Defence Research and Development Canada | Recherche et développement pour la défense Canada

CAN UNCLASSIFIED

Could early adoption of internetworking of intelligent things provide significant advantages?

Paul Labbé

22nd International Command and Control Research and Technology Symposium (22nd ICCRTS), Topic 3: Implications of the Internet of Intelligent Things
Army Research Laboratory - West and USC Institute for Creative Technologies 12015 Waterfront Drive, Playa Vista, CA 90094-2536

Date of Publication from Ext Publisher: November 2017

Defence Research and Development Canada

External Literature (P)
DRDC-RDDC-2017-P100
December 2017

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the *Defence Production Act*.

Template in use: (2012) CR EL1 Advanced Template_EN 2017-11_02-V01_WW.dotm

Abstract

This paper reviews technology advances from different perspectives that could provide safe and cost effective achievable internetworking of intelligent things ecosystems with significant advantages to early adopters. Based on recent science and technology outlook, it appears that we might be at the cusp of practical specialized artificial intelligence in small devices. Similarly the transceiving capabilities of fifth generation cellular phones open access to advanced communication systems with capabilities not available before at low cost and with low energy demand. Future intelligent things will be more aware where they are and will be able to sense their environments either local radio spectrum time history, temperature, humidity and capture surrounding sounds. In addition smaller devices with high memory density and computing capabilities with low power demand make achievable advance security and encryption possible as well as local analytics which will provide more useful and actionable information to be shared. Moving some data analytics closer to all-domain sensors increases the ecosystem energy efficiency, reduces the burden on end users and central data centers. As much as possible, this paper will estimate the potential gain in terms of military mission success rate from the hypothetical adoption of such technologies that minimize operational cost and information management burden with extremely large numbers of data sources.

Keywords: Internet of things (IoT), industrial internet of things (IIoT), internet of intelligent things (IoIT), internet of battlespace things (IoBT), internet of military things (IoMT), internet protocol version 6 (IPv6), contested urban environment (CUE), fifth generation of cellular technologies (5G), jamming, low probability of intercept (LPI), low probability of detection (LPD), artificial intelligence (AI), analytics, track data, emerging technology, efficiency, C4ISR.

1. Introduction

The first objective of this paper is to provide sufficient evidences for a reader to consider that the future of real-time information systems such as for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems will heavily rely on a large number of generic and specialized intelligent things internetworked providing enhanced agility [1] in complex scenarios. This is much beyond what is available today on the smart phones and related services such as linking a visit to a place either a national park or a restaurant and collect geotagged users' comments and photos in order to inform future users. Such capabilities were predicted by the author fifteen years ago [2]. The second objective is to highlight selected technologies and scientific advances that contribute to the roadmap of future C4ISR ecosystems based on internet of intelligent things (IoIT). It is envisaged that such ecosystems would be more manageable, secure and resistant to cyber-attacks, thus capable of supporting deployed forces in operational hostile theaters [3]. The third objective is to estimate the potential gain of early adoption of IoIT C4ISR ecosystems on specific decision making outcomes based on previous studies.

2. Background

The explosion of internet of things (IoT) today is the result of a long progression starting in 1969 with the Advanced Research Projects Agency Network (ARPANET) which was an early packet switching network and the first network to implement the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. Both technologies became the technical foundation of the Internet. The current concept of IoT expands the word internet to all TCP/IP and non-TCP/IP networks. A first non-computer thing connected to Internet, thus considered as the first IoT, was a toaster for demonstration purpose at a conference in October 1989[1]. Under this concept a thing becomes 'smart' when it is identified by a unique IP address and connected to a network. So most smart objects today are not heavily evolved, e.g., smart appliances and TV. Most of them don't have sufficient software, memory and hardware to offer secure communications with encryption. Now one finds that by 2020 there will be billions of devices or things with various degrees of smartness deployed and connected to an internet, e.g., smart vehicles, buildings and cities. Most of the IoTs are wirelessly connected together or via various networks. Some will have advance security and 'geoencryption' or 'location-based encryption' as discussed in [4].

2.1 IoT terminology

IoT IEEE Committee definition: "Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration" [5].

The same committee [5] expressed the following observations from some of its findings: "…it would appear that IoT will be characterized as a set of interworking networks of things that can be made smart if they can be identified, named and addressed (smart objects). 'Things' can be physical objects or their descriptions or data related to them or even relationships between objects. For a majority of definitions a thing will be a node of a network. IoT systems show scaling capabilities, from small systems based on a few sensors up to large and complex systems. Under this perspective the differentiation between nodes is emerging: sensor, actuator, gateway, virtual object. All of them assume ubiquitous connectivity, while each entity performs different functions. Another emerging aspect is the possibility of using functions offered at things' interfaces."

In public security and military scenarios the ubiquitous connectivity cannot be always achievable. This is a significant issue that needs to be addressed for such applications. A better scenario is one where we deploy in a city with a crippled Internet connectivity and degraded cellular phone service access (can be in a contested urban environment, CUE [6, 7]).

[1] https://www.postscapes.com/internet-of-things-history/ (Access date: 18 April 2017). You had to insert the bread.

The evolution of IoT technologies and applications drove specific specialisation and generalisation. For example internet of everything (IoE)[2] is considered a superset of IoT and machine-to-machine (M2M) communication without human interventions is considered a subset of IoT.

Several authors reported on internet of military things (IoMT) [8-11] and internet of battle things (IoBT) [12-20]. Other authors documented tools and prototypes to explore novel ways for human-computer interaction (HCI) with IoT [21]. Some IoT technologies offer better cyber, hacking and security protections due to economic and secrecy of their business, industrial internet of things (IIoT) [22-27]. In fact [3] extended IIoT technologies to public safety and defence including biometrics [28].

Another IoT terminology, the internet of intelligent things (IoIT) [29-31], considers more capable and autonomous things, adding artificial intelligence (AI) and some capabilities of acting without human interventions, although this was more or less included in the spiral of IoT evolution or specialization of the IoT IEEE definition. Adding AI to intelligent communication networks contributes to their adoption in fields like healthcare, military or prediction of seismic activity in volcanoes [31]. IoIT have more computing capabilities for encryption, self-healing and cyber protection. Distributed intelligence adds benefits such as no single point of failure, provides local users with more real-time information and reduces load and traffic to centralized computing. The centralized system helps providing global contexts to local computing which contribute to the coherence of local awareness pictures to a common operating picture (COP) without reducing significantly the timeliness[3] of the local picture.

2.1.1 Specialized artificial intelligence

Several success stories about AI capabilities have been reported over the last decade including studies on the implications of specialized AI [32-36]. For example, once deeply trained at recognising indicators of a type of cancer from a representative imaging data set, a specialized AI demonstrated its abilities to assess large number of such cancers from other imaging data sets that included some imaging data without this type of cancer with no false detections. Then the AI system was able to find cases of the same type of cancer that were not detected by specialists/experts. However it appears that deep learning neural networks and other AI approaches were using large computing capabilities.

Currently this is changing [37]. According to an IEEE Spectrum post (14 Feb 2017) by Katherine Bourzac, engineers are developing specialized hardware for energy-efficient AI. These will be timely addition to the world of IoITs. “Thanks to an artificial intelligence technique called deep learning, computers can now beat humans at the Go game, identify melanomas as accurately as dermatologists do, and help autonomous vehicles navigate the world. Now, circuit designers are working on hardware they hope will lead to the democratization of deep learning, bringing the powerful method to the chips inside smart phones, wearables, and other consumer electronics. To that end, last week at the IEEE International Solid-State Circuits Conference (ISSCC) in San Francisco, academic and industry engineers showed how they have built on work presented at last year’s conference to produce specialized, energy efficient deep-learning processors. This dedicated

[2] https://www.iottechexpo.com/2016/01/m2m/ioe-vs-iot-vs-m2m-whats-the-difference-and-does-it-matter/ (Access date: 20 April 2017).

[3] “It is imperative that data managers understand the time value of data being displayed, take action to ensure timeliness of track information…” http://www.jcs.mil/Portals/36/Documents/Library/Instructions/3115_01.pdf?ver=2016-02-05-175019-390 (Access date: 17 August 2017).

hardware will give electronic devices a new level of smarts because, unlike traditional software, it relies on high-level abstraction like the human brain. What's more, it won't drain the gadgets' batteries. "We're beginning to see that there is a need to develop more specialized hardware to get both performance and energy efficiency," says Mahesh Mehendale, TI Fellow at Texas Instruments in Bangalore. He co-chaired the conference session with Takashi Hashimoto, chief engineer in the technology development laboratory at Panasonic."

"Compared to other algorithms, neural networks require frequent fetching of data; shortening the distance this data has to travel saves energy. Guiseppi Desoli, a researcher at STM's Cornaredo, Italy, outpost, presented a neural network processor that can perform 2.9 trillion operations per second (teraflops) per watt." Not sufficient yet since this means only an hour on a smart phone battery: "only a few teraflops per watt".

