International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 7– No.11, November 2014 – www.ijais.org

Security of Networking Control System in Mobile Robotics (NCSMR)

Rabia Moussaoui
Team Architecture of Systems
LISER-Laboratory ENSEM,
Hassan II University BP 8118
Oasis, Casablanca, Morocco

Hicham Medromi, Adil Lebbat
Team Architecture of Systems
LISER-Laboratory ENSEM,
Hassan II University BP 8118
Oasis, Casablanca, Morocco

Adil Sayouti
Team Architecture of Systems
LISER-Laboratory ENSEM,
Hassan II University BP 8118
Oasis, Casablanca, Morocco

ABSTRACT
A multi-agents system is a system composed of multiple interacting intelligent agents that can be used to solve difficult or impossible problems for an individual agent or monolithic system to solve. Multi-agents systems are open and extensible systems that allow deployment of autonomous and proactive software components. The work presented in this paper proposes a new distributed platform of autonomous control based on a multi-agent mobile system. The first section, concerns the state of the art for security and vulnerabilities of wireless systems. many vulnerabilities associated with wireless devices have been discovered since the creation and use of wireless equipment such as Bluetooth. The second section discusses these vulnerabilities and proposes solutions to secure the control architecture. Finally, the third section presents some experiences and tests with NXT robot.

Keywords
Control architecture, Remote controlled network, Mobile Robotics, Internet, Multi-Agent Systems, autonomous mobile System.

1. INTRODUCTION
For a long time, the human dream of creating intelligent machines able to perform tasks on his behalf. So, humans take less risk to dangerous tasks, or have more time to spend to leisure. networking controlled Systems in mobile robotics can be used in many "boring, dirty or dangerous activities," citing the example of robotics in dangerous environment (space, industrial, military) as the exploration of nuclear areas in this domain, the robot's mission is to explore a nuclear areas, or an inaccessible area for a human to bring us various indicators [1]. Taking the example of a nuclear power station where an increase in radiation levels occurred during an accident or during a natural disaster, the mobile robot is automatically triggered by the acquisition card data to explore areas around the nuclear power station in order to warn residents to evacuate the area. But several vulnerabilities can attack the communication between the data acquisition card and robot.

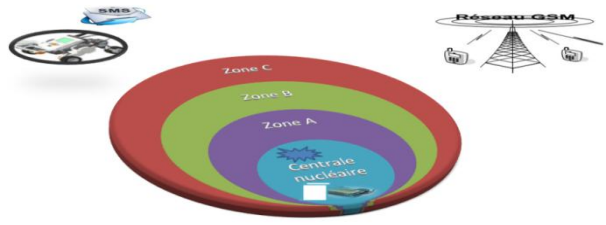


Fig 1: Exploration of nuclear areas by a mobile robot

2. PROBLEMATIC
To achieve its mission the robot must be autonomous and communication between it and the data acquisition card must be secured, the development of autonomous robot has forced us to develop architectures that include different modules. For communication security, many vulnerabilities associated with wireless devices have been discovered since the creation and use of wireless equipment such as Bluetooth. One gap in the communication protocol which is a specific vulnerability to wireless networks is denial of service battery. As elements of a wireless network are nomadic, they are dependent on a limited energy source. A major DoS attacks is to overburden the machine to attack in order to consume as soon as possible its energy. Another problem which is not as simple to implement, is the attack "man in the middle" to steal identification keys and encryption before the start of a session and use the same to personify and / or listen to communications. This problem, however, is not specific to Bluetooth. Most systems major exchanges are prone to this type of attack.

A problem of identity hacking is still possible when using a link key based on the "key unit" where it is quite easy to steal the identity of a caller. Assuming that A and B communicate based on the "key unit" of A, a third speaker C can contact A and get the key. C can therefore use the Bluetooth address of B to masquerade as him.

3. STATE OF ART

3.1 Network-Controlled System
A system is called "network-controlled system" when it communicates with control algorithms and diagnosis through real time communication medium. With this kind of system, new issues must be considered [2]. In particular, it is necessary to control and adapt the communication system and / or application. Both approaches should be considered:

- Control and monitor the network to meet the specifications required by the application [3]: the goal is to better manage communications from a required quality of service QoS [4]. This approach is named "control of the network".
- Adaptation of the application to network performance [5]: in this approach, the goal is to secure the application performance despite the lack of communication mean (ie stability, robustness and fault tolerance). You can also integrate modes "degraded" to tolerate and be especially robust to

problems generated by the network. This approach has the name of "control over the network."

