Adoption of IoT for Defence – Issues & Concerns

P. Narasimha Rao, FIETE & Prof. K. Laxminarayana, FIETE

***Abstract*—**While Defence has been a driver in well connected and machine-to-machine communications; these communications remain within their given channels, not easily shared or aggregated. The Internet of Things (IoT) is an emerging technology which is fundamentally about connecting several different and dissimilar objects into larger networks. Defence leaders who incline to take advantage of the IoT are worried of facing complex technological challenges including handling high Volume and Diversity of data, faster network speeds, and most importantly, the security concerns. Defence leaders are hesitant, not only to rely on data that are open and discoverable between systems but also to be caught up with frequent Information bottlenecks within their operational and intelligence networks. While considering on the adaptation of IoT by Defence, it is very important, to evaluate which applications of IoT would be better suited for the effectiveness of their mission and at what cost. However for Defence the success of the mission is more important than its operational cost. This paper brings out certain issues and concerns that are critical in adopting IoT for Defence. There is a strong need for development of certain Defence-specific IoT applications suited for the effectiveness and success of commander's mission preferably at a reduced inventory and operational cost.

***Keywords*—**C^2 (Command and Control), C^3I (Command, Control, Communication and Intelligence), combat effectiveness, data fusion, Defence-specific IoT, force multipliers, hard kill, Higher Level Command Control (HLCC) Internet of Things (IoT), near-real-time, operational communications, push-pull model, real-time, soft kill, Service Oriented Architecture (SOA), tactical battle field, tactical IoT.

1. Introduction

Defence commanders have always lived and died for want of adequacy and correctness of information for deriving intelligence not only on their own assets but also on those of the adversaries. Victory went to those groups that could generate and analyse more information in a timely manner and, then use, not only to fine-tune their tactical posture but also to regulate their logistical supply, intelligence groups, and support facilities. Thus in Defence, information flow remained at the heart of all activities from logistics to intelligence. The importance and impact of information in deciding the war strategy makes it classified as a deadly weapon in the Defence context.

With the fact that information flow remained at the heart of all activities from logistics to tactics, the Defence is naturally hungry for technology or tools that improve communication, routing, or processing of information.

The Internet of Things (IoT) is one such technology which is fundamentally about connecting several different and dissimilar objects into larger networks. But this new technology brings both opportunities and obstacles because of its inherent organizational and security challenges.

While the Defence has been a driver in connected and machine-to-machine communications, it has been slow to adapt true IoT applications that knit these communications into interoperable, automated cycles. Communications remain within their given channels, not easily shared or aggregated.

Defence leaders who incline to take advantage of the IoT are worried of facing a complex technological and regulatory frame of mind that pose endless choices and challenges. This paper aims at bringing out certain issues and concerns in support of the unique demands of the commanders for their Defence-specific IoT applications.

In this paper, we run through the command control process and its force multiplication advantages to a tactical commander. The push-pull model of force multiplication is explained in terms of data fusion and operational communication. The working concept of IoT is explained from the view point of adopting it to tactical command control in Defence. The priorities and expectations of the Defence as well as the civilians from the IoT are identified. Technical Challenges including handling high Volume and Diversity of data, faster network speed and larger bandwidth, and most importantly the security concerns in adapting IoT for Defence are discussed. The hesitations and inhibitions of using the public domain IoT for Defence are discussed in detail. The essentiality and expectations from Defence specific IoT are highlighted. This paper shares some information available on the public domain internet on certain upcoming techniques and technologies addressing the issues which promise and pave the way for the adoption of IoT for Defence.

II. Priliminary

A. Command and Control Process

An intelligent command and control system has to provide appropriate tools in decision making. A typical command control process [1] involves sensing the enemy's assets and order of battle, planning out the appropriate action plan and acting against the enemy's order of battle to make it ineffective. The sensors could be Communication Support Measures, Radar Support Measures, imagery and/or thermal in nature. These sensors concentrate in their respective areas of responsibility and provide real-time inputs to derive intelligence to be used in the commander's decision making process. The control centre of the commander then collates the information he already had with what he receives from the

P. NarasimhaRao is a Scientist (Retd) from DRDO and a Freelance consultant in Product R&D.

Prof K. Laxminarayana is a Scientist (Retd) from DRDO, Professor in Engineering College and Former Vice-President of IETE.

higher level control centre for further analysis and coalescing with description of the system mission and its goals. After several assertions and activities, such as estimation of the situation, options generation, choosing the best one, planning and instruction (orders) generation, system is ready to act into the area of responsibility. The action could be a soft kill (jamming) or hard kill (firing) depending on the nature and priority of the threat.