2.2 Timeline adapted from IoT history[4]

From initial technologies using electromagnetic signals (1832: An electromagnetic telegraph was created by Baron Schilling in Russia, and in 1833 Carl Friedrich Gauss and Wilhelm Weber invented their own code to communicate over a distance of 1200 m within Göttingen, Germany.) to the first thing (not a computer) connected to a network (1990 by John Romkey), visionaries have predicted the evolution of today IoT (1964: In Understanding Media Marshall McLuhan stated: "....by means of electric media, we set up a dynamic by which all previous technologies, including cities, will be translated into information systems").

The first digital communications were for defence systems (In the late 1950s, early networks of computers included the military radar system Semi-Automatic Ground Environment (SAGE)[5].): In September 1950, a "microwave early-warning radar system at Hanscom Field was connected to Whirlwind using a custom interface developed by Forrester's team. An aircraft was flown past the site, and the system digitized the radar information and successfully sent it to Whirlwind[6]."

The birth of Internet[7] is linked to the ARPANET born in 1969. The conceptual ARPANET evolved the Transmission Control Protocol (TCP) and the Internet Protocol (IP), TCP/IP, with unique identification of its components as IP label (aka, address). Then in 1984 the Domain Name System (DNS) was created due to the small number of IPs available under IP version 4 (IPv4). During that period the key components of the Defence Research Establishment Network, DRENET[8] Canada REF ARPANET connected via University of Rochester were completed under the scientific authority of Paul Labbé while seconded to the Communications Research Center (CRC) Ottawa. In 2011, IPv6[9] was publicly launched - The new protocol allows for 2^{128} (approximately 340 undecillion) addresses or as Steven Leibson puts it, "we could assign an IPv6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths." It evolved from the IPv4 with the intent to correct its various weaknesses such as poor quality of service (QoS) management and security, so IPv6 was born with improved capabilities such as QoS information sharing and management, multicasting, authentication, security, privacy and encryption in mind. It provides more means to combat cyberattacks and network exploitation. It contributes to

[4] https://www.postscapes.com/internet-of-things-history/ (Access date: 18 April 2017).
[5] https://en.wikipedia.org/wiki/Computer_network (Access date: 18 April 2017).
[6] https://en.wikipedia.org/wiki/Semi-Automatic_Ground_Environment (Access date: 18 April 2017).
[7] https://www.postscapes.com/internet-of-things-history/ (Access date: 18 April 2017).
[8] https://tools.ietf.org/html/rfc1020 (Access date: 18 April 2017).
[9] The author participated to an early meeting on IPv6.

detect, monitor, protect, analyze and defend against network infiltrations preventing service/network denial, degradation and disruptions [38-40].

Table 1**:** IPv6 adoption, Access date: 18 Apr 2017 (First 22 Countries sorted by IPv6 use ratio) [10].

Index	ISO-3166 Code	Internet Users	V6 Use ratio	V6 Users (Est)	Population	Country
1	BE	10109309	55.32	5592492	11422949	Belgium
2	DE	70971603	42.05	29844102	80649549	Germany
3	CH	7353067	34.66	2548818	8432417	Switzerland
4	US	288324176	33.53	96674350	325790030	United States of America
5	GR	7063611	33.37	2357278	10900635	Greece
6	LU	553892	31.73	175765	581820	Luxembourg
7	PT	6915955	26.74	1849045	10276308	Portugal
8	GB	60555720	24.84	15040627	65394947	United Kingdom of Great Britain and Northern Ireland
9	IN	465606607	24.72	115074864	1337950022	India
10	JP	114900869	21.67	24902102	126126092	Japan
11	FR	56039156	18.70	10478733	64860135	France
12	CA	32326774	18.33	5924606	36527429	Canada
13	EC	7135628	18.32	1307589	16555983	Ecuador
14	PE	13141549	18.32	2407295	32052560	Peru
15	IE	3838543	18.14	696496	4738942	Ireland
16	EE	1194349	17.11	204335	1306728	Estonia
17	MY	21296431	15.52	3305986	31044361	Malaysia
18	NO	5207437	14.78	769895	5313712	Norway
19	FI	5121012	14.52	743597	5536230	Finland
20	AU	20887921	14.30	2987394	24545149	Australia
21	TT	945247	13.81	130549	1367942	Trinidad and Tobago
22	BR	139942445	13.74	19231305	210756695	Brazil

All of this information is critical to show that public safety and defence IoT augmented information systems could benefit of the inherent potential from pervasive IoT capabilities while preventing denial from such advantages due to malevolent actions to inject false information or denial of services. A good example for IoT protocols is 6LoWPAN[11], "a somewhat contorted acronym that combines the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). 6LoWPAN, therefore, allows for the smallest devices with limited processing ability to transmit information wirelessly using a secure Internet protocol."

The very fixes that have kept IPv4 going have introduced a proliferation of problems that are now having a big impact on the functionality or the operation of the Internet. We are moving to IPv6[12]: "IPv4 has required an increasingly complex set of fixes and bodges to keep it functioning. These problems are not theoretical. They are having a real impact on businesses today. They impact many

[10] https://labs.apnic.net/dists/v6dcc.html (Access date: 18 April 2017).
[11] https://www.link-labs.com/blog/6lowpan-vs-zigbee (Access date: 18 April 2017).
[12] http://www.digit.fyi/ipv6/ (Access date: 18 April 2017).

areas of Internet operations including growth, performance, manageability, security, flexibility and reliability." IPv4 cannot efficiently and securely manage billions of IoTs but IPv6 can.

The transition is not easy. Table 1 shows 22 countries ranked in term of their use ratio of IPv6. Currently organizations have to run in parallel the IPv4 and IPv6 stacks. "The Internet Protocol Version 6 (IPv6) transition is well underway, and as the Internet *in toto* undertakes this massive sea change, it opens a wide scope for potential attack vectors for covert information-stealing, according to NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) research."[13]

2.3 Scenario example excerpted from a DoD policy publication [41]

2.3.1 Case Study: Battlefield Situational Awareness

IoT Uses and Potential Benefits

"The very small size and low cost of sensing and communications devices makes them ideal for deploying in low power networks in forward situations to provide warfighters with enhanced situational awareness, giving them real power to see around corners and across hostile terrain. Connected into communications capabilities built into their uniforms and armor, these capabilities greatly augment their ability to execute their missions and effectively engage and dominate the enemy in difficult environments. With the addition of improved internetworking capabilities, real time situational information can be relayed to command and support facilities remote from the battlefield, allowing advice and additional big picture information to be sent back to the warfighters, again increasing their effectiveness."

Threats and Vulnerabilities

"Imagine that the enemy takes advantage of vulnerabilities in the devices or networking, hacking into or compromising these devices and the information they supply. This may allow the enemy to provide false information to the warfighter and the supporting remote organizations; making decisions and actions, and actions they take either unreliably or dangerously. At the same time, they can also see the information that should have gone to the warfighter, giving them the advantage of the situational awareness and further allowing them to take advantage of the confusion they have created through the injection of false information into the warfighter decision making process."

> Author's comment - Suggested countermeasures: At time of design and manufacturing, select components or chip sets that are certified with the required hardening and redundancy in order to make hacking unsuccessful or detectable. The same for the networks and IoITs with resilient protocols, operating systems and application software for analytics and other functions.

Recommendation

"Prioritize addressing the highest risk vulnerabilities already installed in mission systems, such as ensuring that the information is encrypted where needed. Implement policies and processes (and communicate these changes broadly) to ensure supply chain risk management of a broader array of potential devices that could be deployed with our troops."

[13] https://www.infosecurity-magazine.com/news/nato-ipv6-transition-opens-up/ (Access date: 18 April 2017).

Author's comment - Tactical data links suffered from the lack of full implementation of protocol and system suites across allied nation users.

3. Wireless technologies

Wireless technologies debut started much before the Internet. It was initially used from about 1890 for the first radio transmitting and receiving technology, as in wireless telegraphy, until the new word radio replaced it around 1920. Current advanced wireless technologies are exemplified by the new generations of smart phones which include a variety of sensors such as microelectromechanical systems (MEMS) inertial measurement unit (IMU) that can complement satellite based navigation when denied, e.g., Global Navigation Satellite System (GLONASS) and Global Positioning Satellite (GPS). These smart phones also include substantial memory storage and computing power in addition to manage a variety of network protocols, frequency bands and waveforms. Up to a certain point they can emulate what was developed for military communications two decades ago (around 1997). Under the hood of the radios of some advanced IoT hardware platforms one finds technologies developed for defence such as software define radios (SDRs) which evolved under the US Department of Defense (DoD) Joint Tactical Radio System (JTRS) program[14]. Silicon industry, e.g., National Instruments (NI)[15] (Figure 1), looks beyond today best SDR solutions which evolved from field programmable gate-array (FPGA), radio frequency integrated circuit (RFIC) and digital signal processing (DSP) devices in support of military communications (MILCOM), electronic warfare, signals intelligence (SIGINT) and Fourth Generation (4G) smart phones. Future technologies integrating analog with digital circuits will support IoT and Fifth Generation (5G) smart phones, and other systems yet to be defined.

