HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

POSSIBILITIES AND SECURITY CHALLENGES OF USING IOT FOR MILITARY PURPOSES

A DOLGOK INTERNETÉNEK KATONAI ALKALMAZÁSI LEHETŐSÉGEI ÉS BIZTONSÁGI KIHÍVÁSAI

BOGNÁR Eszter Katalin

ORCID: 0000-0002-3697-7871

bognarek@uni-nke.hu

Abstract

The most recognizable shift in the age of the modern warfare is that information became the most effective weapon of all. The situational awareness based on the collected information became the core of every military operations. Information operations as a new domain entered the battlefield, the integrated network of sensors, weapon systems and platforms became force multiplier. In the advent of new technologies, new tools and processes appeared based on the concept of network-centric warfare. The aim of this article is to introduce the possibilities of using IoT for military purposes and to discover the IoT related security challenges and their potential countermeasures focusing on the devices and technologies used in the military IoT domain.

Keywords: *internet of things, information security, military sensors*

Absztrakt

A modern hadviselés kapcsán leginkább szembetűnő változás az információ, mint fegyver megjelenése. A katonai műveletek alapját a megszerzett információ révén elérhető helyzetértékelési képesség adja. A harctér kibővült az információs dimenzióval, a szenzorok, különböző fegyverrendszerek és platformok közötti koordináció erősokszorozó képességekkel bír. A technológiai fejlődés hatására új eszközök és eljárások jelentek meg a hálózatközpontú hadviselés koncepciójához kapcsolódva. A cikk célja bemutatni az IoT katonai alkalmazási lehetőségeit, a katonai alkalmazások sajátosságait, valamint feltárni az IoT alkalmazásának biztonsági kihívásait és a lehetséges megoldásokat, különös tekintettel a védelmi szférában alkalmazott IoT eszközökkel szemben támasztott speciális követelményekre.

Kulcsszavak: *dolgok internete, információbiztonság, katonai szenzorok*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.03.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.09.29.

INTRODUCTION

The function of recently developed technology of Internet of Things (IoT) is based on interaction, communication between different smart devices/equipments/applications using mostly wireless, radiofrequency technology. The devices that may be part of more complex systems act as smart devices taking decisions about specific context using the possibility of sharing and aggregation of information with other objects. The application of IoT has several important advantages in different applications in civil life like precision agriculture, regulation of public traffic, smart home, healthcare etc.

The military and defense sector has been recently recognized the possibilities of IoT. The introduction of paradigm of network-centric warfare directed the traditional military thinking to new directions and created a new basis for military application of extended communication networks. As the military decision cycle focuses on the information obtained from data to plan different military operations, therefore the defense sector is highly interested in the newest technologies to develop further its information processing technology including information collection, processing and transfer. The modern military operations take place in complex, continuously changing multidimensional environment, and the commanders have less and less time to evaluate information, elaboration of operation plan and taking decision based on all relevant information.

One possible solution of these challenges is the introduction of IoT in the military sector. The modern military equipments have larger and larger data processing and communication capabilities that form complex military information network integrated into military information infrastructure. These systems can be used to obtain more precise situational picture, but also in medical and logistical application.

However, several contraindications were expressed against the adaptation of these new technologies, particularly respecting the data security. The defense mechanisms in traditional computer networks are insufficient due to the high complexity of systems, the limited resources of sensors, not reliable communication links and the remote management. More research is required to identify specific security problems of the technology and to elaborate possible solutions. The aim of this article is to present the military application possibilities of IoT, features of military applications, the security challenges of applications and different solutions of IoT particularly the special requirements for IoT devices applied in defense sector.

DEFINITION, TECHNOLOGICAL BACKGROUND AND MILITARY APPLICATION POSSIBILITIES OF INTERNET OF THINGS

Internet of Things, new communication technology from the XXI. century

The recently developed technology of Internet of Things is based on the connection of several, different separated electronic devices that enables the automatic communication and sharing of information between them. However, until now there is not any exact definition for the Internet of Things due to its very fresh profile. The 2015 IEEE initiative provides a good basis for understanding this new concept and its aim is to give an overview about architectural requirements of development and a well-accepted definition for IoT [1]. The most cited definition was provided in 2017 by Gartner informatics research and consulting company: „The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.” [2]

The technological background of IoT

The IoT includes several separated technologies, like embedded systems, computer networks, cellular network, wireless communication technologies, sensor networks, data analysis, cloud-technology and four important elements contributed significantly to their widespread application:

- the development of microelectronics;
- the development of wireless communication;
- the increase of data storage and data elaboration capabilities;
- introduction of software and platforms for data processing.

