Networking technologies for robotic applications

Vibekananda Dutta
Faculty of Power and Aeronautical Engineering
Warsaw University of Technology
00-665 Warszawa, Poland

Teresa Zielinska
Institute of Aeronautics and Applied Mechanics
Warsaw University of Technology
00-665 Warszawa, Poland

Abstract— **The ongoing progress in networking security, together with the growing range of robot applications in many fields of everyday life, makes robotics tangible reality in our near future. Accordingly, new advanced services, depends on the interplay between the robotics and cyber security, are being an important role in robotics world. This paper addresses technological implications of security enhancement to the Internet of Thing (IoT) – aided robotics domain, where networked robots are expected to work in complex environments. The security enhancement suggested by the NIST (National Institute of Standards and Technology) creates a security template for secure communications over the network are also discussed.**

Keywords— Robots; Security policies; Robotic applications; Internet of Thing (IoT).

I. Introduction

In the field of safety, security and IoT-aided robotic applications the number of devices involved in Machine-to-Machine (M2M) communication is expected to steadily grow in next few years. Research and applications trends are leading to the appearance of the IoT-aided robotic applications [1]. Tele-operation of mobile robots requires wireless communication, what increasingly involves multi-robot network and complex transmission of heterogeneous data.

This position paper, highlights the technological implications including communication security caused by Internet cloud techniques used in robotic systems.

During our recent visit, 2014 IEEE-RAS summer school and workshop on response robotics (Fig. 2 - a), we observed that IoT-aided robotics applications are growing in the cyber-real world crossing, where humans, robots and security enhancement interact in co-operative basis. The National Security Agency (NSA) has published security specification for IoT-aided robotic applications to be preciously implemented in this complex cyber physical world.

It addresses three important security features: (1) communication, (2) authentication, and (3) cyber security policy development and enforcement [2]. The main challenges in the wireless robotics, is the integration of the different intelligent capabilities in to an overall system that support all two teleoperation stages (Fig. 1) [3].

Starting from these premises, and with related to IoT-aided robotic applications, this position paper:

a) envisions possible scenarios: (1) building smart, (2) pervasive, and (3) secure environments.

b) highlights the need for improvising the key concepts of security, privacy, and trust.

c) provides a state of the art, with particular refernce to the following features: (1) communication networks, (2) network security, and (3) robotic applications in distributive and persive environments [4].

The following sections of this paper are organized as follows: in section 2, the authors give an overview of IoT-aided robotic applications. In section 3, the authors discussed network interfacing for robotic applications. In section 4, feasibility of proposed architectures in current IoT-aided robotic applications is introduced. In section 5, wraps up the discussion. Finally, section 6, gives the conclusion.

II. Envisaged IoT-aided robotic applications

In modern world, IoT-aided robotic applications have been successfully applied in several domains, specifically in rescue robots, assisting robots, health care robots, in industrial plans and in the so called smart areas. Nevertheless, few works are carried out on the interaction between these two fields, likely, robotic applications and IoT-aided domain. However it needs more in depth investigation.

Most of the modern robots platforms are equipped with rich sensory sets, complex hardware with advanced computing and communications capabilities. This, make them able to execute complex and coordinated operations. Technology that

