required for the proposed communication protocol. In addition, the SC also provides secured storage for confidential information such as key material. SCs that are suitable for industrial use cases are offered, for example, in Infineon's Optiga family [27].
3) The *Controller* operates as an interface to the IAMR and thus, provides interfaces to connect the NFC enhancement to existing robotic hardware.

C. Machine (Passive NFC Device)

The *Machine NFC Enhancement* component that acts as passive NFC device is shown on the right-hand side of Fig. 1 and comprises the following two components:

1) The *SC* provides an NFC interface as well as secured execution of security relevant code. To be independent of machine states, the SC should be powered by the NFC field of the active device. SCs that provide this feature can be found, for example, in Infineon's SLE78 family.
2) The *Controller* acts as a gateway between SC and existing hardware and thus, provides appropriate interfaces such as Ethernet or I^2C.

D. Communication Protocol

In addition to the NFC enhancement components discussed in Section III-A we also propose a communication protocol

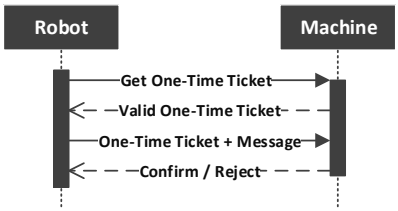


Fig. 2: Sequence diagram of communication handshake.

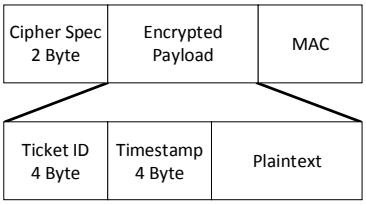


Fig. 3: NDEF packet structure.

that provides the necessary security measures entailed by the transfer of confidential data in industrial scenarios. To protect that data, we identify the following types of attacks that need to be mitigated by our approach:

Eavesdropping: Although NFC has a limited communication range, data *confidentiality* needs to be protected such that no unauthorized party has access to transferred data.

Manipulated Packets: Packet manipulation by potential adversaries must be detected in order to protect data *integrity*.

Authorized Communication Partners: Unauthorized senders must be detected in order to reject data sent by such communication partners. Thus, data *authenticity* is protected.

Replay Attacks: Captured and re-sent data that is unmodified must be identified and rejected in order to mitigate replay attacks and thus, protect the system's *functionality*.

To mitigate all of the mentioned attack types, we propose to apply AE in combination with OTTs. AE is used to provide data confidentiality, integrity, and authenticity. In addition, we use OTTs to detect and mitigate replay attacks. The master requests the OTT from the slave after initiating the communication. OTTs are directly generated at the slave when they are requested. Upon reception of that ticket, the master then is allowed to send a single message to the slave using this ticket. The sequence of this simple handshake and data sending is shown in Fig. 2.

The OTT used in our approach is composed of two components: (i) a random number, and (ii) the issued timestamp of a given ticket. In contrast to other approaches such as Kerberos, where multiple tickets can be issued and used at the same time, our approach only allows one ticket to be valid at any time. That is, if an OTT is requested, the ticket issuer (machine) stores the corresponding *Ticket ID* that comprises a random number and the issue *timestamp*. If a new ticket is requested without the old one being used, the old OTT automatically becomes invalid since it is overwritten. To request an OTT, the requester also needs to specify the timestamp of the OTT request. Both request and OTT are then only valid for a specified amount of time to mitigate replay attacks. Due to the ticket information being confidential, it also needs to be sent encrypted. The NDEF packet structure we use for the whole communication process is shown in Fig. 3. The fields included in this NDEF message are:

Cipher Spec: Specifies the algorithm and used key length for AE. This information is transmitted unencrypted.

MAC: The MAC calculated for the entire message; transmitted unencrypted.

Ticket ID: The OTT's ID (random number) that can be generated using a true random number generator provided by the SC. The ticket ID is transmitted encrypted.

Timestamp: The timestamp of either the ticket request or the ticket issuing. The timestamp is transmitted encrypted.

Plaintext: The information of the transferred message. The plaintext is transmitted encrypted.

IV. Evaluation

To evaluate our presented approach, we discuss two measures that are essential for determining the feasibility for industrial use-cases: security and communication performance.