This process is very often distributed, both the functionally as well as geographically. Also, it is often necessary to provide some kind of cooperation with other C^2 (Command and Control) systems, for example to exchange some current situation data or to synchronize the common activities on the field. Therefore, it is necessary to include network components and provide distributed computing support. Such systems are known as C^3I (Command, Control, Communication and Intelligence) systems.

B. Force Multiplication

C^3I systems are designed to Force Multiplication. The basic principle of force multiplication is to find and use factors that increase the effective power that you have (or reduce that of your opponents). Using multiple multipliers has an even greater effect, such that a well-multiplied small force can successfully take on a much larger force.

In any Defence scenario where regiments are spread across multiple fronts, the commander would want to maximize the force particularly when he had a smaller force when compared with enemy. To put it simply, 'force multiplication' in warfare is a strategy of achieving the 'same with less' and consequently 'more with the same' that dramatically increases the power of the forces that one had at his disposal. By way of achieving the required combat effectiveness, with minimal number of resources, force multiplication makes the available resources be untied/spared to perform other tasks.

Push-Pull model of Force multiplication

Force multiplication in a battlefield is all about "pulling" information about friendly and enemy situations and then "pushing" commands and orders down to the tactical units. In the predated wars, where a commander and all his forces easily seen and within shouting distance, this push-pull model [2] was fairly straightforward, but the expansion of modern battlefields has introduced new challenges.

"Pull" data fusion: Informed decision making is predicated on having comprehensive knowledge of the battlefield. A commander needs to focus is on the aggregate battle space before making any effective decision. He needs to collect the information reported by all sensors from a range of locations, taken over a span of time, bring together volumes of diverse data to paint an accurate picture and thereby understanding the situation at the battle space. Today the pull is often accomplished by data fusion, trying to give a commander the widest, most diverse picture of the battlefield.

"Push" operational communications: The push is the challenge of how to disseminate orders to and among tactical units. As with data fusion, the Defence has a long history of working with such operational communication. While the use of Smartphone by civilians started only in the recent past, every soldier has carried a radio since the 1940s.

C. Internet of Things (IoT)

The Internet of Things (IoT) is a computing concept that describes future where everyday physical objects will be connected to the internet and be able to identify themselves to other devices. IoT is a network of physical devices embedded with software, electronics, sensors and connectivity wherein data/information among user, manufacturer, operator or any other connected devices is exchanged to achieve greater value services IoT is expected to offer advanced connectivity of devices, systems and services that goes beyond machine-to-machine communications and covers a variety of protocols, domains and applications.

With its gaining popularity, IoT is not only finding place but also penetrating into consumer applications, enterprise applications, infrastructure applications, in the functional areas like agriculture, manufacturing, energy management, environment monitoring, metropolitan developments, building & home architecture, medical & health care, elder/child care and so on. The future is not very far for the IoT to become an inevitable part and parcel of our day-to-day life and one cannot think of doing anything without IoT.

III. ADOPTION OF PUBLIC DOMAIN IOT IN DEFENCE

Though we could see the wide-range adoption of IoT in the non-Defence (commercial and civilian) application, the adoption in Defence has been limited. The hesitance in use of IoT by Defence can be explained by analysing the differences in the prioritizing of various aspects by these two classes of users.

While some aspects such as handling large and diverse data, protecting secrecy, privacy, authentication, uninterrupted network connectivity, higher bandwidths, quick reaction times are unquestionably unique for Defence, other functions such as asset tracking and facilities management, closely replicate their civilian counterparts. In these areas, leaders can simply bring in the existing civilian technologies to gain the advantages of new IoT applications. Energy efficiency and management [3] is one such application of IoT that has already proven in the civilian world and can provide immense potential for value capture for the military.

Before considering on the adoption of IoT by Defence, it is very important evaluate which applications of IoT may be better suited for the effectiveness of their mission and at what cost. For Defence, the success of the mission is more important than its operational cost.