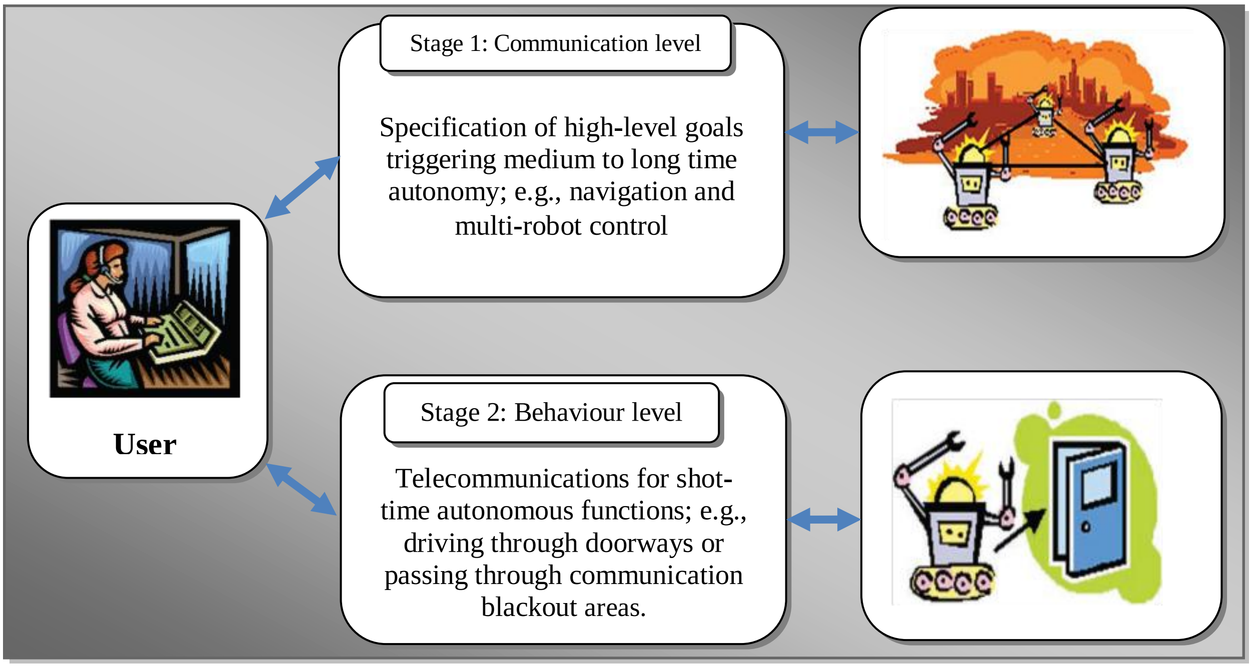


Fig. 2. Mobile robots - two levels of information procession. Communication concerns the high level within the whole group. Behaviour (behavioural level) – mean local decision making network.

(a)

(b)

(c)

Fig. 1. IEEE-RAS workshop in Perth, Australia [9] – a. Typical examples of IoT-aided robots: our laboratory bomb disposal and rescue robot Seekur Jr [10] – b, australian bomb disposal robot, Australia [11] – c. Both robots can operate fully autonomously and perform a coordinated exploration of the area.

makes robots human-friendly and adaptable to different scenario is emerging in several robotic applications [5, 6, 7].

The networked and user interfaced robots, such as rescue robots, human assisting robots, health care robots and robots for military applications, have been identified by the U.S.A. National Institute of Standards and Technology (NIST) (in collaboration with Department of Homeland Security - DHS) as a class of devices in which the hardware, software, including security functions must be developed concurrently [8]. Demonstration, test, and evaluation are crucial in this area because of application of many emerging technologies, Fig. 2-b, c present's examples of robots for technologically demanding tasks.

III. NETWORK INTERFACING FOR ROBOTIC APPLICATION

A fundamental issues that researchers focus in the networks and interfaces domain in robotic applications, is the system integration when the components use different Machine-to-Machine (M2M) communication standards. To this direction are going several EU FP7 research projects [12], such as BETAAS and OPENIOT [13, 14] are focusing: on cloud computing techniques, on security issues, on context aware approaches, and on semantic-oriented design (another examples are RELYONIT [15], ICORE [16], IOT.EST [17], EBBITS [18], and VITRO [19]).

On the other hand, with reference to IoT-aided robotic applications several important, not yet answered questions should be dealt with [20]:

a) to what extent IPv6 (Internet Protocol version 6-ecent), and Transport Layer Security (TLS) standard can be used to deal with complex robotic systems.

b) can the semantic of data excahnge over the network be directly embedded at the Media Access Control (MAC) layer, with aims of enforcing security, privacy, and integrity.

c) robotic communication systems are extremly heterogeneous, thus deserving further research on congestion avoidance, reliable routing mechanisms [21], and on efficient real- time handling of the big data amount.