A. Security Analysis

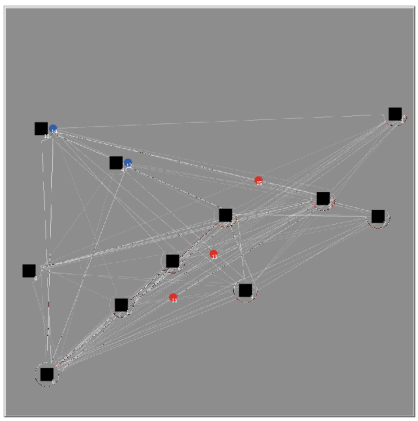
Using the NFC enhancement components discussed in Section III-A in combination with the protocol presented in Section III-D the following security-related properties can be provided by our approach:

CIA: Data **C**onfidentiality, **I**ntegrity, and **A**uthenticity are provided by the applied AE that is executed in a secured environment on the SC. The used key material that is also confidential is protected by the tamper resistance provided by the SC. Thus, eavesdropping, packet manipulation, and unauthorized access can be mitigated by our presented approach.

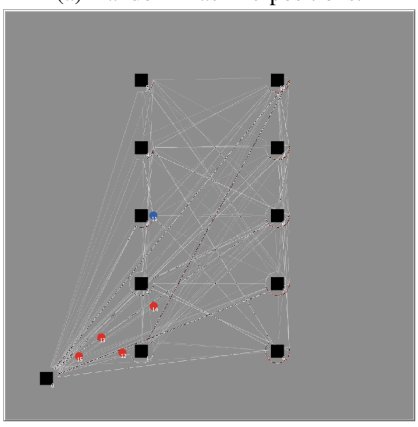
Replay Attacks: By using OTTs, also replay attacks are mitigated since a captured package cannot be re-sent by an attacker to provoke an unwanted machine state. Without this measure, an attacker could, for example, capture a message that configures a machine such that a certain product is produced, and re-send this message at a later time.

B. Communication Performance

We analyze and discuss communication performance-based on two use-cases that are prevalent in industrial scenarios. (i) Robot to machine communication to configure a machine for the respective production process. In network terms, this is a *unicast message*. (ii) To send information such as firmware updates or global configuration changes to all machines, a *multicast/broadcast* is required.



(a) Random machine positions.



(b) Fixed machine positions.

Fig. 4: Simulation setup for (a) randomized and (b) fixed machine positions. The black squares are simulated machines, red circles are moving IAMRs, blue circles represent IAMRs interacting with machines, and white lines represent the IAMRs' trajectories.

C. Unicast Message

To analyze the feasibility of robot to machine communication, we compare the connection timings of a point-to-point wireless TLS connection between two Raspberry PI 3 and our presented approach when sending a message of $256\,\text{bytes}$. In an ideal case where only the two involved devices are in the WiFi network, we measured an average message time including the TLS handshake of about $100\,\text{ms}$. Compared to our approach, the handshake also needs on average $100\,\text{ms}$. That means our approach is able to perform equally as fast as TLS for small amounts of data.

D. Multicast/Broadcast Message

In addition to unicast messages, we also analyze multicast/broadcast messages in the form of a configuration update (e.g. firmware) that should be transported to all machines. Since other technologies such as WiFi or Ethernet offer a faster distribution time than our NFC-based approach, sending urgent broadcast information such as emergency stops is infeasible using our presented approach and needs to be done using other technologies. However, we believe that non-urgent configuration updates can be applied efficiently using our approach.

In this evaluation, we investigate the difference between using a *dedicated update robot* and using a wireless sensor network (WSN) inspired algorithm to deliver broadcast messages *without* having a dedicated update robot. The WSN algorithm we apply is the so-called *Trickle algorithm* [28] where a node sends an update until the same update information received from another node. As evaluation setting, we simulate an RCLL inspired factory floor consisting of 10 production machines and a varying number of IAMRs as shown in Fig. 4 where we consider two cases: (a) machine positions are randomized for each simulation run and (b) machine positions are fixed. We ran 1000 distinct simulations for both scenarios with the number of IAMRs ranging from 1 to 10. The results of that simulation are shown in Fig. 5 where the average time required for a broadcast to reach all machines is plotted. As shown in Fig. 5a, having more than 4 IAMRs would outperform having a dedicated update robot while also being more energy and cost efficient due to not requiring the otherwise necessary additional IAMR. When running the same simulation setting with fixed machine positions where an optimized update schedule for the dedicated update robot can easily be defined (see Fig. 4b), at least 6 IAMRs are necessary to outperform the dedicated update robot (see Fig. 5b).