Table 1 shows the IoT technological stack [4] and the technologies applied at different levels of the stack, respectively. The different endpoint devices are located in the sensing layer at the bottom of the stack. The produced sensors have smaller size and more resources due to the development of the microelectronics. The production of different, even nanometer sized intelligent devices is now possible, therefore there is a large heterogeneity. The architecture, computing capabilities, power resources, data-storage capability of different devices are highly different that makes the interoperability very difficult between them.

The network layer provides smooth communication between the devices using new protocols based on wireless, radiofrequency communication technology. Several different technologies were used by these applications including the Wi-Fi connection, and low bandwidth and shorter-range communication protocols optimized for sensors with lower, constrained resources (e. g. ZigBee, Bluetooth LE, 6LowPan). While for traditional networks several widely accepted de facto standards have been evolved, for the IoT several alternative competing technologies exist. This is highly challenging for the implementation of secure communication between the devices, e.g. the incorrect implementation of ZigBee protocol that is widely used in automation of buildings represents a high security risk [5].

The increase in the number of network devices is automatically accompanied by dramatic increase in the data volume generated by the devices. This large data volume often considered as big data should be stored and processed in real time. The new big data analysis technologies and the cloud technology have contributed significantly to the implementation of these technologies. The widely used cloud technology may solve the problem of efficient management of big data by providing scalable computing capacity and storage volume. There are software and services in the application layer provided by third-party that make the implementation of secure IoT operation even more difficult [3].

IoT layer	Technologies
Sensing layer	Sensor-networks, RFID, cameras, radars etc.
Network layer	ZigBee, Bluetooth, Wi-Fi, 6LoPAN, mobile-networks, GPS etc.
Application layer	smart home, energy/power management, self-driving cars, cloud technology etc.

Table 1 IoT three-layer stack (based on ref. [4])

Present and future military applications of IoT technology

As the military decision cycle focuses on the information obtained from data to plan different military operations, therefore the defense sector is highly interested in the newest technologies to develop further its information processing capabilities including information gathering, processing and transfer to defined person.

The introduction of the network-centric warfare paradigm [20][23] directed the traditional military thinking to new directions and created a new basis for military application of extended communication networks. Although the military application of IoT is still in its early stages, the NATO and US department of defense show large interest in it. The 2015 NATO initiative has started a relevant IST-147 research group under the name „Military applicability of IoT" aiming to identify the possibilities and tentative risks of military application of IoT technology.

In this part several military application areas are described, where the IoT devices have been already introduced or most likely will be introduced. More detailed descriptions are found in the following studies: Zheng and Carter [8], Tortonesi [7] and Fraga-Lamas [9] and Kollár [11].

Logistics

One of the most important applications of sensors in the defense sector is the logistics. The application of this new technology can revolutionize the military capability, the efficiency of the logistic management, precision, reliability, accountability can be improved, and the expenses can be reduced.

One of the most important systems is RF-ITV[1] system of US military [13] that applies RFID labels and satellites to monitor the position and condition of military cargo from sender to the destination. The shipping data are combined and processed with data from the movement detector system (MTS[2]) equipped with localization information that ensures the communication between convoys and web-based maps and report give support for logistic units. The US military labels weekly 16000 shipments with the RF-ITV system based on 2010 data that forms the largest RFID-based shipment monitoring system all around the world.

Fire-control system

The automatic system controlled by sensors is used first for fire-control systems. These systems use sensor data to react even faster and more precise to new events. The integrated marine ballistic missile defense system Aegis applies high performance computer and radar technology to monitor and aim at enemy targets.

It was used first time by US Marine Corps and was followed by deployment by Australian, Japanese, Spanish, Norwegian and Korean Marine Corps. The high preciseness AN/SPY[3] radar system can detect, monitor and direct missiles completely automatically and simultaneously to 100 different targets [8].

