Application of IoT in Military Service

Renuka C. Sonare
Department of Electronics & Telecommunication
Government College of Engineering,
Chandrapur, Maharashtra, India

Dinesh V. Rojatkar
Department of Electronics & Telecommunication
Government College of Engineering,
Chandrapur, Maharashtra, India

ABSTRACT

Internet of Things (IoT) links the objects of the real world to the virtual world, and enables anytime, anywhere connectivity for anything that has an ON and OFF switch. It constitutes to a world where physical objects and living beings, as well as virtual data and environments, interact with each other. Large amount of data is generated as large numbers of devices are connected to the internet. So this large amount of data has to be controlled and converted to useful information in order to develop efficient systems. In this paper, we focus on to an application of IoT in military service that is used to reduce the time and increase speed. IoT based intelligent transportation systems, deffense & security, Industry & most important Health monitoring system are designed to support the Smart City vision & various field which aims at employing the advanced and powerful technologies for the administration of the people and many service.

Keywords: Internet of Things, defense and public safety, smart city, Health monitoring system, Industry, Transporation

1. INTRODUCTION

The Internet of Things (IOT) is today's commercial effort to integrate a wide variety of technical and commercial information-generating components to provide new business opportunities based upon device and system intelligence. This technology is the large scale commercialization of technology that has been developed and proven by the U.S. Department of Defense over the past fifteen years. In much the same way as NASA and the early space program in the 1960s spurred innovations in chip technology, automation, propulsion, and miniaturization that developed into innovative consumer products, solutions developed from the concept of network-centric warfare translate directly to the foundations of today's commercial IOT. One response to these challenges is to introduce the concept of Internet of Things (IoT) into the military domain. The Internet of Things is extensively developed world-wide with a focus on civilian applications. IOT is a paradigm that considers the pervasive presence of a variety of smart things/objects in the environment. By means of wireless and wired connections, they are able to interact and cooperate with each other to create new applications/services in order to reach common goals. Objects/things make themselves recognizable and can behave intelligently by making context related decisions thanks to information aggregation and sharing with other objects. Furthermore, they can be components of complex services. However, the integration of heterogeneous sensors and systems diverse in technology, environmental constraints, and levels of fidelity is a challenging issue not only for military organizations. for use of IOT in military environment such as smart bases that incorporate commercial IOT technologies in buildings, facilities, etc., force protection at bases as well as maritime and littoral environments, health and personnel monitoring, monitoring and just in-time equipment maintenance Architectural aspects of military IOT infrastructure, including security, information, and

communication architectures, work flow/business processes, interoperability and Integration of disparate technologies

The study officially kicked off in January last year and will wrap up with a final report in December 2018. ―Everybody in the area of information technology can see that the IoT is growing in the commercial world at phenomenal rates. The question is how we in the military think about that in terms of benefits, threats and the risks and challenges of using this sort of technology,‖ says Peter Lenk, chief of service strategy and innovation, NATO Communications and Information Agency. ― We see a lot of parallels in the commercial world, the civilian world of smart cities, health monitoring, surveillance applications, smart buildings, smart vehicles—the list keeps going.‖ NATO militaries may, for example, adopt smart city technologies for smart bases, he adds. Or within smart cities, NATO forces may tap into existing civilian systems, such as smart traffic control capabilities. ―Everybody who thinks about it for a little while sees a lot of potential, but there are questions that need to be answered before we rush into things,‖ Lenk offers.

The IoT may provide a number of military benefits, including lower costs for technology such as sensors and drones, greater awareness of the combat situation and faster, more effective decision making.

2. APPLICATION OF IOT IN MILITARY SERVICE

1. DEFENSE

While the military has been a driver in connected and machine-to-machine communications such as radio frequency identification, more commonly known as RFID, it has been slow to adopt true IoT applications that knit these communications into interoperable, automated cycles. Communications remain within their given channels, not easily shared or aggregate.