The secure networking, allows robots to access a huge amount of data, Transport Layer Security (TLS) is the cryptographic protocol suggested by the NIST for secure communication. TLS is put on the top of traditional protocols like e.g., TCP [22, 23]. About 2010, the term cloud robotics has been introduced [24], it is novel paradigm in robotic applications, where robots can take the advantages of the Internet network as resource for massive parallel computation and for almost real time knowledge sharing [25, 26].

In the structure of the mobile robot-Internet interface shown in Fig. 3, the robot subscribes the information from the cloud, and its sensors - including vision; deliver the information to the cloud (they are publishers).

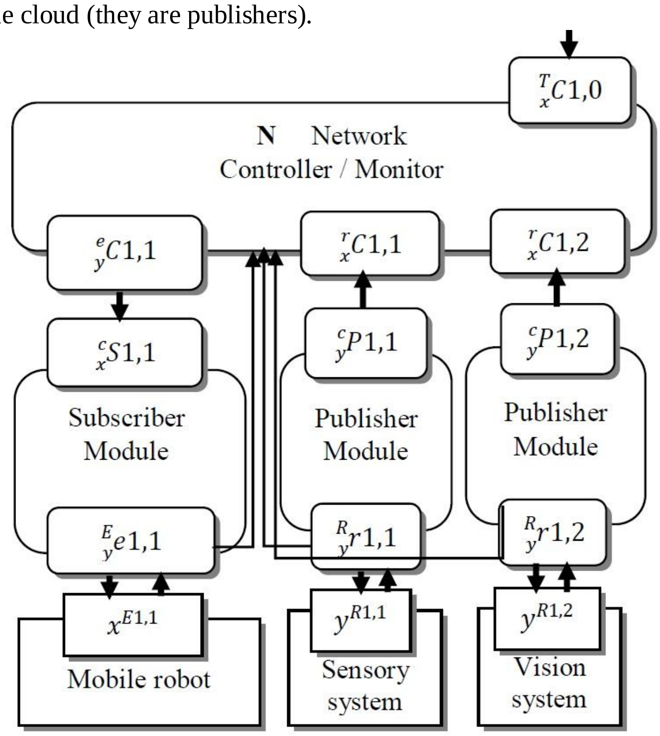


Fig. 3. Shows the structure of mobile robot- Internet interface proposed using the concept proposed in [42, 28] and adapted in [31].

In the figure the symbols mean the following:

N – Network controller / monitor,

${}^{T}_{x}C1{,}0$ - cloud data buffers / data packages,

${}^{r}_{x}C1{,}1, {}^{r}_{x}C1{,}2$ - network controller interfaces for publishers,

${}^{e}_{y}C1{,}1$ - network controller interfaces for subscriber,

$x^{E1,1}, y^{R1,1}, y^{R1,2}$ - lower layer network interfaces,

${}^{R}_{y}r1{,}1, {}^{R}_{y}r1{,}2$ - lower layer input buffers of the publishers (sensors, vision),

${}^{E}_{y}e1{,}1$ - lower layer output buffer of the subscriber (of the robot,

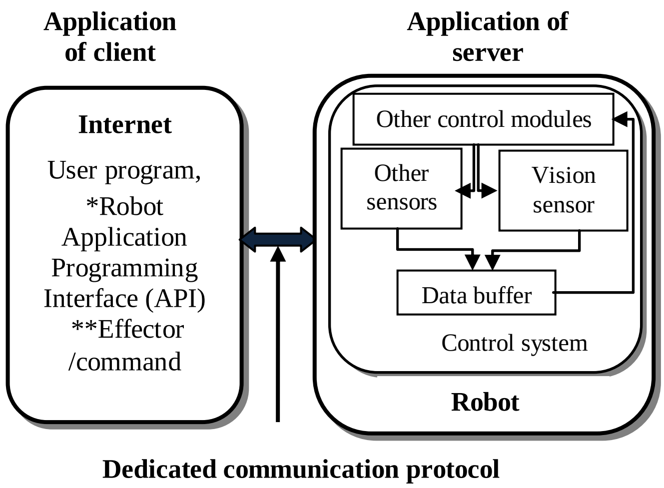
${}^{r}_{y}P1{,}1, {}^{r}_{y}P1{,}2$ - higher layer output buffers of the publishers with Quality of Service (QoS) mechanisms,

${}^{c}_{x}S1{,}1$ – higher layer input buffer of the subscriber with Quality of Service (QoS) mechanisms.