Military training

The IoT technology can be applied even during military training. The different combat situations can be modeled by virtual reality. The positions and physiological condition of soldiers are detected by sensors during the military training. The obtained video- and audio-data can be evaluated later anytime.

One of the simulation systems used by several armies including the US army and Hungarian Defense Forces is the MILES[4]. It can simulate real combat situations like the well-known laser tag game. The sensors attached to the uniform of the soldier detect the laser light, count the

[1] RD-ITV – Radio Frequency In-Transit Visibility –
: https://trainer.rfitv.army.mil/login/Login.do
[2] MTS – Movement Detection System –
: http://www.alu.army.mil/alog/issues/julaug05/success_mts.html
[3] AN/SPY radar – http://missiledefenseadvocacy.org/missile-defense-systems-2/missile-defense-systems/u-s-deployed-sensor-systems/anspy-1-radar/
[4] MILES – Multiple Integrated Laser Engagement

detections and provides a sound signal. The newer version of MILES is more complicated and can simulate combat situation with combined arms [8].

Health monitoring

The different sensors play an important role also in the health monitoring of individual soldiers. The soldiers are equipped with special helmets with integrated control-sensors to detect concussion and other brain traumas. Small, intelligent telemetric health monitoring and healthcare devices are more and more frequently used in combat situation, therefore the first aid/healthcare service can be provided without any staff for soldiers. The Tempus Pro [17] deployed by US, British and Norwegian Army is an advanced system that can monitor virtual signals. Figure 1 depicts the field operation of Tempus Pro equipment by a soldier.

Figure 1 Field operation of Tempus Pro [17]

Energy management, smart military bases

The IoT technology can be applied in military application and build smart military bases using the concept of smart cities that are already introduced to practice. The smart military bases would be such facilities that are able to optimize the energy resources of the military bases using the inherent properties of the technology. These bases would contribute to the comfort feeling of the employer of the base, monitor the different events in the base and register the entry and exit of the staff. Small projects aiming the optimization of energy support were already running like the 2015 NATO Smart Energy[5] initiative that had a military operation in military training base in Bakony-mountain in Hungary.

Intelligence, C4ISR

The application of IoT technology has the higher benefit in case of C4ISR systems. The C4ISR[6] systems use several millions of sensors on different platforms to ensure developed situational awareness. The highly complex and widespread network including several millions of sensors (sensors in different platforms like unmanned aerial vehicles, radars, video-cameras, infrared or passive infrared sensors, unattended ground sensors, portable devices) provides real time data for combat troops and decision makers. These data can be integrated and used for a common operational picture supporting the decision making by commanders, improved coordination and control on the operational area.

[5] NATO Smart Energy: http://www.natolibguides.info/smartenergy/documents
[6] C4ISR - C4: Command, Control, Communications and Computers –
ISR: Intelligence, Surveillance and Reconnaissance

The energy saving property and lifetime of devices are highly crucial in real combat situation, therefore further development of different hardware, communication protocols and software elements is required for optimization of energy management of devices. The currently running DARPA N-Zero project [14] aims to extend the lifetime of sensors connected to a network in real combat situation from months to years.

The design and operation of devices should fill all requirements related to architecture of military equipments and transfer capabilities. Tactical networks are required that enables encrypted communication and hardly decipherable data transfer. On the other hand, the rate of data transfer of these networks is significantly smaller than that of cellular networks.
Some research projects aim to develop solutions using wideband radiofrequency that fills the IoT requirements. The project granted to Harris has a function to develop new generation radio system [21] for combat situation. The system serves simultaneously more than 200 users and enables high-speed data transfer, while it fulfils special military purposes and encrypting requirements. The high number and different types of data represent a great challenge for the data processing [22].

The concept of combat soldier using intelligence network appeared during the US Nett Warrior program that developed persistent Android devices for US army [8]. These devices correspond to the military equivalent of the commercially available Samsung Galaxy Note II smartphones with the function to enable more precise information via combat military applications like Blue Force Tracking, 3D maps and targeting applications. The main C4ISR data integration platform of US army, the Distributed Common Ground System (DCGS)[7] analyses and combines the data obtained from sensors located in different platforms and gives an overview about position and arrangement of friendly and enemy troops ensuring better coordination and control in combat situation.