This is interesting since SDR like technologies allow monitoring/sensing, in almost real time, the radio frequency (RF) spectrum in order to better use what is currently available at specific locations. This is related to the Innovation, Science and Economic Development Canada (ISED)[16] Grand Challenge programs to maximize the benefits that Canadians derive from the use of RF spectrum. These include Communications Research Centre (CRC) Grand Challenge programs such as the Spectrum Environment Awareness (SEA) and the Making Better Use of Spectrum (MBUS). It's all about RF spectrum management for ISED. Here specialized IoIT could contribute in generating at low cost a geographical map of frequency availability at a given time and location. Also in military operations such capabilities could enhance our forces visualisation of opposing forces and civilian RF activities as function of time and geolocation. Such dynamic picture of RF activities could contribute to deduce or anticipate opposing force course of actions and intents.

[14] JTRS was a family of software-defined radios that were to work with many existing military and civilian radios. It included integrated encryption and Wideband Networking Software to create mobile ad hoc networks (MANETs).
[15] http://www.ni.com/white-paper/53706/en/ (Access date: 11 April 2017).
[16] Formerly Industry Canada (IC).

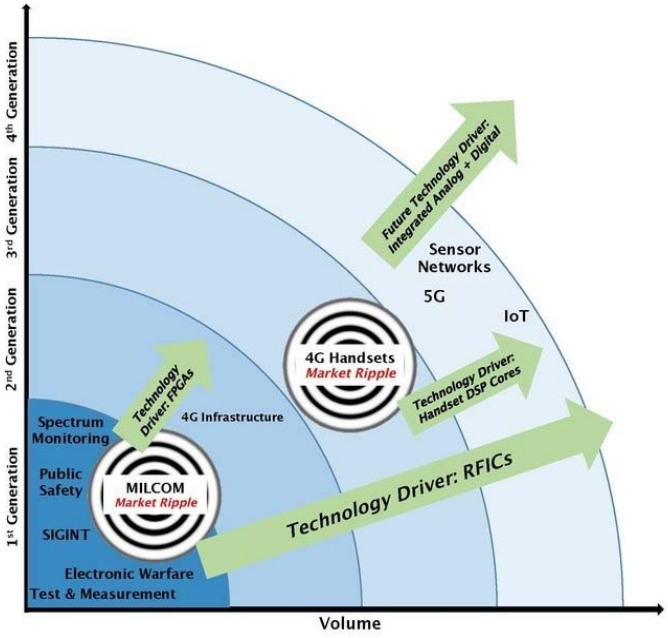

Figure 1: Successive generations of SDRs have come to dominate the radio industry and will continue to evolve[17]

3.1 Wireless security

In order to tackle the broad subject of security or cybersecurity [2, 3, 8, 10, 18, 42-62] for wireless communications we have to consider the three dimensions of wireless communication security, i.e., information security (INFOSEC) as that defending against unauthorized access to or modification of information; communications security (COMSEC) as that keeping important communications secure; and transmission security (TRANSEC) making it difficult for someone to intercept or interfere with radio communications without prior knowledge of accurate waveforms, modulation schemes, and coding [49]. The basic strategy against a radio communication is to detect, intercept, exploit, and jam the communication signals. To counter these, one tries to achieve a low probability of detection (LPD), low probability of interception (LPI), low probability of exploitation (LPE) and better anti-jamming. One of the challenges is if someone increases the transmitter power to combat jamming then the LPD will suffer. So other approaches have to be sought, e.g., using more coding gain and spread the signal[18] in order to both combat jamming and obtain a lower LPD [63]. With a lower LPD comes usually lower LPI and LPE.

Moreover, in a defence and security scenario the offending organizations trying to jam transmission, expects allied organizations to identify the position of the jammer and eventually request to stop the malevolent jamming or be destroyed. So a good jamming strategy is to use a jamming signal with just enough power and for a specific short elapse of time in order to decrease the probability to be localised.

[17] http://www.ni.com/white-paper/53706/en/ (Access date: 11 April 2017). NI copyright permission duly signed on 24 April 2017 for Paul labbé to use this illustration.

[18] "interference suppression for direct sequence spread-spectrum code-division multiple-access (CDMA) systems using the minimum mean squared error (MMSE) performance criterion."
http://www.ece.utah.edu/~ece6961/project/madhow_MMSE_94.pdf (Access date: 25 April 2017).

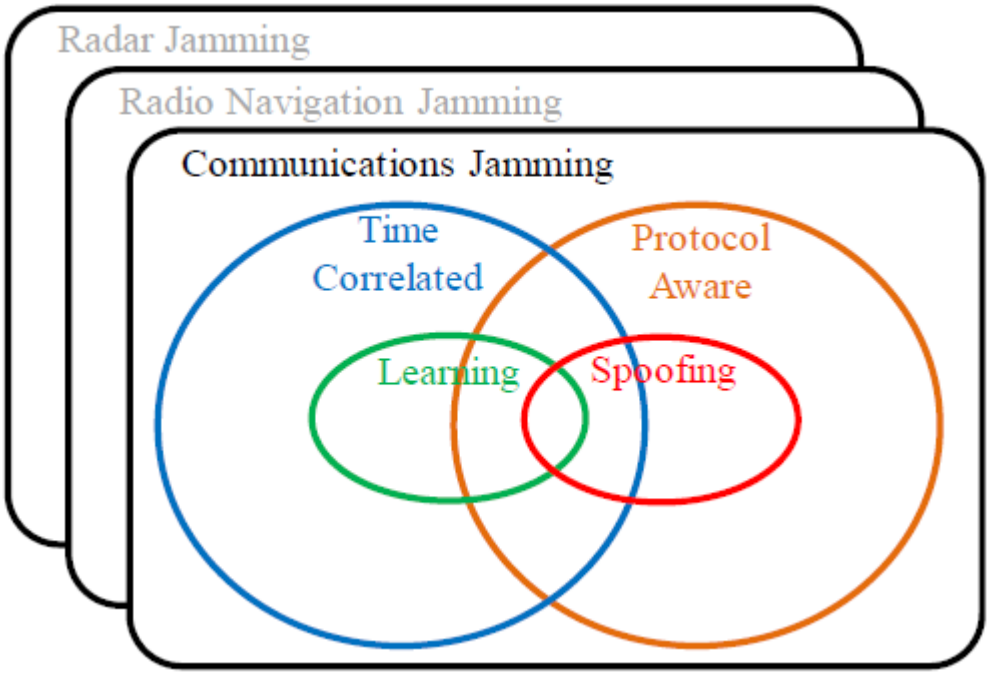

Figure 2**:** Key capabilities of a jammer and how they relate (Illustration from [50])[19].

Typical jammer capabilities from Figure 2 allow devising an even better jammer strategy by deducing the type of protocol and error correction capabilities of the communication to disturb, this is protocol jamming. Reading reference [50], we find that the authors' intent of the jamming taxonomy paper is "to help researchers place newly discovered jamming or anti-jamming strategies within a larger context of known strategies in a way that is consistent with modern electronic warfare." The authors refer to the Common Attack Pattern Enumeration and Classification (CAPEC)[20] which "is a catalog and taxonomy of cyber-attack patterns, created to assist in the building of secure software. Each attack pattern provides a challenge that the attacker must overcome, common methods used to overcome that challenge, and recommended methods for mitigating the attack." For example, performance improvements in terms of energy efficiency, data streaming speed and accuracy require using system and network self-awareness at various layer levels of the IoT stack [64-70] in order to counter interference or jamming, These networks may share QoS information about the receiving spectrum as seen by the wideband front end of their SDR from each participant location.

A communications jammer, Figure 3, can have one or more of the following major capabilities: time correlated, protocol-aware, ability to learn and signal spoofing.

When a jammer has no knowledge of the protocol to be defeated, it may use digital radio frequency memory (DRFM) jamming (a.k.a. repeater jamming or follower jamming) in the simplest form of correlated jamming. Also it can estimate the automatic gain control (AGC) time constant of the receiver to be jammed.

[19] With the permission from the authors; Labbé-Lichtman, 3 April 2017.
[20] https://capec.mitre.org (Access date: 22 April 2017).