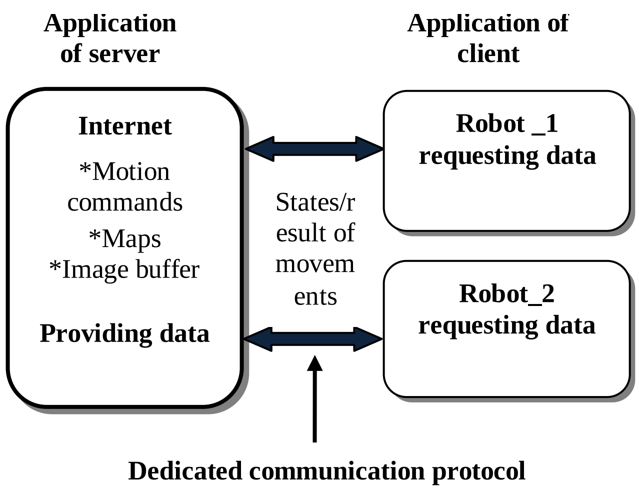
The publisher / subscriber module sends the acknowledgement of status information, Quality of Service (QoS) requirement, and QoS feedback to the network monitor establishing communication between Machine-to-Machine (M2M) and Machine-to-Cloud (M2C) respectively.

IV. Feasibilty of proposed architectures in current IoT-aided robotic applications

This position paper cannot conclude without addressing the important question if current technologies are mature enough to let sufficient network interfaces in robotic applications.



(a)



(b)

Fig. 4. General concept of internet architecture: communication medium between client (Internet) and server (Robot) – a, communication medium between server (Internet) and client (Robot) – b.

The internet is the data storage. In this case, the robots are clients requesting the data, and the internets are server providing it data. The data can be different types: (1) motion data, (2) maps, (3) image buffer and so on (Fig. 4-b). On other side, when the internet is the client and robot is the server is used when controlling multi robots, because all the decision and motion strategies are provided in internet cloud (Fig. 4-a).

Taking into account of above, the authors presented the features of most current diffused robots (see Table. 1), trying to address this question with reference to the different scenarios. Nowadays there are several robots available in the markets designed for a wide spectrum of IoT-aided robotic applications [27, 6]. According to [29], specialized robots are classified to two categories: service robots and field robots, executing supportive task for humans (e.g., domestic, personal mobility assistance, and rescue). The International Federation of Robotics (IFR) [43] expects that nearest future will bring, a rapid development of field robots, what - due to high level of such robots complexity and autonomy will stimulate the development of new communication techniques.

Table-1 proposes an outlook on the current commercialized robots belonging to both service robots and field robots categories, taking into account type, principal features, network interfacing [44], and application areas. Such information can be explicitly revealed from the references (freely downloaded from the corresponding websites).

V. Discussion

This position paper identified the challenges concerning IoT-aided robotic applications, with particular reference (Table-1) to their technological and scientific implications. Basis on the state of art the following observations, important for developing the robotic oriented Internet tools were made:

a) robots are expected to act in complex scenarios (e.g., outdoor environments), the short-range communication methods, sematic-based services, information centric networking, and security problems are here significant [20].

b) the largest challenge for wireless communications over the network are the links quality, when controling by cloud many moving robots [30].

c) there is the need for protocol able to deliver messages in a secure manner within the secure network in outdoor sceanrios with user-robot interfacing, while assuring a high communication effeciency with high transmission and processing speed. Due to hazards in the networks traffic conditions, such requirements is difficult to achieve [45].

d) it is needed to investigate a secure communication in order to achieve goals in complex scenarios. Information Technology (IT) is required also the introduction of specific netwrok interfaces that cloud indentify untrusted devices with inhibit their actions within the whole system.