IoT technology in Hungarian Defense Forces

Hungary as all other NATO members should be able to participate in network centered operations therefore the Hungarian Defense Forces should be interested in and adapt new technologies.

Although the implementation of IoT technology for Hungarian Defense Forces has not done yet due to mainly financial reasons, but several initial steps to this direction can be already recognized like the participation in NATO Smart Energy program, the smart border barrier with different types of sensors on the Hungarian-Serbian border to control the illegal migration [19], or the MILES system used in the military training. The Zrínyi 2026 defense and development program, which started in January 2017, might eliminate these financial problems as in accordance with the decision of the Hungarian government the military expenses of the budget increases by 0.1% of the GPD each year providing a good basis for rational developments and implementations. Although there is not sufficient public information about the plans of the program, but several acquisitions are expected based on the main tasks of military organizations in 2018 (5/2018, II. 23), and the directive of the Ministry of Defense about the most important trends during the period 2019-2020 [18]. That could help the digitalization of the Hungarian Defense Forces and the introduction of new technologies like the IoT. Today, the greatest challenge for the Hungarian Defence Forces is the protection of the country's borders, which can ensure the defence of the country's population against the illegal immigration, smuggling and terrorism. The application of smart IoT sensors, e.g. acoustic and seismic unattended ground sensors buried in the ground could significantly improve the detection rate of the already

[7] DCGS – Distributed Common Ground System

installed smart fence on the Hungarian-Serbian border. Further possibilities of IoT are the development of a modern, network-integrated custom equipment system that can increase the combat ability of the soldier in the Hungarian Defense Forces [31] and the sensor application in the case of unmanned aerial and ground vehicles.

Summary

The Table 2 summarizes the initial adaptation of IoT technology and the military applications that were described in more detail in this section.

IoT application area	Relevant systems	Applied technologies
Logistics	RF-ITV	RFID, geolocation, RF detector, cloud
Fire-control systems	AEGIS	radar, laser, sensor-networks, geolocation, cloud
Military training	MILES	geolocation, virtual reality, sensors operating in different sensing ranges, servers
Healthcare and health monitoring	Tempus Pro	biosensors, servers
Intelligence, C4ISR	Distributed Common Ground System (DCGS) Nett Warrior	radar, laser, sensor-networks, geolocation, cloud
Energy management, Smart military bases	NATO Smart Energy	Sensor-networks, cloud

Table 2 IoT solutions and technological background used in defense sector

SECURITY CHALLENGES AND POSSIBLE SOLUTIONS

Introduction

The most important concern related to the IoT technology in both civil and military area is the data security. More and more devices are connected in a large extended network and the increase of number of devices and the system complexity provides increasing number of different types of security risks.

It is highly remarkable how important is data security in the IoT strategy of USA [24] and NATO [10] and how the most important strategic principles are postulated for the introduction of IoT devices in military application or the development, operation of special military IoT technologies:

- already during the planning phase should be considered the data security and built-in in the system;
- continuous security updates and vulnerability management;
- following proven practices for the realization of data security;
- facilitating the sharing of proven practices;
- the interoperability should be supported between different devices;
- the education of informatics and data security should be supported.

Features of IoT systems from data security and data protection perspective

As all other new technologies, the Internet of Things represent several challenges besides the undeniable benefits. As the IoT is tightly connected to communication and information technology, therefore the challenges of information security and data protection should be met. Although there are many similarities between the traditional communication systems and IoT

systems, but in point of view of data security and data protection large deviations are expected due to the special features of IoT technology. The common protection mechanisms used in traditional systems (firewalls, IDS/IPS[8] systems etc.) are usually not always sufficient.
In spite of traditional communication systems, the IoT technology has the following features [6]:

- high-number of devices;
- heterogeneous networks;
- the devices can be anywhere and are difficult to protect;
- problems with the limitation of energy resources;
- the increasing number of information results in an urgent challenge to establish reliable data security;
- the intrusion or attack could be more efficient and detrimental due to the high-number of connections between systems;
- dynamic characteristics of systems.