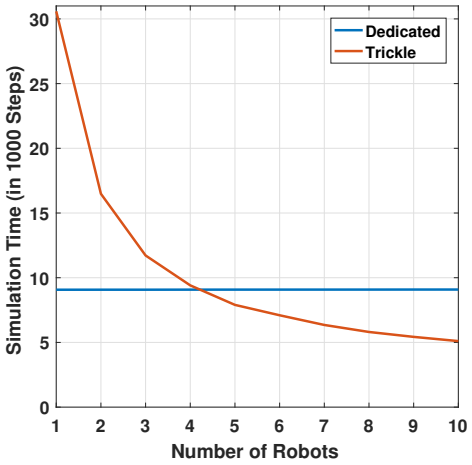
V. Conclusion and Future Work

In this paper we propose to consider NFC as an alternative to other wireless technologies in industrial contexts and RoboCup competitions. To account for the security and performance requirements of industrial data transfer, we present NFC enhancement components that can be used to equip existing as well as new devices with NFC functionality. In addition to that, we also propose a secured communication protocol that relies on AE and OTTs to provide data confidentiality, integrity, and authenticity while also mitigating replay attacks. We show the feasibility of our presented approach in terms of a security analysis as well as performance evaluations for two messaging scenarios. As future work, we plan to also evaluate WSN routing protocols regarding their efficiency if combined with our NFC-based communication approach.

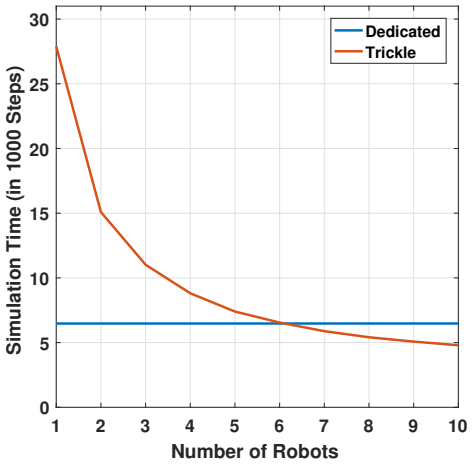
Acknowledgment

This project has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 692480. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Germany, Netherlands, Spain, Austria, Belgium, Slovakia.

IoSense is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2016 and April 2019. More information: https://iktderzukunft.at/en/.



(a) Random machine positions.



(b) Fixed machine positions.

Fig. 5: Simulation results for (a) random machine positions and (b) fixed machine positions for 1 to 10 IAMRs.

REFERENCES

[1] T. Bauernhansl, M. Ten Hompel, and B. Vogel-Heuser, *Industrie 4.0 in Produktion, Automatisierung und Logistik: Anwendung· Technologien· Migration*. Springer-Verlag, 2014.

[2] A. Willig, K. Matheus, and A. Wolisz, "Wireless Technology in Industrial Networks," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1130–1151, 2005.

[3] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and Mitigating the Impact of RF Interference on 802.11 Networks," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 4, pp. 385–396, 2007.

[4] A. L. Brandão, J. Sydor, W. Brett, J. Scott, P. Joe, and D. Hung, "5GHz RLAN Interference on Active Meteorological Radars ," in *Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st*, vol. 2. IEEE, 2005, pp. 1328–1332.

[5] B. Edwards, "Say Goodbye to Sneakernet Chores with LAN Inventory," *LAN Times*, vol. 12, no. 21, p. 85, 1995.

[6] S. Arumugam, R. K. Kalle, and A. R. Prasad, "Wireless Robotics: Opportunities and Challenges," *Wireless personal communications*, vol. 70, no. 3, pp. 1033–1058, 2013.

[7] Z. Wang, M. Zhou, and N. Ansari, "Ad-hoc Robot Wireless Communication," in *Systems, Man and Cybernetics, 2003. IEEE International Conference on*, vol. 4. IEEE, 2003, pp. 4045–4050.

[8] T. M. Chiwewe, C. F. Mbuya, and G. P. Hancke, "Using Cognitive Radio for Interference-Resistant Industrial Wireless Sensor Networks: An Overview," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1466–1481, 2015.