VI. Conclusion

In this paper, the authors addressed challenging topics in IoT-aided robotic applications: (1) communication networks, (2) network interfacing and (3) security policies. Those problems with reference to the traditional communication networks with information centric architecture are very worth to investigate. In-addition, the redefinition of security – primitive's represents cornerstone of the network interfacing techniques for IoT-aided robotics-world. Nevertheless, to fully exploit the potential of advanced technology in the next years, a solid effort in both protocols and applications design is required in order to make the envisioned IoT-aided robotics world a reality in the near future.

TABLE I. ROBOTS ENABLING THE ENVISAGED IOT – AIDED ROBOTIC APPLICATIONS

Type of robots	Model	Description	Network interface	Computational Mobility	Applications
			WiFi / Ethernet		
Humanoid	NAO [32]	Support for human-robot interaction activities, in wide range of indoor environments.	Supporting both features	Medium	Health care, Home
	REEM [33]		Supporting both features + 3G (UMTS)	High	Health care, Home, Industrial
	PR2 [34]		Supporting both features	Medium	Home and Research
Domestic / Service	Care-o-bot 3 [35]	Assisting humans in their daily life activities and also in industrials environments.	Supporting both features	High	Health care, Home, Industrial
	PeopleBot [36]		Supporting both features	High	Home , Industrial
	StockBot [37]		Only supporting WiFi features	Medium	Industrial
Field / Ground	Husky [38]	General purpose robots for both indoor and outdoor environments. Also used for R &D section.	Supporting both features	High	R &D, Military, Rescue
	Guardian [39]		Supporting both features	High	R &D, Military, Rescue
	Pioneer 3-AT [40]		Supporting both features	Medium	R &D, Military
	Seekur [41]		Supporting both features	High	Military, Rescue, bomb disposal
Marine	Kingfisher [42]	Control marine areas.	Supporting both features	High	Military, Rescue

ACKNOWLEDGMENT

This work was supported by the HERITAGE project (Erasmus Mundus Action 2 Strand 1 Lot 11, EAECA/42/11) funded by the European Commission.

REFERENCES

[1] M. R. Palattela, N. Accettura, X. Vilajosana, T. Watteyna, L. Grieco, G. Boggia and M. Dohler, "Standardized protocol stack for the internet of (imptotant) things," *Communications Surveys & Tutorials, IEEE*, vol. 15, pp. 1389-1406, 2013.

[2] H. King and B. Hannaford, "Breaking the Interoperabitlity Barrier through Emmerging Standrads in Teleoperation, Technical Report," University of Washington, 2009.

[3] J. Abouaf, "Trail by Fire; Teleoperated Robot Targes Chernobyl," *IEEE Comp. Graphics Applications*, vol. 18, no. 4, pp. 10-14, 1998.

[4] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Brihhs and R. Braynard, "Networking named content," in *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*, 2009.

[5] M. Rooker and A. Brik, "Multi-Robot Exploration under the Constraints of Wireless Netwroking," *Control Engineering Practice*, vol. 15, no. 4, pp. 435-445, 2007.

[6] S. O. and B. Khatib, in *Springer handbook of Robotics*, Springer, 2008.

[7] C. Chien, K. Kim, B. Liu and M. Gen, "Advance decision and intelligence technologies for manufacturing and logistics," *J.Intell. Manufact*, vol. 6, no. 23, pp. 2133-2135, 2012.

[8] A. N., "Workshop on Future Directions in Cyberphysical Systems Security," Department of Homeland Security.