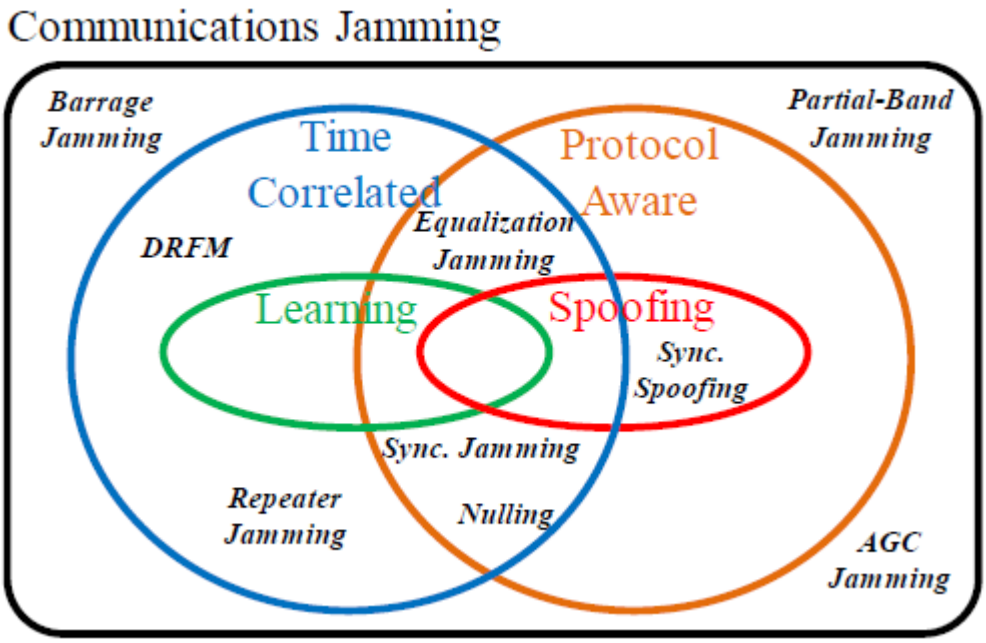

Figure 3: Specific jamming techniques discussed in literature, mapped according to key jammer capabilities (Illustration from [50])[21].

More information about radio communication jamming and network security could be found in [50, 57]. In addition we have to consider the significant research and findings on self-healing networks and sensor networks [15, 56, 57, 61, 71-78] which offer an adaptive approach to counter jamming, adverse propagation, interferences and noise.

Next we have to consider the INFOSEC and COMSET aspects assuming that attacks are within the internetworking. In such cases encryption, randomization and utilisation of blockchain should be sufficient to protect the information. Also this creates a big challenge in managing crypto keys over a large number of IoITs via wireless links [54, 79, 80]. Other studies show techniques to increase the physical layer security (PHYLAWS) [27, 81-83].

IoIT, being a more capable IoT, offers a variety of means to support cybersecurity. For example, adopting IPv6 (or equivalent for non TCP/IP network) is a first step as explained in [84]. In addition IoIT can run continuously a personal security agent (PSA). From the point of view of recent ransomware attacks the IoIT application layer should be carefully designed and implemented with appropriate password updating. In addition a bill[22] was introduced to address several of the issues with IoT cybersecurity, 'Internet of Things Cybersecurity Improvement Act of 2017': To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes. It is expected to cover issues such as distributed denial of services (DDoS) attacks, secure password management, eavesdropping, encryption, device tampering, spoofing, data integrity, security, authentication, etc. IoT cybersecurity was covered by seral authors [3, 45, 54] and organisations identified in Section 4.1.

[21] With the permission from the authors; Labbé-Lichtman, 3 April 2017.

[22] https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017 (Access date: 17 August 2017).

4. Experimental observations

Observations from an intelligence, surveillance, and reconnaissance (ISR) exercise in 2004: During Atlantic Littoral ISR Exercise (ALIX)[23] it was noted that the high volume of data transfer required for transmitting the video from uninhabited aerial vehicles (UAVs) or remote-controlled aircraft, that the surveillance imagery exceeded the satellite channel capacity in northern latitudes causing substantial delays to the otherwise real-time data and loss of critical data. It appears that more data processing by the sensor or the UAV would have reduced the required high data rate transfer to a central node and increased the timeliness of critical data or actionable information to concerned end users.

For ALIX the surveillance video was sent to a central data processing center and analysed by various experts. Then data were selectively sent to appropriate offices of principal interest, e.g., information about the littoral to Environment Canada.

More detailed analyses of unclassified data about coalition preparedness exercises were published by the author and will be used to provide an order of magnitude of potential improvements that could be achieved when improving timeliness of critical information for over-the-horizon targeting. The documentations about these exercises could be accessed on the Web[24] [85].

4.1 Relation between analytics and track data

There is a variety of analytics that have been developed and tested so far but some that have been used more specifically in digital military information systems are related to track data. In order to understand the following discussion on military track data, here is an excerpt from a reference document on the subject of tactical data links (TADILs) [86]. Impact of the positional accuracy, dead reckoning and timeliness of track data on mission success rate have been reported based on the analyses of various military exercises [87-89].

"Track Identification: Track identification is reported on TADIL J as an environment, identification, platform, platform activity, specific type, or nationality… Surveillance: Messages that support the surveillance function fall into three general areas: track and track amplifying information, track management information, and positional references, which include points, strobes, and fixes. Tactical data systems (TDSs) that support surveillance normally use active sensors, such as radar or IFF[25], or receive position information and status directly from TADIL C or TADIL J participants. These TDSs generate near real-time track reports that are exchanged with JTIDS[26] on the surveillance NPG"[27]. In addition to radar tracks, other types of sensors, for example, signal intelligence, infrared, and electro-optical, can also generate real-time track reports to be shared on the surveillance NPG.[28]

---

[23] http://mdacorporation.com/docs/default-source/brochures/isg/surveillance-and-intelligence/c4isr/airborne-surveillance-and-intelligence-systems/historyuavs.pdf?sfvrsn=4 (Access date: 13 June 2017).
[24] http://dodccrp.org/events/5th_ICCRTS/papers/Track6/064.pdf (Access date: 13 June 2017).
[25] Identification, friend or foe (IFF).
[26] Joint tactical information distribution system (JTIDS) unit (JU) assignments – JU address, participant type and sequence number, transmission mode, track numbers, terminal output, user type, initial entry identification, secondary JU address, track number block.
[27] Network Participation Groups (NPGs).
[28] www.adtdl.army.mil in Tadil J (Access date: 24 April 2017).

So a track could be related to statistical time series when trying to follow the movement of entities in a battlefield. From some previous experiments, when analytics (man operated or autonomous) are far remote from the sensors, the resulting data suffer from some time lateness, sometimes with delays that make track data almost useless. When the analytics and pre-processing are done close to the sensors and the result instantly forwarded to tactical operators (or autonomous actuators) we observed more timely and useful data for real time decisions and actions. The improvement of the success rate of interception in reference studies [85] were in excess of 50% when the average delay was reduced by about 40%. But these percentages don't translate well from one scenario to another one but this trend is certainly valid for large varieties of scenarios. For CUE when tracked opposing entities are lurking behind the next corner obviously there is a need for data updates with small delays like one second and precision location like a meter. In a building or a tunnel this becomes even more challenging if the area was not surveyed *a priori*.

In the reviewed material on IoT systems, the trend is to move data processing of raw sensor data to the IoT (the sensor) when possible in order to improve the (timeliness and positional accuracy for moving target) value of actionable information at the tactical level. Trade-offs need to be made when sensors are powered by batteries, i.e., one needs to estimate the amount of energy required to transmit a lot of raw data at high rate versus the energy required for processing the raw data and sending a clean track data point or series thereof. This also points to the fact that if we want secure communications in addition, we need IoT with more computing capabilities and buffer memory space, and consequently more energy capacity for a given period without re-supplying. This could be curbed when the IoT could scavenge energy from the environment such as from solar panels, some fuel and energy efficient network protocols [10, 12, 44, 55, 90]. Many other alternatives exist but often for very low power budget[29] as described in IEEE Spectrum [91] (Wireless Sensors That Live Forever: Energy harvesters and radioisotopes fuel tiny transmitters). Such harvesters do not produce enough power for most of our applications.

In [92] the authors used an information value loop comprising elements about value drivers, stages and technologies to develop an understanding of the value to operations, risk and advantages, and overall cost of integrating IoT sensing and actuating in support to military decision making and operations. They found a cost reduction for the infrastructure. Using cost reduction from IIoT they observed that battlespace awareness improvement could be achieved with low security risk from the increased number of things (although this assumes an increase in the surface that could be the object of cyberattacks). "Defense and intelligence leaders have followed suit: The CIA[30] and Defense Information Security Agency (DISA) have leaned on civilian expertise, working with commercial companies to bring the cloud and software to secure government networks.[31] Thus, the infrastructure for dealing with the data volume of tactical IoT applications is, potentially, already in place."