The number of smart devices organized in network exceeds currently the total population of the earth. This represents a great challenge as the network has high-number of heterogeneous nodes and devices: the devices with different energy management, different communication protocols and hardware and software-components made by different producers that makes the implementation of defense mechanisms used for classical systems very difficult.

While the servers and workstations for classical systems are localized in a well-protected inner unit, the PCs, notebooks, sensors in different sizes can be found everywhere and difficult to protect against damages and theft. The IoT devices operate usually with accumulator or solar cells and have low computing capacity and memory. The devices with limited resources are not suitable to handle systems with complex security solutions like complicated encrypting algorithms. The main element of Internet of Things is the universal informatics: the daily used devices became part of our life, collect data about us and share these data by connecting with other devices. All these data transfers represent mostly underestimated potential risk for data security.

The increase in the number of devices organized in a network generates larger and larger volume of data those protection and supplement with user access require more sophisticated solutions. While the extent of tentative attack extends to the border of the system, the security risks affect broader range and include more serious damages in case of IoT technology due to the informatics solutions that are used generally. Further challenge originates from the dynamic, self-organizing property of networks whereby different devices can connect and disconnect anytime to different networks, thus the corresponding data security anti-measure should be always adjusted accordingly.

Cyber-attack against military IoT systems and possible protection mechanisms

The largest drawback of IoT technology is the serious risks in data security. Several studies try to find solutions to problems of different types of vulnerability. As this complex system includes several different technologies, therefore the variation of possible attacks is remarkable high as well. One of the most organized methods of intrusion is the decomposition of IoT technology into layers and the analysis of possible intrusions in individual layers.

This section demonstrates the intrusion possibilities in three layers of IoT occur in military systems (sensing layer, network layer, application layer) and the possible countermeasures

[8] IDS/IPS – Intrusion Detection System/Intrusion Prevention System

against the intrusion (Oracevic, A. et al.[25], Mouaatamid, El. O. et. al.[26], Andrea, I. et al.[27], Jing, Q. et al.[28] and Wrona, K. [29]).

Intrusion in the sensing layer

One of the most vulnerable points of military system for intrusions is the sensing layer. This layer is responsible for data collection and those data collection sensors works in this layer that play also role in data collection and transfer. The sensors of the sensing layer should prevent different types of physical attacks like damage of data collection units and shortening of the lifetime and functionality of sensors. Among in the previous section presented applications areas, the RFID and the intelligence sensor-networks without surveillance represent enhanced risk, because these systems consist of physically exposed sensors with limited resources that communicate with low density performance signal.

The most important intrusion types:

- tampering of nodes: tampering of all or parts of nodes, introduction of new legal node or access to nodes data via electronic or physical connection (USB connection);
- jamming: The intruder perturbs with high density signal the radiofrequency communication between nodes. The node is unable to fulfill its function and it denies finally the service (Denial of Service - DoS);
- physical damage;
- sleep deprivation attack: The most sensing nodes of the IoT system are supplied with replaceable elements, and in absence of communication it switches to sleeping mode to prolong the lifetime of the battery. The intrusion keeps the nodes awake that induces more energy consumption, therefore the nodes are discharged faster.

There are several modes of protection against intrusions in the sensing layer:

- secure boot, node validation: the software and hardware should be validated by low calculation demanding encrypting algorithms;
- checking the data integrity and reliability: A diagnostic tool should be installed in all devices to ensure that data are not damaged, and the data transfer should be achieved with encrypting mechanism;
- the built-in data deleting mechanisms could protect against physical intrusion and data theft

Intrusions in network layer

The communication between nodes is achieved in data transfer media. As it is about very important, confidential data therefore is highly crucial to ensure the confidentiality, integrity and accessibility of the data.

The main types of intrusions in network layer:

- spoofing: the intruder identifies itself as another user of the network and gets unauthorized access to special data;
- sinkhole attack: the intruder deviates the network traffic to one specific target, therefore the data are not transferred to the original address (DoS), and furthermore sometimes they are diverted to an unauthorized user;
- man in the middle attack: The intruder influences the communication between two sensor nodes via the network and monitor the data transfer and collects data;
- denial of service: The network node is bombed by high number of requests therefore it becomes unable to fulfill its function;
- eavesdropping: The enemy detects and decrypts messages between the devices in the network.