[9] http://wiki.ssrrsummerschool.org/doku.php?id=2014:home

[10] http://tmr.meil.pw.edu.pl/index.php?/pol/Laboratorium-Robotyki/Elementy-laboratorium-badawczego-robotyki/Duzy-robot-mobilny

[11] http://www.abc.net.au/news/2010-02-03/the-nt-police-bomb-disposal-robot-rolls-out-in/322020

[12] http://ec.europa.eu/research/fp7/index_en.cfm

[13] http://www.betaas.eu/

[14] http://openIoT.eu/

[15] http://www.relyonit.eu/

[16] http://www.IoT-icore.eu/

[17] http://www.ebbits-project.eu/

[18] http://ict-IoTest.eu/

[19] http://www.future-internet.eu/activities/fp7-projects.html

[20] G. L.A, R. A., C. S., S. S., P. G. and P. D. Di, "IoT-aided robotics applications: Technological implications, target domains and open issues," *Computer Communications*, vol. 54, pp. 32-47, 2014.

[21] Z. L., E. D., J. V. and Z. B., "Named data netwroking (ndn) projects," NDN-0001, 2010.

[22] H. C.M, "Assessing the Scalability of a Multiple Robot Interface," in *ACM/IEEE Int'l. conf. Human-Robot Interaction (HRI'07)*, New York, 2007.

[23] C. C., E. C., F. M. and R. R., "Guidelines for the selection and use of Transport Layer Security (TLS) Implementations," NIST Special Publication 800-52, 2005.

[24] K. J., "Cloud-enable robots," in *IEEE-RAS International Conference on Humanoid Robotics*, 2010.

[25] G. E, "Cloud robotics: connected to the cloud, robots get smarter," *IEEE spectrum.*

[26] R. Arumugam, V. Enti, L.Bingbing, W. Xiaojun, K. Baskaran, F. Kong, A. Kumar, K. Meng andG. Kit, "Davinci: a cloud computing framework for service robots," in *IEEE International Conference on Robotics and Automation*, 2010.

[27] Z. L., W. K. and V. d. L. H., "Special issue on assitive robotics [from the guest editors]," *IEEE Atomation Magazine*, pp. 16-19, 2013.

[28] C. Zielinski, T. Kornuta and T. Winiarski, "A Systematic Method of Designing Control Systemsfor Service and Field Robots," in *19-th International Conference on Methods and Models in Automation and Robotics (MMAR)*, Poland, 2014.

[29] B. Andreas, S. Soren and K. Pathak, "A netwroking framework for teleoperation in safety, security and rescue robotics," *IEEE Wireless Communications*, 2009.

[30] V. Dutta and N. Kesswani, "Designing vision based autonoumous Docile-x mobile robot for real time applicatiosn in soccer behaviors," *Journal of Automation, Mobile Robotics and Intelligent Systems*, vol. 8, no. 4, pp. 40-51, 2014.

[31] https://community.aldebaran-robotics.com/doc/

[32] http://pal-robotics.com/en/products/reem/

[33] https://www.willowgarage.com/pages/pr2/overview

[34] https://www.care-o-bot.de/en/care-o-bot-3/hardware/technical-data.html

[35] http://www.mobilerobots.com/ResearchRobots/PeopleBot.aspx

[36] http://pal-robotics.com/en/products/stockbot/

[37] http://www.clearpathrobotics.com/husky/tech-specs/

[38] http://www.robotnik.es/web/wp-content/uploads/2014/06/Robotnik_Guardian-e1.pdf

[39] http://www.mobilerobots.com/ResearchRobots/P3AT.aspx

[40] http://www.mobilerobots.com/ResearchRobots/Seekur.aspx

[41] http://www.clearpathrobotics.com/kingfisher/tech-specs/

[42] Kornuta T. and C. Zielinski, "Robot control system design exemplified by multi-camera visual servoing," *Journal of Intelligent and Robotic Systems*, vol. 77, no. 3, pp.499-524.

[43] http://www.ifr.org/

[44] T.Y and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in: IEEE Symposium on Security and Privacy, 2003, pp.110-122.

[45] M. Blaze., J. Feigenbaum, J. Lacy, "Decentralization trust management," in :IEEE Symposium on Security and Privacy, 1996, pp.164-173.