[29] Piezoelectric or microelectromechanical systems (MEMS) cantilever convert mechanical motions into electricity a power budget of between about 0.1 microwatt and 1 milliwatt. The device was able to create sufficient output energy to achieve a 5-mW RF pulse every three minutes. Most important, because the half-life of Ni‑63 is just over 100 years, the device could function autonomously, according to Lal and Tin, for about that long.
[30] Central Intelligence Agency (CIA).
[31] Frank Konkel, "The CIA is bringing Amazon's marketplace to the intelligence community," Defense One, February 10, 2015, www.defenseone.com/technology/2015/02/cia-bringing-amazons-marketplace-intelligence-community/105054/, (Access date: 27 March 2015).

If some of the analytics are closer or integrated in IoIT sensors, it will make it easier to combine such data with existing military tactical data systems, like Link 16[32] (or NILE[33], aka Link-22), that exchange track data with various elements in a battlefield. That could be different from the view of cyberwarfare where the friendly and opposing forces try to use the public Internet to their respective advantages as illustrated in Figure 4.

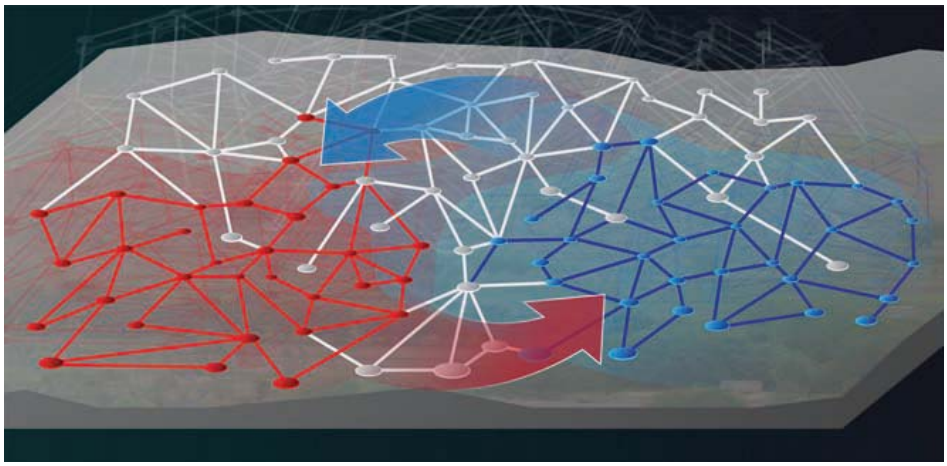

Figure 4: Example from [16] where combatants (red and blue nodes) perform cyberattacks partly through the civilian Internet of Things (gray nodes), to which they will be inevitably connected[34].

IoBT may involve some overwhelming cognitive load if the systems are not well designed. In fact "human warfighters under extreme cognitive and physical stress will be strongly challenged by the IoBT's complexity and the information it will produce. The IoBT will have to assist humans in making useful sense of this massive, complex, and perplexing ocean of information". That means that a well-adapted IoBT system should provide concise actionable information by using analytics and other processing to exploit the raw data from the multitude of sources and sensors available to produce information suitable to first responders or combatants. This is a good opportunity to use the AI capabilities of IoITs.

IoBT is expected to include improved more intelligent versions of current systems including unattended ground systems, all environments unmanned vehicles or drones and fire-and-forget missiles as pointed out in [93]. Soldiers will often collaborate with robots or autonomous systems especially for high-risk tasks such as explosives detection and neutralisation. Directed energy and electromagnetic weapon attacks could compromise digital and communication systems. Anticipating such attacks and training for alleviating as much as possible the impact on mission success will be necessary.

Even during cyberattacks one can access a surveillance street camera on the civilian Internet of Things and use an application to detect if it has been tempered or if the video feed is real or substituted, also an illumination flare could be used to check if the background light changes.

[32] Link 16 is a military tactical data exchange network used by NATO. Its specification is part of the family of Tactical Data Links. With Link 16, military aircraft as well as ships and ground forces may exchange their tactical picture in near-real time.
[33] NATO Improved Link Eleven (NILE) Program.
[34] Authorisation to use this illustration was provided by the author (Kott-Labbé, 13 April 2017).

4.2 An example of application: real-time cooperative blue-force tracking

Here is a description excerpted from "Cooperative blue-force tracking (BFT) and shared situation awareness (SA) in complex terrains" [89] where smart entities could be labelled as IoITs.

Improved shared awareness depends on a variety of factors spread over different domains, from cognitive psychology to information technology. Research on the latter, the focus of [89], has resulted in improvements in networks, networked sensors, geolocation, data fusion, information management and information sharing. The novel aspect is that it explores the potential synergy gained by integrating such improvements in such a way that the probability of failures of any component does not unduly reduce the overall performance. This synergy results from integrating the following: advanced mobile ad hoc networks (MANETs), wireless self-healing autonomous sensing networks (SASNet), radio location measurements, Global Positioning System (GPS), inertial navigation system (INS) based on higher-precision low-cost miniature inertial measurement units (IMUs), geographic information system (GIS), and capable handheld devices for command and control (C2) and information management (IM) with interfaces to users such as touch-screen displays usable in cold, hot, dusty, wet, low-light and full-sun environments.

Such integration in handheld devices can be applied to domestic, commercial and military applications. It allows for the provision of unprecedented levels of self- and shared-situation awareness (SA) and decision making capabilities for disperse civilian and military operations, providing continuous shared blue-force tracking (BFT) of assets and people in all conditions, including indoor, as well as more persistent sensed data about non-participating elements or opposing forces in an operational theatre. The novel solutions for cooperatively generating and sharing localization information use an integrated sensor-based GPS-INS-GIS-Radio system.

One important justification for the proposed integration is based on the fact that at the Earth's surface, GPS signals are very weak, making them susceptible to jamming and attenuation. Conversely, the small distances between nodes make MANET cooperative radio networking, network localization and tracking relatively resistant to jamming. Advanced MANET radio signals allow for much improved measurements of time of arrival (TOA), time difference of arrival (TDOA), and sometimes angle of arrival (AOA), for locating a source of signal position in two or three dimensions. More information and simulation results are available in [89].

5. Anticipated potential improvement by having smart processing at the sensor itself

Previous studies of various architectures of information processing and exchange in support of large coalition preparedness exercises focussing on the outcomes of engagements based on the quality of the information provided to decision makers (or simulated ones) allowed to propose a general model (Figure 5) linking engagement success rate to timeliness and intrinsic positional accuracy of sensors (accuracy is inversely proportional to each circular-uncertainty area (CUA) of a sensor report) [2, 85, 87]. When comparing the engagement success rates using the hypothetical architecture changes described in [2] one observed significant improvements as the high rate of sensor reports is processed more closely to the sensors. The best performance is when the global information from the command and fusion centres is sent to the local unit processing its organic data from its sensors (organic in this context means own local sensors without the need of radio, satellite or wide area networks). This architecture change allowed improving the timeliness of tactical actionable information to decision makers and weapon systems.

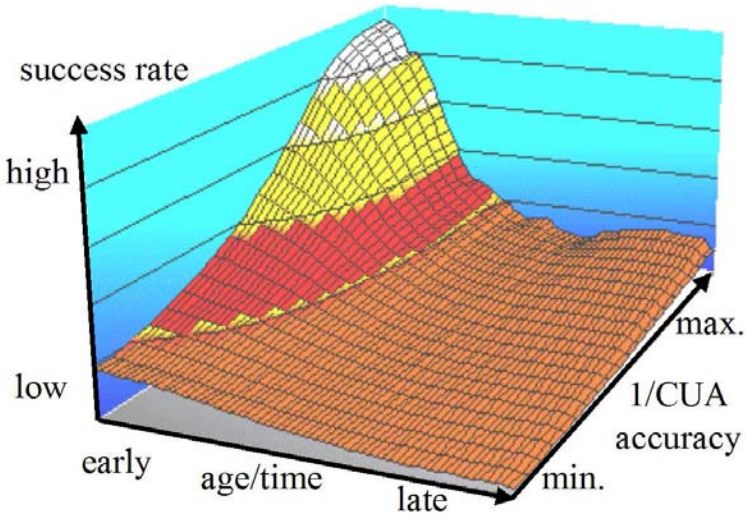

Figure 5: Potential mission success rate as function of input information age and accuracy for a fixed effectors' strategy [2].

At the time of these exercises little automations to sensor analyses and data fusion were available. These processes were human intensive. Now we have more autonomous data processing and data fusion available but too much of these processes are still done at centralized facilities or high performance military platforms or centres. One of the proposed architecture changes assumed that the federated database is replaced by a virtually federated database, i.e., distributed across the federation of platforms and sensors. For this change (labeled Change 3 in [2]) it was found that the optimistic maximum improvement was 54% of the maximum total possible of 63% based of perfect fusion processing and sharing (no time delays associated with these functions and perfect fusion of data from all available sources). "This 54% increase imposes a Change 3 that includes instantaneous situation assessment using all available information, perfect synchronization and negotiation among participants, and that information exchange delays and losses are null."