There are different types of validating mechanisms as protection measure against intrusion in the detector layer like safety routing solutions and encrypting between end-to-end connections.

Intrusion in the application layer

Trojans, viruses and spy programs can steal, tamper data or results in deny of services via running malicious scripts in the application layer by damaging the devices of the IoT system and the confidentiality of data stored in the system. The intrusion detecting systems, access control lists, key management and firewalls are potential protecting tools against these intrusions. The application of private clouds decreases significantly the risk, but several important factors should be taken into account by operation of cloud services by third-party. Figure 2 summarizes the most important intrusions and possible countermeasures.

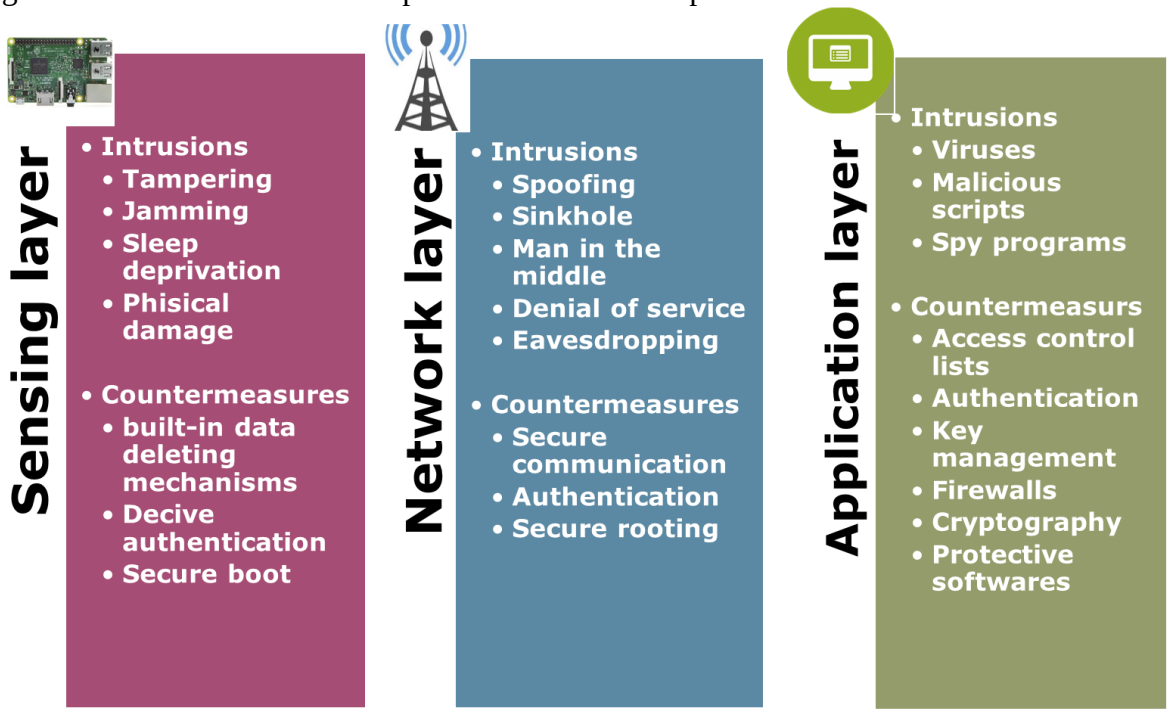

Figure 2 The most important intrusions and possible countermeasures (Made by the author)

SUMMARY

The widespread application of Internet of Things will influence significantly the military operations in the future. The application of smart sensors installed on weapon system on different platforms like ships, unmanned fighters, ground vehicles offers new possibilities for the army. The efficiency of military operations, the quality of different services can be enhanced and cost reduction and saving of human life can be achieved. The commanders can take real time decisions based on IoT technology by meaning of complex military information networks that can be used efficiently for acquiring of more precise situational picture and informational superiority.

The new technology described in this paper offers significant developments in several different military application areas. The recent projects in the comprehensive virtual simulation of military training, the networking soldier, smart health monitoring/healthcare, self-driven vehicles, smart logistic systems, smart military bases, smart energy management, integrated intelligence analysis systems mark the initial trend and important developments on this field is expected in the future.