Civilian IoT successes in cost reductions through utilities and facilities management also can provide a useful roadmap [3] for the Defence in an area with immense potential for value capture. Though the knitting of the IoT fabric seems to be mostly in the lines of command control, its texture and strength is however not found adequate to meet the stringent operational requirements of tactical Defence. The unique demands of the commanders would therefore be certain Defence-specific IoT applications suited for the effectiveness of their mission success preferably at a reduced inventory and minimal operational cost.

D. Implementation of IoT by Defence

The Defence has already implemented many of the foundational components of IoT in both pull and push; however, data often remain disconnected—separate value loops with separate flows of information. The dream of true IoT capability in operational communications is not new and Defence has already been trying to integrate frontline forces, sensors, weapons systems, and communications. Until recently, there was a holdup at the communicate stage and the technology simply did not exist to make these systems work as desired. They could not connect to other systems nor did the communications systems have enough power to transmit the volume of information created.

The communication abilities of systems for Defence should be very high. And when it comes to distributed communications, the communication network and appropriate services have to carry different real-time or near-real-time data such as graphics, image, video, voice or any alphanumeric data. The mobility of both, either potential users in the tactical battle field or the commanders at the decision makers at higher levels, the whole system has to be supported as well. In those circumstances, the network security, safety, and efficiency are of crucial importance. Any network failure or bottleneck can produce a lot of problems including a total system failure disabling its decision making and command and control functions, due to the lack (delay) of data or even of their corruption.

With the well registered importance of communication technology to its framework, the Defence culture has however, not adapted (evolved into) true IoT functionality. Defence leaders are hesitant not only to rely on data that are open and discoverable between systems but also to be caught up with frequent Information bottlenecks within their operational and intelligence networks.

B. Technical challenges in adopting IoT for Defence

In this section we throw some light on certain technical concerns and expectations of adapting IoT for Defence. They include:

Huge volume of data

As the connectivity of sensors increases and they start supplying data, the system can become overwhelmed with the huge volume of data in transit. This increase in data may force an upgrade to a system's network infrastructure to increase bandwidth, or, alternatively, the performance of intelligent data filtering and throttling by edge devices. Storing and (quickly) retrieving large volumes of data is not a uniquely Defence task—other areas of government have made substantial progress on this challenge. Thus, the infrastructure for dealing with the data volume of tactical IoT applications is, potentially, already in place.

Diversity of data

Diversity of data, on the other hand, poses unique challenges to cloud implementation in the Defence. Indeed, Defence data-fusion applications incorporate not only videos but still-imagery, signals intelligence, human intelligence, ground sensors, battlefield reports, map data, and a host of other data sources. Aggregating these disparate types of data necessitates a common set of data standards to be consented. Creating a common set of standards calls for the involvement multiple agencies, commands, and Defence services involved in the production, transmission, and consumption of all of these data types. Such an exercise is not yet reported to have been initiated.

Speed & Bandwidth

Where "pull" was limited by the process challenge of breaking down multiple, siloed data standards (i.e., failures in aggregation and the standards that support them), IoT usage in operational communications is constrained by the technical limitations in mobile communications networks' bandwidth and robustness. While a consumer's 4G LTE smartphone will routinely post download speeds in the range of 8 to 9 Mbps, the commercial satellite network used by Defence for mobile network access posts a top speed of less than 0.5 Mbps. These speeds are more than enough if soldiers need only voice communication or to send short text-only messages. Current Defence communications systems cannot provide a soldier in the field with the bandwidth that a true IoT application would require—and certainly not wirelessly. This challenge is similar to what the commercial networking infrastructure is facing with the proliferation of smart, video-enabled phones and tablets. In the commercial world, network bandwidth and quality-of-service challenges are being addressed with the use of high-bandwidth carrier grade network infrastructure.

Security concerns

The biggest concern for adopting the public domain IoT in Defence that justifies its demand for a Defence specific, tactical IoT is the "security". Concerns have been raised that the IoT 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 concerns are similar to those of conventional servers, workstations and smart phones, but security challenges (especially cyber attacks) are unique to IoT. Some challenges would include industrial security controls, hybrid systems, IoT-specific business processes, and end nodes. As a response to increasing concerns over security, we need to secure the Internet of things by promoting knowledge and best practice. Device data can be protected by use of cryptographic standards and encryption.