With the advances in low cost, small form factor and low power demand of specialized AI for IoIT we expect similar level of improved success rates of outcomes for the decision made from the actionable information generated by virtually federated sensors (including UAVs, motes and other autonomous platforms using some AI). The resulting percentage of improvement due to AI imbedded in all significant IoIT will depend on the types of scenarios at play, types of engagements and targets tracked as well as types of decisions sought. However, the author is convinced that there are sufficient evidences to say that having more intelligent and fast processing at the sensors level would generally provide a clear advantage to forces using this technology than those not taking advantage of it.

In addition as indicated previously about ALIX, instead of sending unprocessed high volume of sensor data which exceeded the satellite data rate, causing significant discontinuities in the sharable picture, sending high-value actionable information at a much lower data rate demand would have demonstrated a much higher rate of real time useful information for immediate decision making.

6. Conclusion

The reviewed technology advancements provided some indications that it is possible to develop safe and cost effective achievable internetworking of intelligent things ecosystems with significant advantages to early adopters. Based on recent science and technology outlook, it appears that we are at the cusp of practical specialized artificial intelligence in small devices but energy demand is still an issue. Similarly the transceiving capabilities of 5G smart cellular phones open access to advanced communication systems with SDR capabilities not available before at low cost and with low energy demand. Future intelligent things will be more aware where they are and will be able to sense their environments either local radio spectrum time history, temperature, humidity, capture surrounding sounds and other sensed data. In addition smaller devices with high memory density and computing capabilities with low power demand makes achievable advance security and encryption possible as well as local analytics which will provide more useful and actionable information to be shared. Moving some data analytics closer to all-domain sensors increases the ecosystem energy efficiency, reduces the amount of raw data transmitted, and the burden on end users and central data centers.

More work is required to accurately estimate the potential gain in terms of mission success rate from the hypothetical adoption of such technologies that minimize operational cost and information management burden with extremely large numbers of data sources. However first order estimates for target interceptions and other time constrained tactical actions or manoeuvers are very promising.

Could early adoption of internetworking of intelligent things provide significant advantages? It appears that there are more evidences in favor of this hypothesis than an opposite affirming that the increase in the number of devices susceptible to cyberattacks and hacking would deny such advantages. The adoption of improved AI, protocols, software and hardware will contribute to make the evolved IoIT ecosystems more agile in face of unknown threats. In addition the AI components of such ecosystems could contribute to respond to any (cyber) attacks in real time or much faster than a human operator could do. In addition one should consider the fact that building an IoT network and its cloud is inexpensive. NASA's Jet Propulsion Laboratory (JPL) IT CTO suggests[35]: “build an IoT network that's separate from the regular network”.

Other studies should examine the social aspect of the AI components, interactions with human and acceptation of AI in military affairs.

7. References

[1] D. S. Alberts, *The Agility Advantage* (US DOD Command & Control Research Program). 2011.

[2] P. Labbé, Z. Maamar, E. Abdelhamid, B. Moulin, R. Proulx, and D. Demers, "Recommendations for Network-and Internet-based Synchronized E-activities for Location-and Time-dependent Information," in *7th International Command and Control Research and Technology Symposium, 7th ICCRTS*, Loews Le Concorde, Québec City, Canada, 2002, p. 27: CCRP.

[35] http://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjM3dOW7bvVAhWs24MKHcUiAzUQFgguMAE&url=http%3A%2F%2Fwww.informationweek.com%2Fstrategic-cio%2Fexecutive-insights-and-innovation%2Fthe-jet-propulsion-laboratory-reaches-for-the-cloud%2Fd%2Fd-id%2F1319821&usg=AFQjCNErWe_6855C1wvC8a3AA5xzaqFjDg (Access date: 3 August 2017)

[3] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, "A Review on Internet of Things for Defense and Public Safety," *Sensors,* Article vol. 16, no. 10, pp. 1-44, 2016.

[4] R. Karimi and M. Kalantari, "Enhancing security and confidentiality in location-based data encryption algorithms," in *Fourth International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2011)*, 2011, pp. 30-35.

[5] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)," in "IEEE Internet Initiative | iot.ieee.org," 2015, Available: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

[6] K. Ivanova, G. E. Gallasch, and J. Jordans, "Automated and Autonomous Systems for Combat Service Support: Scoping Study and Technology Prioritisation," Australian Government, Department of Defence, Defence Science and Technology October 2016, Available: https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TN-1573.pdf.

[7] M. A. Kolodnya, P. H. Deitzb, and T. Phama, "MINI-DASS: a New Missions & Means Framework Ontological Approach for ISR PED Missions... the magic rabbits," Accessed on: 17 April 2017 Available: http://internationalc2institute.org/s/16-75-zj2w.pdf

[8] J. Chudzikiewicz, J. Furtak, and Z. Zielinski, "Fault-tolerant techniques for the Internet of Military Things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, 2015, pp. 496-501: IEEE.

[9] J. Chudzikiewicz, J. Furtak, and Z. Zielinski, "Secure protocol for wireless communication within Internet of Military Things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 508-513: IEEE.

[10] T. Kaur and D. Kumar, "Wireless multifunctional robot for military applications," in *2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS)*, 2015, pp. 1-5.

[11] J. Lee, L. Kant, A. McAuley, K. Sinkar, C. Graff, and M. Patel, "Planning & design of routing architectures for multi-tier military networks," in *MILCOM 2012 - 2012 IEEE Military Communications Conference*, 2012, pp. 1-7.

[12] NATO, "Advanced Autonomous Formation Control and Trajectory Management Techniques for Multiple Micro UAV Applications / Contrôle d'une formation autonome évoluée et gestion des trajectoires techniques d'applications pour micro UAV multiple," in "RTO-EN-SCI-195," Research and Technology Organization, Neuilly-sur-Seine (France) Systems Concepts and Integration Panel, Educational Notes RTO-EN-SCI-195, 01 Jun 2008, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.

[13] Missouri S&T, "Missouri S&T gets funding to develop battlefield 'smart dust'," *American Ceramic Society Bulletin,* Article vol. 89, no. 8, pp. 4-4, 2010.

[14] G. Hua, Y. X. Li, and X. M. Yan, "Research on the Wireless Sensor Networks Applied in the Battlefield Situation Awareness System," in *Advanced Research on Electronic Commerce, Web Application, and Communication, Pt 2*, vol. 144, G. Shen and X. Huang, Eds. (Communications in Computer and Information Science, 2011, pp. 443-449.

[15] L. Kant, W. Chen, C. Lee, A. Sethi, and M. Natu, "D-FLASH: Dynamic Fault Localization and Self-Healing for Battlefield Networks," presented at the Proceedings for the Army Science Conference (24th), Orlando, Florida, 29 November - 2 December, 2005. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA432120

[16] A. Kott, A. Swami, and B. J. West, "The Internet of Battle Things," *Computer,* Article vol. 49, no. 12, pp. 70-75, 2016.