The most important drawback of the widespread military application of IoT technology is the high vulnerability of these complex systems. Although some research projects have been started on this field, but until now no sufficient safety mechanisms fulfilling the demand of the IoT technology have been elaborated. The recently available solutions focus on the adaptation of mechanisms of traditional PC networks to the devices with smaller energy resources (small cryptographic algorithms with low calculation demands, diagnostic methods, optimized routing solutions in the point of view of energy consumption). I share the opinion that the implementation of comprehensive data security requires a new approach. The project of DARPA LADS [30] is a new, revolutionary initiative, which does not follow the traditional protecting mechanism avoiding the limitation due to the limited energy resources of IoT devices. The program focuses on the development of such a technology that are suitable to associate different types of physical changes like electromagnetic radiation, power fluctuation, thermal output changes to the function of the device. These patterns could serve as a reference later. The abnormal change of the physical modality can be an indicator of the incorrect operation, eventually an intrusion into the system. This problem is a hot-field in the military application research, as the information control provides the most important advantage. The different IoT technologies offer very attracting solutions for this demand. Hungary as a member of the NATO should participate also in this inevitable digitalization development.

REFERENCES

[1] IEEE Internet Initiative: Towards the definition of the Internet of Things (IoT), https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (letöltve: 2018. 04. 28.)

[2] HUNG, M., Gartner: Leading the IoT: Gartner Insights on How to Lead in a Connected World, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf (letöltve: 2018. 04. 28.)

[3] IHS Markit: IoT trend watch 2018, https://ihsmarkit.com/Info/0118/iot-trend-watch-2018.html (letöltve: 2018. 04. 28.)

[4] ZHAO, K., GE, L. (2013). A survey on the internet of things security. Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013, 663–667.

[5] ZILLNER, T., STORBL, S.: ZigBee exploited: The good, the bad and the ugly. Black Hat USA, 2015 https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf (letöltve: 2018. 04. 29.)

[6] KAMRANI, F., WEDLING, M., RODHE, I.: Internet of Things: Security and Privacy Issues, FOI Swedish Defence Research Agency, Defence and Security, Systems and Technology, 2016. FOI-R--4362—SE, https://www.foi.se/report-search/pdf?fileName=D%3A%5CReportSearch%5CFiles%5C0317a384-8808-414a-9e4c-95743fc22436.pdf (letöltve: 2018. 04. 28.)

[7] TORTONESI, M. et al.: Leveraging Internet of Things within the Military Network Environment – Challenges and Solutions. In: Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, 2016, pp. 111-116.

[8] ZHENG, Denise E. – CARTER, William A.: Leveraging the Internet of Things for a More Efficient and Effective Military; A Report of the CSIS Strategic Technologies Program, Rowman & Littlefield, Lanham, 2015.

[9] FRAGA-LAMAS, Paula – FERNÁNDEZ-CARAMÉS, Tiago M. – SUÁREZ-ALBELA, Manuel – CASTEDO, Luis – GONZÁLEZ-LÓPEZ, Miguel: A Review on Internet of Things for Defense and Public Safety. In: Sensors, Vol. 16. Issue 10., 2016, 1644, doi:10.3390/s16101644, http://www.mdpi.com/1424-8220/16/10/1644/pdf (letöltés ideje: 2018.01.07.)

[10] TONIN, M.: The Internet of Things: Promises and Perils of a Disruptive Technology, NATO Report, 2017. https://www.nato-pa.int/document/2017-internet-things-tonin-report-175-stctts-17-e-bis (letöltve: 2018. 04. 29.)

[11] KOLLÁR Csaba.: Az IoT katonai felhasználási lehetőségei és fejlesztés irányai. In: Hadmérnök, XII. évf. 4. szám, 2017, pp. 146-158. http://hadmernok.hu/174_15_kollar.pdf (letöltés ideje: 2018.01.07.)

[12] US DOD and NATO plan Battlefield Internet of Things connecting sensors, wearables, weapons, minitions, platforms and networks for information dominance, http://idstch.com/home5/international-defence-security-and-technology/cyber/internet-things-battlefield/?print=pdf (letöltés ideje: 2018. 05. 01.)