These two approaches are complementary and today their combination is interesting to have more security of communication. In this case it is referred deco-design or co-design. Then, the service quality is considered simultaneously with the desired system performance [6].

3.2 Control Loop

A mobile robot is controlled by a control loop, as illustrated in Figure 2. Iteratively, this loop is reading the data received by the sensors, interprets, calculates and sends motor commands to the actuators. Typically, this loop is executed about ten (10) times per second; the frequency may vary depending on the types of sensors and actuators used. The control loop is not unique; used according to the architecture; it can be decomposed into several sub-loops to control arranged in different ways [7] [8].

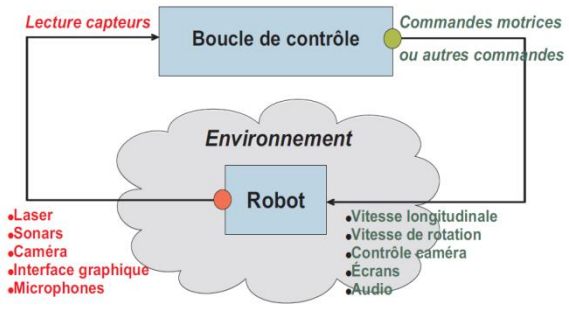


Fig 2: Control Loop

3.3 Communication security in wireless protocol

3.3.1 The security controller

Mechanisms and security policies that can be supported by Bluetooth as mentioned above are possible through a component called the security controller (Security Manager) [10]. The security controller is the entity that decides which policies are applied when a connection request is made. Based on service, device type and level of reliability, security controller may require application-level authentication, encryption of the session and any other specific access policies [9].

The security controller needs information about devices such services before making a decision. This information is stored in the two databases including the device database and the service database.

1 - The system database stores information about the type of device, its reliability and the length of link key used for encryption.

2 - The service database stores information about authentication requirements, authorization and encryption for services

The typical process followed by the security controller by providing access to a device for a particular service is as follows:

1 - The remote device requests access

2 - The connection request comes to L2CAP

3 - L2CAP request to the security controller to grant access

4 - The controller asks the device and service databases

5 - If the device is reliable, so the security controller may or may not require authentication or authorization

6 - If the device is not reliable, the security controller can close the connection or impose authorization. The level authentication occurs when Bluetooth link keys are exchanged. According to the security policy access, the security controller could invite an application protocol for enforcing security application level such an arrangement username / password for authentication. Support is also included for other authentication schemes by the controller interface security.

7 - The security controller will then decide whether the access service requires encryption link. If so keys are negotiated and exchanged at the L2CAP connection and continue to be established protocol. Alternatively, if the device is in security mode 3, the security controller asks the LMP to authenticate and encrypt the communication before the connection is established. The general architecture of Bluetooth security is presented in the following figure:

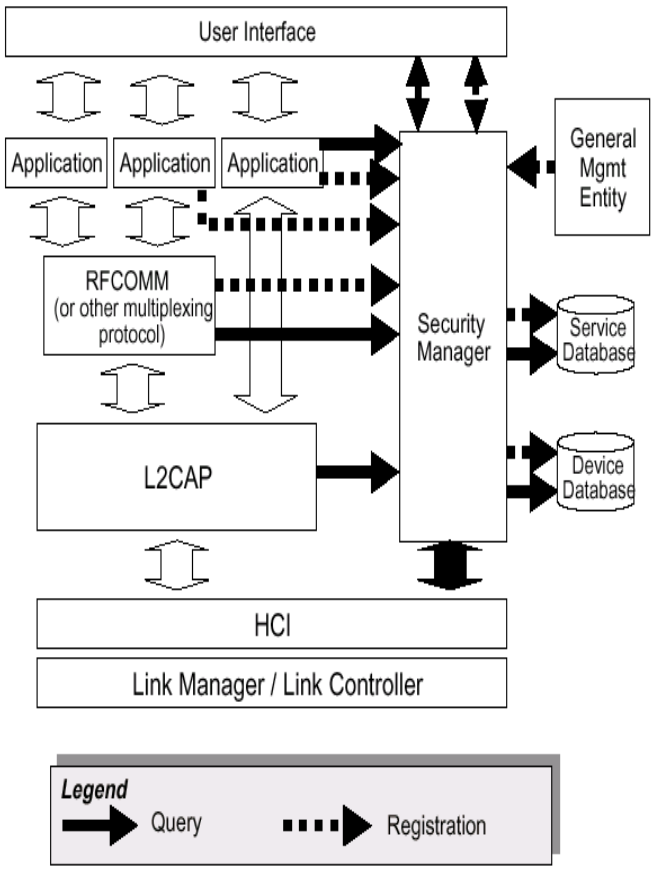


Fig 3: General architecture of security in Bluetooth

4. SECURITY MODE

Depending on the characteristics of Bluetooth, the devices can operate in one of three security modes:

• Security Mode 1: Unsecured;

• Security Mode 2: Secure the application level;

• Security Mode 3: Secure at the link layer.

Mode 1: This mode is the less secure in which the Bluetooth device does not run any security method. A Bluetooth device in this mode is a mode of network discovery. It allows a Bluetooth device to offer its services to all Bluetooth devices within range.

Mode 2: This mode allows securing in software by setting the Bluetooth device Bluetooth profiles. It imposes security after the establishment of the link between devices at L2CAP level. This mode allows the establishment of flexible security policies with controls application layer protocols running parallel to the lower layers.

Mode 3: This mode operates in the link layer of the OSI model, it imposes security controls such as authentication and encryption at the Baseband layer is identical to mode 2 but adds functions of authentication and encryption before the connection is established.

5. COMMUNICATION SECURITY APPROACH

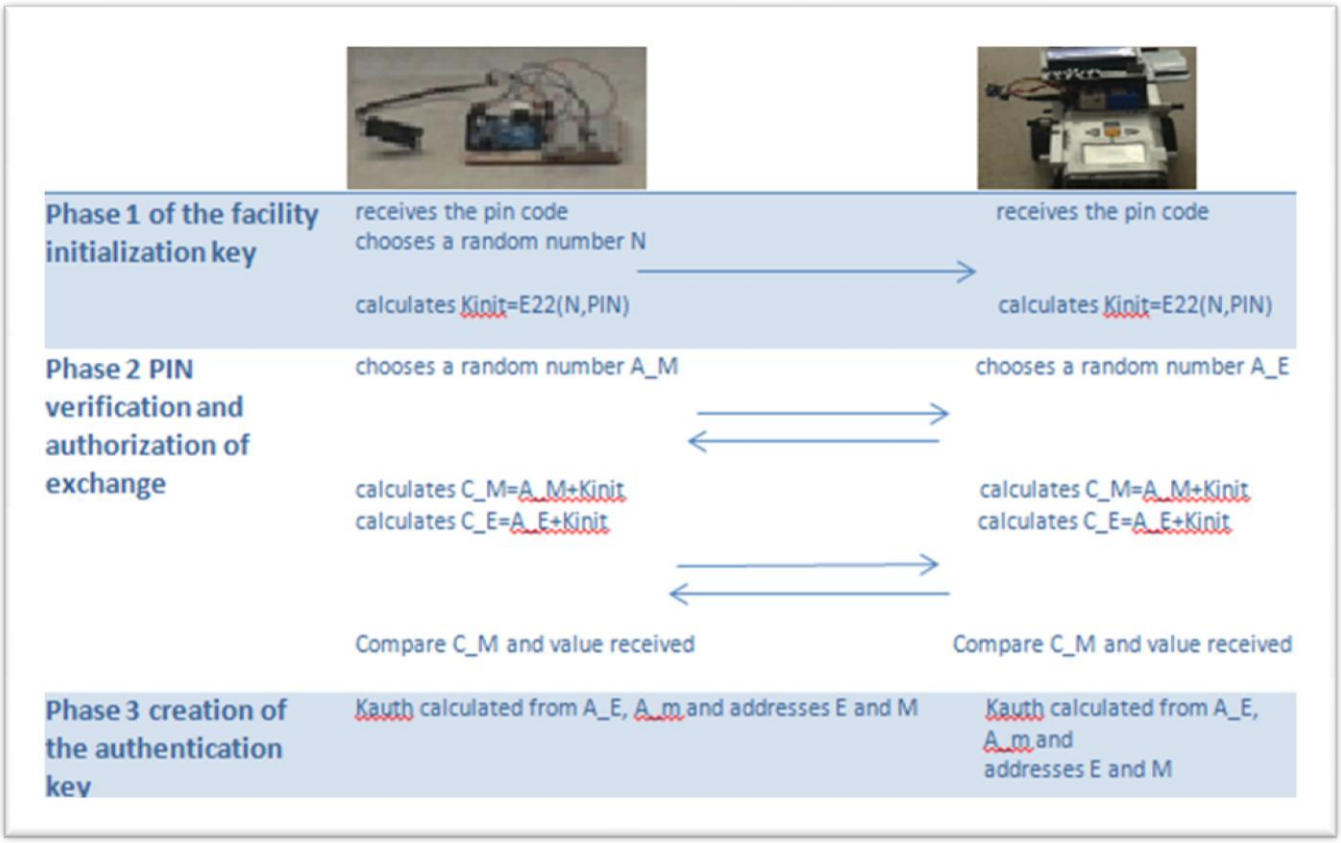
Bluetooth security protocol that we have adopted is based on the use of the following three parameters:

- A random number RAND to simulate the random 128-bit. It changes frequently and is produced by the Bluetooth device.

5.1 Encryption and Privacy Procedures

After the link key had been established and the authentication was successful, the encryption key is generated by the E3 algorithm and Bluetooth encryption system is ready to systematically encrypt the payload for transmission. The encryption process involves a binary encryption seed E0 which is used for data encryption [11].

The binary seed E0 consists of three elements; the primary key generator, the key generator payload and component of encryption / decryption [12]. The main register of the bit string contains four records, known as Linear Feedback Shift Register (LSFR). These records are of lengths 25, 31, 33 and 39 giving a total length of 128 key. The Payload generator combines the input bits in the appropriate divisions and shifts to the four registers of the main generator of the binary key. E0 takes as parameters; the Kc which is the encryption key generated by E3, a random number, the device address BD_ADDR and the device clock A. By using the output of E0 algorithm, KSTR, and data to transmit. The encrypted text is Formulated in data packets for transmission.



- Dependent address of the physical device BD-ADDR (Bluetooth Device Address): Every Bluetooth card is assigned a permanent and unique 48-bit address during construction. This address allows others to trust in the person at the other end of the communication.
- Personal identification code PIN: This is a personal code that is assigned to the user. This PIN can be stored on 1-16 bytes. The PIN can be stored in non-volatile memory device. These parameters are used to create keys for authenticating and encrypting data transfers to secure them.

5.2 Security Control Architecture

This architecture includes an explicit representation of the cooperation process agent with other agents in the system.