[17] M. Maher, "Joint Tactical Radio System: Tactical Network Planning and Management," in *MILCOM 2007 - IEEE Military Communications Conference*, 2007, pp. 1-7.
[18] P. P. Ray, "Towards an Internet of Things based architectural framework for defence," in *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, 2015, pp. 411-416.
[19] S. Ray, "In-Theatre Sense & Respond Logistics In-Theatre S&RL - TA5. Investigation of Selected Decision Support and Disruptive Technologies," Defence Research and Development Canada, Valcartier Research Centre, Quebec QC (CAN);Thales Canada, Quebec Que (CAN), Canada, Contract Report DRDC-RDDC-2016-C250, 01 Feb 2016, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.
[20] N. Suri *et al.*, "Analyzing the Applicability of Internet of Things to the Battlefield Environment," in *2016 International Conference on Military Communications and Information Systems (ICMCIS)*, Brussels, Belgium, 2016, pp. 117-122.
[21] M. Kranz, P. Holleis, and A. Schmidt, "Embedded interaction: Interacting with the internet of things," *IEEE internet computing,* vol. 14, no. 2, pp. 46-53, 2010.
[22] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics,* vol. 10, no. 4, pp. 2233-2243, 2014.
[23] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer,* vol. 44, no. 9, pp. 51-58, 2011.
[24] W. Yeager and J.-H. Morin, "Introduction to Cloud and the Internet of Things: Challenges and Opportunities Minitrack," in *Proceedings of the 50th Hawaii International Conference on System Sciences / Cloud and Internet of Things:: Challenges and Opportunities Minitrack*, 2017, p. 5931.
[25] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (IIoT)–enabled framework for health monitoring," *Computer Networks,* vol. 101, pp. 192-202, 2016.
[26] C. Johnson, "Securing the Participation of Safety-Critical SCADA Systems in the Industrial Internet of Things," Accessed on: 24 April 2017, Available: http://eprints.gla.ac.uk/130828/1/130828.pdf
[27] M. R. Palattella *et al.*, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications,* vol. 34, no. 3, pp. 510-527, 2016.
[28] W. C. Buhrow, *Biometrics in support of Military Operations; Lessons from the Battlefield*. Boca Raton, FL: CRC Press, 2017.
[29] Y. Chen and H. Hu, "Internet of intelligent things and robot as a service," *Simulation Modelling Practice and Theory,* vol. 34, pp. 159-171, 2013.
[30] J. Kaivo-oja, P. Virtanen, H. Jalonen, and J. Stenvall, "The effects of the internet of Things and big data to organizations and their knowledge management practices," in *International Conference on Knowledge Management in Organizations*, 2015, pp. 495-513: Springer.
[31] A. Arsénio, H. Serra, R. Francisco, F. Nabais, J. Andrade, and E. Serrano, "Internet of intelligent things: Bringing artificial intelligence into things and communication networks," in *Inter-cooperative Collective Intelligence: Techniques and Applications*: Springer, 2014, pp. 1-37.
[32] P. Stone *et al.*, "Artificial Intelligence and Life in 2030," *One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel,* 2016.
[33] A. Esteva *et al.*, "Dermatologist-level classification of skin cancer with deep neural networks," *Nature,* vol. 542, no. 7639, pp. 115-118, 2017.
[34] L. Kumar and A. Sureka, "Using Structured Text Source Code Metrics and Artificial Neural Networks to Predict Change Proneness at Code Tab and Program Organization Level," in

Proceedings of the 10th Innovations in Software Engineering Conference, 2017, pp. 172-180: ACM.

[35] D. Jeannerat, "Human-and computer-accessible 2D correlation data for a more reliable structure determination of organic compounds. Future roles of researchers, software developers, spectrometer managers, journal editors, reviewers, publisher and database managers toward artificial-intelligence analysis of NMR spectra," *Magnetic Resonance in Chemistry,* vol. 55, no. 1, pp. 7-14, 2017.

[36] J. Lemley, S. Bazrafkan, and P. Corcoran, "Deep Learning for Consumer Devices and Services: Pushing the limits for machine learning, artificial intelligence, and computer vision," *IEEE Consumer Electronics Magazine,* vol. 6, no. 2, pp. 48-56, 2017.

[37] K. Bourzac, "To Get AI in Everyday Gadgets, Engineers Go to Specialized Hardware," no. February, 14 Feb 2017 | 15:00 GMT. Accessed on: 14 June 2017, Available: http://spectrum.ieee.org/tech-talk/semiconductors/processors/to-get-ai-in-everyday-gadgets-engineers-go-to-specialized-hardware

[38] C.-M. Chen, S.-C. Hsu, and G.-H. Lai, "Defense Denial-of Service Attacks on IPv6 Wireless Sensor Networks," in *Genetic and Evolutionary Computing: Proceedings of the Ninth International Conference on Genetic and Evolutionary Computing, August 26-28, 2015, Yangon, Myanmar - Volume 1*, T. T. Zin, J. C.-W. Lin, J.-S. Pan, P. Tin, and M. Yokota, Eds. Cham: Springer International Publishing, 2016, pp. 319-326.

[39] L. Wang *et al.*, "Survey on distributed mobility management schemes for Proxy mobile IPv6," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, 2014, pp. 132-138: IEEE.

[40] A. J. Jara, S. Varakliotis, A. F. Skarmeta, and P. Kirstein, "Extending the Internet of Things to the Future Internet through IPv6 support," *Mobile Information Systems,* vol. 10, no. 1, pp. 3-17, 2014.

[41] DoD CIO, "DoD Policy Recommendations for The Internet of Things (IoT)," U.S. Department of Defense, Chief Information Officer (CIO) December 2016.

[42] M. L. Das, "Privacy and Security Challenges in Internet of Things," in *Distributed Computing and Internet Technology, Icdcit 2015*, vol. 8956, R. Natarajan, G. Barua, and M. R. Patra, Eds. (Lecture Notes in Computer Science, 2015, pp. 33-48.

[43] R. S. Ferrell, "Uninterrupted Information Crucial to Agile Army," *Army Magazine,* Article vol. 66, no. 10, pp. 151-154, 2016.

[44] L. Jaeseung, S. Yunsick, and P. Jong Hyuk, "Lightweight Sensor Authentication Scheme for Energy Efficiency in Ubiquitous Computing Environments," *Sensors (14248220),* Article vol. 16, no. 12, pp. 1-14, 2016.

[45] J. Keller, "DARPA eyes cybersecurity for Internet of Things and embedded computing," *Military & Aerospace Electronics,* Article vol. 27, no. 7, pp. 8-8, 2016.

[46] K. Klawon, J. Gold, K. Bachman, and D. Landoll, "Considering IIOT and Security for the DoD," in *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR Vii*, vol. 9831, M. A. Kolodny and T. Pham, Eds.: Proceedings of SPIE, 2016.

[47] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 839-858: IEEE.

[48] F. Li, Y. Han, and C. Jin, "Practical access control for sensor networks in the context of the Internet of Things," *Computer Communications,* vol. 89–90, pp. 154-164, 9/1/ 2016.

[49] C.-H. Liao and T.-K. Woo, *Adaptation from transmission security (TRANSEC) to cognitive radio communication*. INTECH Open Access Publisher, 2012.

[50] J. P. M. Lichtman, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, J. H. Reed, "A Communications Jamming Taxonomy," *IEEE Security & Privacy,* Feb. 2016.
[51] O. R. Merad Boudia, S. M. Senouci, and M. Feham, "A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography," *Ad Hoc Networks,* vol. 32, pp. 98-113, 2015.
[52] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks,* vol. 10, no. 7, pp. 1497-1516, 9 2012.
[53] S. Nagy, "Report on Cisco Live Melbourne 2015," DSTO Cyber and Electronic Warfare Division, Edinburgh (AUSTRALIA), Ottawa, Canada, General Document DSTO-GD-0880, 01 Jun 2015 2015, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.
[54] H. Ning, H. Liu, and L. T. Yang, "Cyberentity Security in the Internet of Things," *Computer,* vol. 46, no. 4, pp. 46-53, 2013.
[55] A. Singla, A. Mudgerikar, I. Papapanagiotou, and A. A. Yavuz, "HAA: Hardware-Accelerated Authentication for internet of things in mission critical vehicular networks," in *MILCOM 2015 - 2015 IEEE Military Communications Conference*, 2015, pp. 1298-1304.
[56] J. A. Stankovic, "Adaptive and Reactive Security for Wireless Sensor Networks," Virginia Univ, Charlottesville Dept of Computer Science 2007.
[57] J. A. Stankovic, "Robust and Secure Localization," Virginia Univ, Charlottesville 2009.
[58] L. Wenchao, Y. Ping, W. Yue, P. Li, and L. Jianhua, "A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network," *Journal of Electrical & Computer Engineering,* Article pp. 1-8, 2014.
[59] T. Zhang, H. Antunes, and S. Aggarwal, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," *IEEE Internet of Things Journal,* vol. 1, no. 1, pp. 10-21, 2014.
[60] B. Zhu, A. Joseph, and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 2011, pp. 380-388.
[61] S. Zhu, G. Cao, and P. Liu, "Distributed Self-healing Mechanisms for Securing Sensor Networks," State Univ. of New York at Buffalo, Amherst Research Foundation 2010.
[62] C. Belisle, V. Kovarik, L. Pucker, and M. Turner, "The software communications architecture: two decades of software radio technology innovation," *IEEE Communications Magazine,* vol. 53, no. 9, pp. 31-37, 2015.
[63] R. C. Dixon, *Spread Spectrum Systems: With Commercial Applications*. New York, NY, USA: John Wiley & Sons, Inc., 1994.
[64] M. Möstl, J. Schlatow, R. Ernst, H. Hoffmann, A. Merchant, and A. Shraer, "Self-aware systems for the Internet-of-Things," in *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)*, 2016, pp. 1-9: IEEE.
[65] S. Kounev *et al.*, "The Notion of Self-aware Computing," in *Self-Aware Computing Systems*: Springer, 2017, pp. 3-16.
[66] A. F. Cattoni, M. Musso, and C. S. Regazzoni, "Integration Between Navigation and Data-Transmission Systems in a Software Defined Radio Framework," 2007.
[67] A. F. Cattoni, M. Musso, and C. S. Regazzoni, "SDR Analog Front-End Architecture For Simultaneous Digitalization of Data Transmission and Navigation Signals," in *SDR Forum Technical Conference*, 2007.
[68] P. Labbé, D. Arden, L. Li, and Y. Ge, "Self-Aware / Situation Aware; Integrated Handhelds for Dispersed Civil and Military Urban Operations," *Inside GNSS,* vol. 2, no. 2, pp. 34-45, March/April 2007.