[9] V. C. Gungor and G. P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches," *IEEE Transactions on industrial electronics*, vol. 56, no. 10, pp. 4258–4265, 2009.

[10] X. M. Zhang, Y. Zhang, F. Yan, and A. V. Vasilakos, "Interference-Based Topology Control Algorithm for Delay-Constrained Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 4, pp. 742–754, 2015.

[11] A. Frotzscher, U. Wetzker, M. Bauer, M. Rentschler, M. Beyer, S. Elspass, and H. Klessig, "Requirements and current solutions of wireless communication in industrial automation," in *Communications Workshops (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 67–72.

[12] M. N. Rooker and A. Birk, "Multi-robot exploration under the constraints of wireless networking," *Control Engineering Practice*, vol. 15, no. 4, pp. 435–445, 2007.

[13] Y. Liu, M. Mazurkiewicz, and M. Kwitek, "A Study Towards Reliability- and Delay-Critical Wireless Communication for RoboCup Robotic Soccer Application," in *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*. IEEE, 2007, pp. 633–636.

[14] F. Santos, L. Almeida, L. S. Lopes, J. L. Azevedo, and M. B. Cunha, "Communicating among Robots in the RoboCup Middle-Size League," in *Robot Soccer World Cup*. Springer, 2009, pp. 320–331.

[15] F. Santos, L. Almeida, P. Pedreiras, L. S. Lopes, and T. Facchinetti, "An Adaptive TDMA Protocol for Soft Real-Time Wireless Communication among Mobile Autonomous Agents," in *Proc. of the Int. Workshop on Architecture for Cooperative Embedded Real-Time Systems, WACERTS*, vol. 2004. Citeseer, 2004, pp. 657–665.

[16] A. Birk and C. Condea, "Mobile Robot Communication Without the Drawbacks of Wireless Networking," in *Robot Soccer World Cup*. Springer, 2005, pp. 585–592.

[17] V. Coskun, B. Ozdenizci, and K. Ok, "A Survey on Near Field Communication (NFC) Technology," *Wireless personal communications*, vol. 71, no. 3, pp. 2259–2294, 2013.

[18] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication (NFC)," in *Workshop on RFID security*, 2006, pp. 12–14.

[19] M. Bellare and C. Namprempre, "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2000, pp. 531–545.

[20] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer Science & Business Media, 2013.

[21] N. Haller, "The S/KEY One-Time Password System," in *In Proceedings of the Internet Society Symposium on Network and Distributed Systems*, 1994.

[22] B. C. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," *IEEE Communications magazine*, vol. 32, no. 9, pp. 33–38, 1994.

[23] R. Anderson and M. Kuhn, "Tamper Resistance - a Cautionary Note," in *Proceedings of the second Usenix workshop on electronic commerce*, vol. 2, 1996, pp. 1–11.

[24] N. Tomatis, G. Terrien, R. Piguet, D. Burnier, S. Bouabdallah, K. O. Arras, and R. Siegwart, "Designing a Secure and Robust Mobile Interacting Robot for the Long Term," in *Robotics and Automation, 2003. Proceedings. ICRA'03. IEEE International Conference on*, vol. 3. IEEE, 2003, pp. 4246–4251.

[25] T. Niemueller, D. Ewert, S. Reuter, A. Ferrein, S. Jeschke, and G. Lakemeyer, "RoboCup Logistics League Sponsored by Festo: A Competitive Factory Automation Testbed," in *Automation, Communication and Cybernetics in Science and Engineering 2015/2016*. Springer, 2016, pp. 605–618.

[26] F. Zwilling, T. Niemueller, and G. Lakemeyer, "Simulation for the RoboCup Logistics League with Real-World Environment Agency and Multi-level Abstraction," in *Robot Soccer World Cup*. Springer, 2014, pp. 220–232.

[27] J. Haid, "Hardware-based solutions secure machine identities in smart factories," *Boards & Solutions*, pp. 10–13, 2016.

[28] P. Levis, N. Patel, D. Culler, and S. Shenker, "Trickle: A Self-Regulating Algorithm for Code Propagation and Maintenance in Wireless Sensor Networks," in *Proceedings of the 1st USENIX/ACM Symposium on Networked Systems Design and Implementation*, 2004.