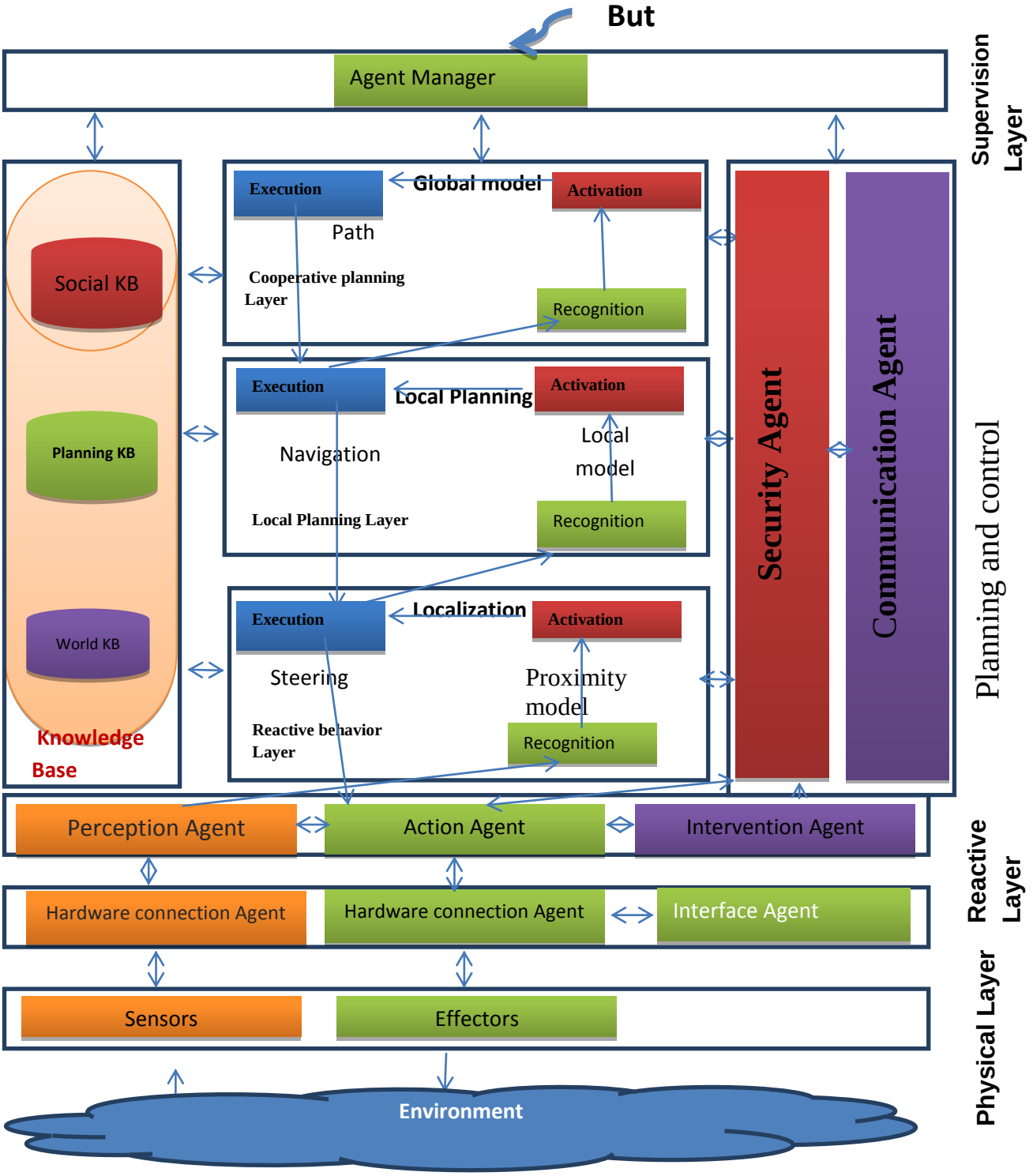


Fig 5: Security Control Architecture

The reaction layer includes collection agent which allows the perception after treatment to determine the location of the mobile unit and to create representations of the environment [13]. For the perception of the environment, several modules can perform the execution of a different action, to choose the most appropriate action; the modules are organized in hierarchical layers [14], each layer having a different priority. The upper layers represent more abstract tasks that are detailed with tasks more concrete and simple, the upper layers with a priority less than the lower layers. The lower layers correspond to simple tasks and they have a higher priority [15]. The action agent defines the sequence of actions leading

to the goal by the remote user, the location of the mobile system, the current action, the representations of the environment and their validity.
Communication agent allows through different communication protocols (internet, radio, Bluetooth,...) to control the system, while going through the security agent that encrypts and decrypts data.

Security Agent:

• It enables the secure transmission via the encryption.
• Responds to a risk.
• It ensures the integrity: data must be as safe and reliable, and should not be altered accidentally or intentionally.
• Ensures confidentiality: only authorized agents have access to information that is intended for them. Unwanted access must be prevented.
• Ensures availability: the system must function flawlessly during the periods of use, ensuring access to services and installed with the expected response time resources.
• It ensures authentication: agent identification is fundamental to manage access to relevant areas of work and maintain confidence in the exchange relations.

Finally, with the layer of control, mobile system can monitor and make decisions. There is a hierarchy that is connected with the knowledge base and layers of planning. Each level of abstraction gives information to the next level.