E. Expectation on tactical IoT

The tactical IoT, need to provide the secure interface enabling the seamless integration of information exchange between the hard-to-reach (and mobile) tactical deployments and the more strategic (fixed or deployed) HLCC (Higher Level Command Control) centres. The platforms and devices used in the tactical battle space operate with low bandwidth and low operating power making communications constrained, information exchange of critical data difficult. Differing levels of security classifications and differing network owners further compound the issue. Thus there would be a need to have some tactical cross domain architecture to protect the boundary between the low and high security classifications. The prime expectations of a battle field commander, on such tactical IoT include:

Connecting Command & Control with the tactical battle space

Establishing this communications link, and enabling the access to and sharing of critical information and tactical intelligence on assets, people and equipment, and thereby enrich the holistic operational picture for Command & Control is an essential pre requisite for any force multiplication exercise.

Dynamic, Real-Time Intelligence

Connecting tactical IoT sensor-based devices and bringing the data into the Command & Control space unifies information management [4] across the architecture/formation. By automating data transmission without human intervention, tactical IoT can provide an accurate, dynamic, real-time information and intelligence that will allow users at every level in the command chain to plot, visualize and share a consistent and accurate operating picture. The enriched situational awareness enables improved decision-making. The enablement of communications also widens the potential for tactical users to share or send information across the battle space or back up the command chain.

The integration of IoT across the Defence enterprise ensures multiple applications draw on the same information sources. Given the nature of the information being exchanged, in the tactical environment, security of the system is of paramount importance. This shall take place within a highly secure environment that enables the different mechanisms to coherently and seamlessly talk to each other, delivering a fusion of near real-time information to the intended end users in the formation.

Hence the integration of IOT for the tactical environment shall:

- Be built with security at its heart to protect the inter connect, assuring the integrity of the information exchanged.
- Provide users with the ability to fully exploit both real time and historic information across the mission to inform military decisions, and increase the effectiveness of force resources.
- Enable the collaboration and trusted sharing of applications and information that enrich the whole picture available to Command and Control operations, truly enabling information to be a real Force Multiplier.

IV. SOME UPCOMING TECHNIQUES & TECHNOLOGIES

The factors for the slowing down the adoption of IoT by Defence are by now well appreciated and the concern stake holders have already started addressing the real concerns. Some of the products of such research are already reaching the battlefield:

The Army has begun testing prototypes of its Integrated Sensor Architecture, which allows for dynamic discovery of sensors. Using this architecture, for example, a soldier walking through an area could quickly locate a sensor hidden in the ground and read off data about whether any enemy vehicles had passed through the area over the past 24 hours.

Without the ubiquitous cellular signal upon which we rely in our daily lives, these Defence IoT networks operate over tactical radios. The qualitative requirements enlisted recently for a tactical radio sounds more like a futuristic smartphone than a traditional single-channel VHF radio. The next generation of high-bandwidth radios that could make these integrated networks a reality are already under development.

Multi-Function Radio must be able to form a 100-node self-healing mesh network and automatically connect within five seconds. With a minimum 5 Mbps data rate, it is about as fast as the 4G LTE smartphone in your pocket, while meeting military durability and encryption requirements.

Next-generation processors [5] include many new hardware features aimed at providing a highly trusted compute platform. For example, Intel® processors include an implementation of the Trusted Platform Module (TPM), designed to secure hardware through cryptography and other security techniques. In addition, technologies such as ARM® TrustZone®, Free scale Trust Architecture, and Intel Trusted Execution enable the integration of both software and hardware security features to create a platform that endures over the lifetime of the deployment with a wide range of software builds.

Fujitsu [4] has developed an innovative Architecture that enables the seamless integration of hard-to-reach tactical information with existing operational information and intelligence. Fujitsu's solution provides the secure interface between the tactical architecture and more strategic, HQ-based communications. The architecture exploits the open lean services architecture developed by 2iC and published by MOD, to provide a Service Oriented Architecture (SOA) within the tactical environment.