The challenge is that defense leaders wishing to take advantage of the IoT face a complex technological and regulatory landscape that threatens to mire their efforts in endless choices and challenges. This article aims to help leaders navigate complex IoT decisions by pointing out which applications may be better suited for their goals related to cost efficiency and/or war fighter effectiveness. In each case, we will use

Deloitte‘s Information Value Loop as an analytical framework to identify the key investments necessary to realize the IoT‘s potential benefits. Concerns have been raised that the Internet of things is being developed rapidly without appropriate consideration of the profound security challenges involved[and the regulatory changes that might be necessary . Most of the technical security issues are similar to those of conventional servers, workstations and smartphones, but the firewall, security update and anti-malware systems used for those are generally unsuitable for the much smaller, less capable, IoT devices

2. HEALTH MONITORING SYSTEM

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. Other consumer devices to encourage healthy living, such as, connected scales or wearable heart monitors, are also a possibility with the IoT. More and more end-to-end health monitoring IoT platforms are coming up for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements. Medical advancements have taken many forms, such as the Research & Development Corporation (DEKA) prosthetic limbs for disabled amputees. The battery powered arm uses myoelectricity, a device that converts muscle group sensations into motor control. FDA has already approved these arms in 2014.

3. SMART CITY

The Internet of Things (IoT) shall be able to incorporate transparently and seamlessly a large number of different and heterogeneous end systems, while providing open access to selected subsets of data for the development of a plethora of digital services. Building a general architecture for the IoT is

hence a very complex task, mainly because of the extremely large variety of devices, link layer technologies, and services that may be involved in such a system. In this paper, we focus specifically to an urban IoT system that, while still being quite a broad category, is characterized by their specific application domain. Urban IoTs, in fact, are designed to support the Smart City vision, which aims at exploiting the most advanced communication technologies to support added-value services for the administration of the city and for the citizens. This paper hence provides a comprehensive survey of the enabling technologies, protocols, and architecture for an urban IoT. Furthermore, the paper will present and discuss the technical solutions and best-practice guidelines adopted in the Padova Smart City project, a proof-of-concept deployment of an IoT island in the city of Padova, Italy, performed in collaboration with the city municipality. IEEE Internet of Things Journal (Volume: 1, Issue: 1, Feb. 2014) Smart city monitoring and leveraging services in smart city environments for disaster response and other activities. Smart Parking: The smart parking service is based on road sensors and intelligent displays that direct motorists along the best path for parking in the city [16]. The benefits deriving from this service are manifold: faster time to locate a parking slot means fewer CO emission from the car, lesser traffic congestion, and happier citizens. The smart parking service can be directly integrated in the urban IoT infrastructure, because many companies in Europe are providing market products for this application. Furthermore, by using short-range communication technologies

4. INDUSTRY

The growth of the internet of things (IoT) is drastically changing how consumers interact with their cars, homes and appliances, but the aptly named second digital revolution has major implications for industry too. From machine-learning, machine-to-machine communication to artificial intelligence, the industrial internet of things (IIoT) takes IoT technologies and directly applies them to industrial concerns and in the process improves efficiency and productivity. While consumer-focused IoT solutions have dominated headlines in recent years and the relatively long life cycles of industrial equipment has limited growth in this sector so far, major firms and manufacturers are beginning to embrace IIoT on a big scale, attracted by the opportunity to drive down costs and increase competitiveness.

5. TRANSPORATION

The Internet of Things (IoT), enterprises can accelerate productivity, profitability and operations with solutions designed specifically for their processes. With the right IoT solution in place, enterprises can connect all devices across a centralized cloud network, and capture and share their mission-critical data, allowing them to gain real-time visibility of their operations. This actionable insight is what provides organizations the Enterprise Asset Intelligence they need to make improvements. This enhanced business knowledge can be gained through a set of enabling technologies in the areas of asset management, cloud, mobile and big data. End to End Visibility-Transportation and logistics businesses around the globe are focused on maximizing supply chain efficiency in order to sustain profitability and viability. However, to reach this level of performance, they need to make end-to-end improvements. Complete visibility facilitates more effective, timely decisions and reduces delays through quicker detection of issues. Mobile devices, such as radio frequency identification (RFID), barcode scanners and mobile computers, have become a major influence in supply chain visibility and operations.