6. TESTS AND EXPERIENCES

In the first step, a random number is generated at the acquisition card and PIN will be sent with the mobile robot, it is calculated using an algorithm E22, which will also be made at the acquisition card and send to mobile robot that will compare the value received with the result, once this stage is reached, the authentication key will be created at the base of the robot ID, name, random number and PIN. To secure communication, capture card launches investigation passkey robot concerned to alert him to go explore the affected areas, once it verifies the key to looking robot, the robot will automatically move to the area.

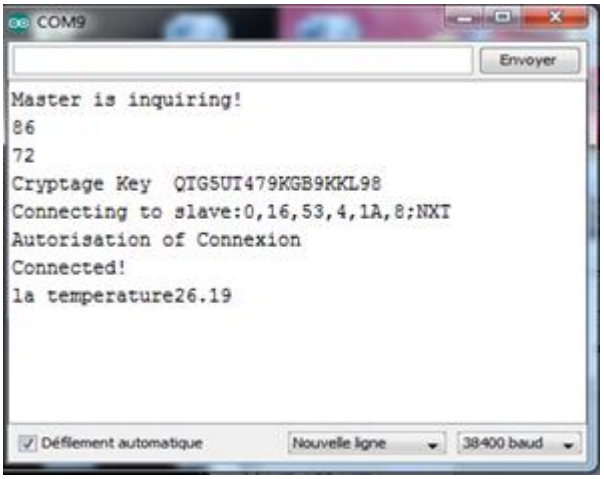


Fig 6: Connection between the card and the robot

➔ Automatic launch NXT robot

The NXT robot starts automatically by an alert on static acquisition card which localizes in the nuclear power station, the robot starts to areas where the population is condensed to measure radiation levels and temperature, after that an SMS is send to evacuate the areas.

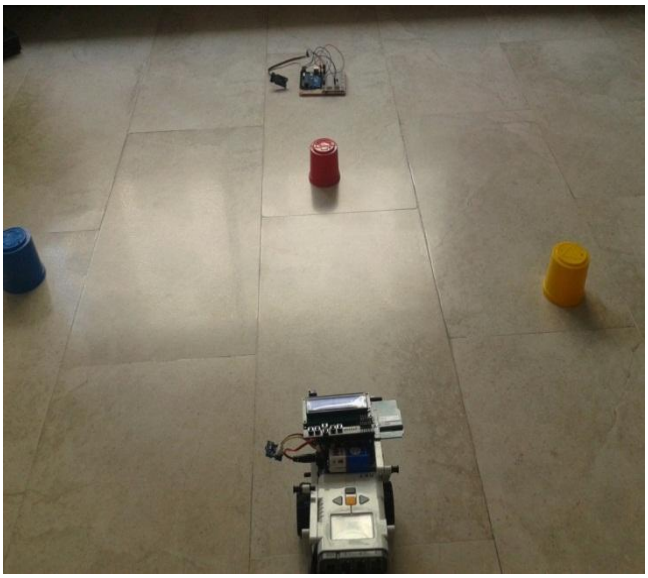


Fig 8: Launching the robot to areas at risk of radiation

The data acquisition card (Arduino) and the NXT robot communicate using Bluetooth protocol. To secure the communication of some vulnerabilities, this application opted for security controls such as authentication and encryption at the Baseband layer, before the connection is established. The two Bluetooth devices are coupled using a symmetric key. This step enables the robot and the Arduino board to share a secret key used to encrypt and decrypt data. This secret key is designed using an algorithm implementing the physical address of paired devices, random number but above sesame permanently stored in hardware (PIN, password, etc ...). Symmetric sesame required when pairing operation reports directly to the device used.

The key combination: combination Key KAB, This is among the link key, KAB is derived from two Bluetooth devices, bluetooth module, Arduino Card and NXT Robot. It is produced for each pair of devices and is used when more security is required.

The encryption key: encryption key, can change from 8 to 128 bits, it ensures safe passage for every packet transmitted between devices during the transfer session. This key is derived from the current link key, and each time encryption is required, it is regenerated again.