V. SUMMARY AND CONCLUSION

Though the knitting of the IoT fabric seems to be mostly in the lines of command control, its texture and strength is however not found adequate to meet the stringent operational requirements of tactical Defence. While the Defence can, to a certain extent, enjoy the advantage of the state-of-the-art civilian mobile telecommunication such as 4G LTE, those advances will likely need to be paired with advanced, Defence-specific communications architectures. After all, the average consumer does not need a network of rugged, encrypted, frequency-hopping, multiband radios. But for the Defence, the communication abilities of systems have to be very high. And when it comes to distributed communications, the communication network and appropriate services have to carry different real-time or near-real-time data such as graphics, image, video, voice or any alphanumeric data. The network security, safety, and efficiency are of crucial importance. Any network failure or bottleneck can produce a lot of problems including a total system failure disabling its decision making and command and control functions, due to the lack (delay) of data or any corruption in such data. The need of the commanders would therefore be certain Defence-specific IoT applications suited for the effectiveness of their mission success preferably at a reduced inventory and operational cost.

For Defence, the success of the mission is more important than its operational cost. Thus, while considering on the adaptation of IoT by Defence. It is very important evaluate which applications of IoT would be better suited for the effectiveness of their mission and at what cost.

The factors for the slowing down the adoption of IoT by Defence are by now well appreciated and the concern stake holders have already started addressing the real concerns. Some of the products of such research are already reaching the battlefield. Continued developments in network technology and data standards promise to create a tactical IoT that can unify the push and the pull, remaking battle space awareness into a truly modern process.

ACKNOWLEDGMENT

The authors express their gratitude to their parent organisation ie., DRDO, for providing the platform and opportunity to interact, work with and learn from professionals from academia, industry, user groups, on modern warfare system. The knowledge and experience gained from their association is the source of inspiration to write this paper. The authors also thank all the content providers given in the references for sharing their works over the net for public access.

REFERENCES

[1] Slobodanka Djordjevic-Kajan, Ejub Kajan, Dejan Mitrovic, "Towards Active C3I Systems", TELSIKS '97, 8-10 , October 1997

[2] Michael E. Raynor and Mark J. Cotteleer, "The more things change: Value creation, value capture, and the Internet of Things," Deloitte Review 17, July 27, 2015

[3] Joe Mariani, Brain Williams, Brett Loubert, "Continuing the march The past, present, and future of the IoT in the military", Deloitte University Press, 2015.

[4] "Fujitsu Tactical IoT, Connecting Command and Control with the Battlespace", Fujitsu, 2017.

[5] "The Internet of Things for Defense", Wind River, 2015

Mr P. Narasimha Rao, born in September 1955, has obtained his M.Sc (Tech) degree in Applied Physics with specialization in Electronics in the year 1977 from Andhra University, Vishakhapatnam. India.

He started his career as a Research Associate in the Dept of Meteorology & Oceanography of Andhra University. He joined DRDO in the year 1979 and contributed in various capacities to the design and development of electronic subsystems and systems for major Defence Projects/Programs. During his 36 years of working with DRDO for more than 36 years, he had a stake in several Major and Prestigious Programs of DRDO. He is retired from DRDO and is now a Free Lance Consultant on Product Innovation through indigenous R&D.

Mr. Rao is a Fellow and a Chartered Engineer of IETE. He is one among the few internationally certified Senior Project Management Professionals in India. He is also a Certified Reliability Professional. He is a life member of other professional bodies like the Indian Science Congress Association, Society for EMC Engineers (India) and Instrumentation Society of India. He has authored two book entitled "Product Research and Innovation made Easy – a PRIME to Make in India" and "The Realism of Life.

Prof. K. Laxminarayana, Born in July 1942, has obtained BE degree in ECE in the year 1965 from Osmania University, Hyderabad and ME degree in ECE in the year 1974 from Indian Institute of Science, Bangalore, India.

He joined DRDO in the year 1965 and contributed in various capacities to the design and development of electronic subsystems and systems for major Defence Projects/Programs. During his working with DRDO for 37 years, he had made significant contribution towards the development of indigenous technology for secure communications and EW systems. After retirement from DRDO, he joined as Professor in an Engineering College affiliated to JNTU, Hyderabad in 2003. As a volunteer of an NGO, he is mentoring youth to become successful entrepreneurs.

Prof Laxminarayana is a Fellow, Chartered Engineer and Ex Vice President of IETE. He is Life Fellow of Institute is Engineers (India) and Broadcast Engineering Society. He is member of Indian Science Congress Association, Indian Society for Technical Education, Society for EMC Engineers (India) and IEEE.