3. FIGURE:
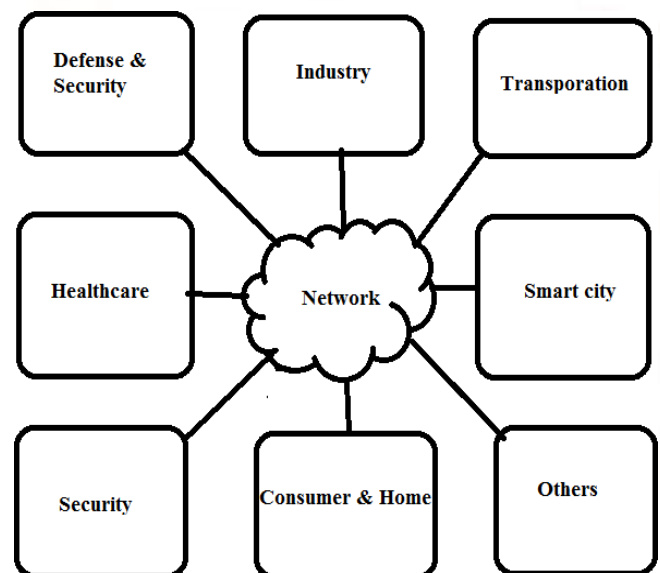
Figure 1-Representation of IOT in military service

CONCLUSION

IOT is very important idea to develop various things in different service. We can use IOT concept to create the new invention in various military service. IOT uses such as Defense, Health monitoring system, Smart city, Security, Industry and Transporation etc.

IOT is the extension of Internet by design; most of the security and privacy issues of the internet would be inherited by the Iot. We analyzed the solutions currently available for the implementation of urban IOTs. This technology is close to being standardized, and industry players are already active in the production of devices that take advantage of these technologies to enable the applications of interest. Thus we conclude that IoT is the most concerned topic in today's world. The most developed and developing countries are moving rapidly in this field. So why do we not use this concept in the defence industry and make a powerful and secure defence industry. Many countries defence organization have taken their steps towards the development but Indian defence is still lagging behind the technology. So we require to do some research showing some interesting innovations in the field and improve the architecture of defence.

4. FUTURE WORK

Internet of Things is an integrated part of future internet and could be defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network. In the IOT ,things are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information _sensed' about the environment, while reacting autonomously to the _real/physical world' events and influencing it by running processes that trigger actions and create services with or without direct human intervention. Interfaces in the form of services facilitate interactions with these _smart things' over the internet, query and change their state and any information associated with them, taking into account security and privacy issues.

REFERENCES

1) Zhu, et al. ―Intelligent transportation system based on Internet of Things.‖ WAC 2012.
2) 6 benefits of IoT for hospitals and healthcare5Posted on July 18, 2016 in health,kevin Patel service assurance technology analyst,xangati
3) Dr Peter Lenk (NATO Communications and Information Agency, The Hague, The Netherlands) and Dr Niranjan Suri (U.S. Army Research Laboratory, Adelphi, MD, USA) in _Defense service'
4) Dr Konrad Wrona (NATO Communications and Information Agency, The Hague, The Netherlands)
5) Andrea Zanella, Nicola Bui, et,al ―Internet of things for smart cities‖ IEEE Internet of things journal vol.1, February 2014. [
6) L. Atzori, A. Iera, and G. Morabito, ―The internet of things: A survey,‖ Computer. Networks., vol. 54, no. 15, pp. 2787–2805, 2010. [5] Hasan Omar Al-Sakran ―Intelligent traffic information system based on integration of Internet of Things and Agent technology‖, IJACSA ,vol 6, 2015.
7) Laisheng Xiao, ―Internet of Things: a New Application for Intelligent Traffic Monitoring System, Journal of Networks, vol 6, 2011.
8) K. Ashton, ―That Internet of Things thing, RFiD Journal, 2009. [
9) Ian G Smith, Ovidiu Vermesan, Peter Friess and Anthony Furness, ―The Internet of Things 2012 New Horizons‖, IERC -Internet of Things European Research Cluster 3rd edition of the Cluster Book, pp:5-8.
10) Sridhar Iyer, IIT Bombay RFID: Technology and Applications, 2005.
11) Fiche d information, Factsheet, ―Introduction to Cloud Computing‖.
12) M. A. Hussain, P. Khan, K. K. Sup, Wsn research activities for military application, in: 11th IEEE International Conference on Advanced Communication Technology, 2009, pp. 271-274.
13) Schneier Bruce (1 feb 2017) ―Security and the Internet of Things‖.
14) Hasan Omar Al-Sakran ―Intelligent traffic information system based on integration of Internet of Things and Agent technology‖, IJACSA ,vol 6, 2015.
15) Laisheng Xiao,―Internet of Things: a New Application for Intelligent Traffic Monitoring System, Journal of Networks, vol 6, 2011.
16) K. Ashton, ―That Internet of Things thing, RFiD Journal, 2009.