7. CONCLUSION

This work, have shown the vulnerabilities that can attack the networks controlled systems in mobile robotics and some solutions to secure the control architecture system. The multi-agents systems can be used for designing and developing distributed autonomous and intelligent architectures in different fields like remote control, security and telecommunications. The implementations presented in this paper validate the choice of the multi-agents systems.
In perspectives, one of the major challenges of the network controlled system that is the constraint energy data acquisition boards will be detailed. And also the platform will be used beyond mobile robotics.

8. REFERENCES

[1] Éric Beaudry, 2006, « Planification de tâches pour un robot mobile autonome », Chapitre 4, page 21, Mémoire présenté au Département d'informatique FACULTÉ DES

SCIENCES UNIVERSITÉ DE SHERBROOKE, Québec, Canada, août 2006.

[2] J.Zhao, H.Liu,W.LI. 2013, Periodic Data Prediction Algorithme in Wireless SensorNetworks. Communication in Computer an Information Science,Volume 334 (2013), 695-701.

[3] Boissier, O.,Gitoon,S. et Glize,P. 2004, Caractéristques des systèmes et des applications. In Systèmes multi-agents. TEC DOC, 2004.

[4] R.Moussaoui, H.Medromi, 2011, 3ème édition des Journées Doctorales en Technologies de l'Information et de la Communication (JDTIC 2011) ENSA de Tanger, « Architecture de la localisation des systèmes mobiles en utilisant les SMA (système multi agent) ».

[5] A. Albore, E. Beaudry, P. Bertoli et F. Kabanza, 2006 : Using a contingency planner within a robot architecture. à paraître dans Proceedings of Workshop on Planning, Learning and Monitoring with Uncertainty and Dynamic Worlds, in conjunction with the 17th European Conference on Artificial Intelligence.

[6] A.Sayouti,F.Moutaouakkil,H.Medromi, 2012, «The Interaction-Oriented Approach for Modeling and Implementing Multi-Agent Systems», International Review on Computers and Software (I.RE.CO.S), Vol. 5, N. 2,March 2012.

[7] A.Sayouti,F.Qrichi-aniba,H.Medromi, 2009, «Modeling Autonomous Mobile System with Agent Oriented Approach», International Journal of Computer Science and Network Security (IJCSNS), Vol. 9, N. 9, pp. 316 à 321, Septembre 2009.

[8] F.Moutaouakkil, H.Medromi, 2012, "Developping Multi-agent System Robotics" Journal of Materials Science and Engineering- 2012.

[9] M.Luk, G. Mezzour, A.Perrig, V.Gligor. MiniSec, 2007: a Secure Sensor Network Communication Architecture. In Proceedings of the 6th International Conference onInformation Processing in Sensor Networks, ISBN:978-1-59593-638-7, 479.

[10] H.Mansouri, F.Moutaoukil,H.Medromi. 2014, An autonomous intelligent gateway for wireless sensor network based on mobile node. International Journal of Advanced Computer Science and Applications (IJACSA) IJACSA, Volume 5 Issue 3, March 2014.

[11] H.Mansouri, S.Benhadou, H.Medromi. 2012, Energy security optimization in wireless sensor network based on multiagent system architecture. International Review on Computers and Software (I.RE.CO.S.), Vol.7, n. 2 (2012).

[12] H.Mansouri,H.Medromi,A.Sayouti. 2012, A GSM based remote wireless automatic monitoring of mobile robot , International Journal of Research and Reviews in Computer Science (IJRRCS)Vol. 3, No. 3, ISSN: 2079-2557, June 2012.

[13] Sayouti, A., Qrichi Aniba, F., Medromi, 2008, *Tele-robotic over Internet Based on Multi-agents System*, International Review on Computers and Software (I.RE.CO.S), Vol. 3, N. 6, pp. 666 – 671, November 2008).

[14] R.Moussaoui, H.Medromi, F.Moutawakil, 2014, International Review on Computers and Software (I.RE.CO.S.), Vol. 9, n 1 January 2014, ISSN 1828-6003, Page 74, " Design and Modeling of SMA Architecture Using MaSE Methodologies ".

[15] R.Moussaoui, H.Medromi, H.Mansouri, 2013, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 5, September-October 2013, SSN 2278-6856, "Planning architecture for control of an intelligent agent ".