[69] P. Labbé, "GPS and GIS Integration in Mobile Equipment for Improved Mobile Emergency Operations," in *Proceedings of the 12th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1999)*, Nashville, TN, 1999, pp. 545-554.

[70] P. Labbé, D. Arden, and L. Li, "GPS-INS-Radio and GIS Integration into Handheld Computers for Disperse Civilian and Military Urban Operations," in *Proceedings of the 2007 National Technical Meeting of The Institute of Navigation*, The Catamaran Resort Hotel, San Diego, CA, 2007, pp. 998 - 1010.

[71] D. Waller, I. Chapman, and M. Michaud-Shields, "Concept of Operations for the Self-healing Autonomous Sensor Network," Defence R&D Canada - Centre for Operational Research and Analysis, Ottawa ON (CAN), Technical Memorandum DRDC-CORA-TM-2008-052, 01 Jul 2009, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.

[72] Y. Zhou, J. Schembri, L. Lamont, and J. Bird, "Experiments and analysis of stand-alone GPS for relative location discovery for SASNet," Defence R&D Canada, Ottawa ONT (CAN), Technical Memorandum DRDC-OTTAWA-TM-2010-140, 01 Aug 2010, Available: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc107/p533710_A1b.pdf.

[73] B. Ricard, "Le noeud de capteur SASNet," Defence Research and Development Canada, Valcartier Research Centre, Quebec QC (CAN), Canada, Scientific Report DRDC-RDDC-2014-R70, 01 Dec 2014, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.

[74] L. Li, "Localization in Self-Healing Autonomous Sensor Networks (SASNet): Studies on Cooperative Localization of Sensor Nodes Using Distributed Maps," Defence R&D Canada - Ottawa, Ottawa ONT (CAN), Ottawa, Canada, Technical Report DRDC-OTTAWA-TR-2008-020, 01 Jan 2008, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.

[75] M. Deziel, "A Reliable Transport Protocol for Resource Constrained Nodes / Un Protocole de transport avec garantie de livraison pour les appareils de communications aux ressources limitées," Defence Research and Development Canada, Ottawa Research Centre, Ottawa ON (CAN);Communications Research Centre, Ottawa ONT (CAN), Contract Report DRDC-RDDC-2014-C109, 01 Jun 2014, Available: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc198/p800537_A1b.pdf.

[76] C. Widdis, "SASNet Sensor Signal Processing Algorithms: Part 1," Defence R&D Canada - Valcartier, Valcartier QUE (CAN);MacDonald Dettwiler and Associates Ltd, Dartmouth NS (CAN), Contractor Report DRDC-VALCARTIER-CR-2009-010, 01 Jan 2009.

[77] W. Shen, "Self-Reconfigurable Robots for Adaptive and Multifunctional Tasks," presented at the AIAA SPACE 2009 Conference & Exposition, AIAA SPACE Forum, Pasadena, California, 2008.

[78] D. Waller, "A Simulation Study of the Effectiveness of the Self-healing Autonomous Sensor Network for Early Warning Detection," Defence R&D Canada - Centre for Operational Research and Analysis, Ottawa ON (CAN), Technical Memorandum DRDC-CORA-TM-2009-019, 01 Jul 2009, Available: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc87/p531821.pdf.

[79] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials,* vol. 17, no. 4, pp. 2347-2376, 2015.

[80] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things Security" Hands-On"," *IEEE Security & Privacy,* vol. 14, no. 1, pp. 37-46, 2016.

[81] Y. Deng, L. Wang, K.-K. Wong, A. Nallanathan, M. Elkashlan, and S. Lambotharan, "Safeguarding massive MIMO aided hetnets using physical layer security," in *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, 2015, pp. 1-5: IEEE.

[82] F. Delaveau, A. Evesti, J. Suomalainen, and N. Shapira, "Active and passive eavesdropper threats within public and private civilian wireless-networks–existing and potential future countermeasures–a brief overview," *Proceedings of SDR,* pp. 11-20, 2013.
[83] P. Pirinen, "A brief overview of 5G research activities," in *2014 1st International Conference on 5G for Ubiquitous Connectivity (5GU)*, 2014, pp. 17-22: IEEE.
[84] S. Datta, "Cybersecurity-An Agents based Approach?," *DSpace@MIT,* Accessed on: 2017-04-09 Available: http://hdl.handle.net/1721.1/107988
[85] P. Labbé and R. Proulx, "Impact of Systems and Information Quality on Mission Effectiveness," in *5th International Command and Control Research and Technology Symposium, 5th ICCRTS. 2000.*, Canberra, ACT, Australia, 2000, p. 36: CCRP.
[86] DoD, "Introduction to tactical digital information link J and quick reference guide (TADIL J)," HQ TRADOC ATDO-A, Fort Monroe, VA 2000.
[87] P. Labbé, L. Lamont, Y. Ge, and L. Li, "Creating a Dynamic Picture of Network Participant Geospatial Information in Complex Terrains," in *proceedings of the International Conference on Global Defense and Business Continuity (ICGD&BC), First International Workshop on Tracking Computing Technologies (TRACK)*, Santa Clara, California, 2007, p. 13: IEEE.
[88] P. Labbé, "Collaborative Blue-forces Tracking and Beyond," ed. DRDC Ottawa: proceedings of the Pan-TTCP Workshop on the Robustness and Vulnerability of Network Centric Warfare 2007, p. 44 slides.
[89] P. Labbé, L. Lamont, Y. Ge, and D. Arden, "Cooperative Blue-force Tracking (BFT) and Shared Situation Awareness (SA) in Complex Terrains," in *proceedings of the Sensors & Electronics Technology (SET) Panel Symposium on Military Capabilities Enabled by Advances in Navigation Sensors, NATO RTA-SET-104*, Antalya, Turkey, 2007, p. 20.
[90] R. A. Van den Braembussche, "Micro Gas Turbines – A Short Survey of Design Problems," in "Applied Vehicle Technology Panel," Research and Technology Organization, Neuilly-sur-Seine (France) RTO-EN-AVT-131, 01 Dec 2005.
[91] S. Adee, "Wireless sensors that live forever; Energy harvesters and radioisotopes fuel tiny transmitters," *IEEE Spectrum,* vol. 47, no. 2, pp. 14-14, 2010.
[92] J. Mariani, B. Williams, and B. Loubert. (2015)6 July) Continuing the march: The past, present, and future of the IoT in the military; The Internet of Things in defense. *The Internet of Things in the defense industry*. Available: https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-military-defense-industry.html
[93] A. Kott, D. S. Alberts, and C. Wang, "Will Cybersecurity Dictate the Outcome of Future Wars?," *Computer,* vol. 48, no. 12, pp. 98-101, 2015.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC
Defence Research and Development Canada
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Could early adoption of internetworking of intelligent things provide significant advantages?

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Labbé, Paul

5. DATE OF PUBLICATION (Month and year of publication of document.)

December 2017

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

22

6b. NO. OF REFS (Total cited in document.)

96

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

External Literature (P)

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC
Defence Research and Development Canada
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2017-P100

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11a. FUTURE DISTRIBUTION (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Any limitations on further dissemination of the document, other than those imposed by security classification.)

12. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This paper reviews technology advances from different perspectives that could provide safe and cost effective achievable internetworking of intelligent things ecosystems with significant advantages to early adopters. Based on recent science and technology outlook, it appears that we might be at the cusp of practical specialized artificial intelligence in small devices. Similarly the transceiving capabilities of fifth generation cellular phones open access to advanced communication systems with capabilities not available before at low cost and with low energy demand. Future intelligent things will be more aware where they are and will be able to sense their environments either local radio spectrum time history, temperature, humidity and capture surrounding sounds. In addition smaller devices with high memory density and computing capabilities with low power demand make achievable advance security and encryption possible as well as local analytics which will provide more useful and actionable information to be shared. Moving some data analytics closer to alldomain sensors increases the ecosystem energy efficiency, reduces the burden on end users and central data centers. As much as possible, this paper will estimate the potential gain in terms of military mission success rate from the hypothetical adoption of such technologies that minimize operational cost and information management burden with extremely large numbers of data sources.

---

13. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Internet of things (IoT), industrial internet of things (IIoT), internet of intelligent things (IoIT), internet of battlespace things (IoBT), internet of military things (IoMT), internet protocol version 6 (IPv6), contested urban environment (CUE), fifth generation of cellular technologies (5G), jamming, low probability of intercept (LPI), low probability of detection (LPD), artificial intelligence (AI), analytics, track data, emerging technology, efficiency, C4ISR.