[13] Defense Industry Daily: RFID Technology: Keeping Track of DoD's Stuff, 2010, https://www.defenseindustrydaily.com/rfid-technology-keeping-track-of-dods-stuff-05816/ (letöltés ideje: 2018. 05. 01.)

[14] International Defence, Security & Technology: DARPA's N-Zero extends the lifetime of IoT devices and remote sensors from month to years, 2017, http://idstch.com/home5/international-defence-security-and-technology/technology/energy/darpa-s-n-zero-program-will-allow-unattended-wireless-sensor-network-monitoring-for-years/ (letöltés ideje: 2018. 05. 01.)

[15] BROWNE, J.: Strong Defense Depends On a Technological Edge, 2017, http://www.mwrf.com/systems/strong-defense-depends-technological-edge (letöltés ideje: 2018. 05. 01.)

[16] HAASE, N.: Distributed Common Ground System–Future: Moving into the 22nd Century Today, JFQ 77, 2nd Quarter, 2015, http://ndupress.ndu.edu/Media/News/Article/581879/distributed-common-ground-systemfuture-moving-into-the-22nd-century-today/ (letöltés ideje: 2018. 05. 01.)

[17] Tempus Pro: Tempus Pro: https://www.rdtltd.com/products/tempus-pro-advanced-vital-signs-monitor/ (letöltés ideje: 2018. 05. 01.)

[18] 5/2018. (II. 23.) HM utasítás a honvédelmi szervezetek 2018. évi feladatainak, valamint a 2019-2020. évi tevékenysége fő irányainak meghatározásáról

[19] BOGNÁR E.: Szenzorhálózatok határvédelmi alkalmazása, HADMÉRNÖK XII: (3) pp. 175-187., http://hadmernok.hu/173_16_bognar2.pdf (letöltve: 2018. 05. 02.)

[20] HAIG ZS., KOVÁCS L., VÁNYA L., VASS S.: Elektronikai hadviselés. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[21] HARRIS: US Special Operations Command Awards Harris Corporation $255 Million IDIQ Contract for Next-Generation Manpack Radios. https://www.harris.com/press-releases/2017/06/us-special-operations-command-awards-harris-corporation-255-million-idiq (letöltés ideje: 2018.01.07.)

[22] MARIANI, Joe – WILLIAMS, Brian – LOUBERT, Brett: Continuing the march: The past, present, and future of the IoT in the military. https://www2.deloitte.com/insights/us/en/focus/internet-of-things/iot-in-military-defense-industry.html (Letöltve: 2018.01.07.)

[23] DEAKIN, Richard S.: Battlespace Technologies – Network-Enabled Information Dominance. Artech House, Boston, 2010. ISBN: 978-1-59693-337-8

[24] US Department of Homeland Security: Strategic principles for securing the internet of things (IoT), 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf (letöltés ideje: 2018. 05. 02.)

[25] ORACEVIC, A. et al.: Security in Internet of Things: A Survey, In.: Proceedings of the International Symposium on Networks, Computers and Communications (ISNCC), Morocco, 2017

[26] MOUAATAMID, EL O. et al.: Internet of Things Security: Layered classification of attacks and possible Countermeasures, E-Ti: Electronic Journal of Information Technology, Issue 9, pp. 66-80. 2016.

[27] ANDREA, I. et al.: Internet of Things: Security vulnerabilities and challenges, In.: Proceedings of the IEEE Symposium on Computers and Communication (ISCC), Cyprus, 2015.

[28] JING, Q. et al.: Security of the Internet of Things: perspectives and challenges, Wireless Networks, Volume 20, Issue 8, pp. 2481–2501, 2014.

[29] WRONA, K.: Securing the Internet of Things A Military Perspective, In: Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015.

[30] DARPA LADS: https://www.darpa.mil/program/leveraging-the-analog-domain-for-security (letöltve: 2018. 05. 02.)

[31] GÁCSER Z.: A katona harci képességét növelő korszerű, hálózatba integrált egyéni felszerelésrendszerének kialakítási lehetőségei a Magyar Honvédségben, Budapest: ZMNE, 2008. (PhD értekezés)