Research on Military Applications of Internet of Things

Yan Yang

Officers College of PAP, Chengdu, Sichuan, 610213

Keywords: military applications; Internet of Things

Abstract: In order to better promote military information construction, through the analysis of the technical characteristics and advantages of the Internet of Things, the future of military applications of the Internet of Things is discussed, and the Internet of Things is described in military logistics, inventory management, future battlefields, weapons and equipment management, and intelligence in camps, and other aspects of the application program, and pointed out that the military Internet of things in the information security risks. It is believed that with the further development and improvement of technology, the Internet of Things will change the pattern of war in the future.

1. Introduction

Once the concept of the Internet of Things was introduced, it was immediately followed by extensive attention and attention from governments, academia, industry, and news media. The promotion of Internet of Things technology will not only become a driver for economic development [1], but also open up opportunities for industry with unlimited potential for development, and it will also have a huge impact on the existing military system landscape. At present, the world's major military powers have already smelled the atmosphere of this wave of tides, and they have formulated standards, research and development techniques, and applied them in an attempt to occupy a favorable position in a new round of military reforms. As early as 1999, the International Conference on Mobile Computing and Networks held in the United States proposed that "the sensor network is another development opportunity that humankind will face in the next century." In 2003, the U.S. Department of Defense pushed RFID bar code identification technology to make it known to the world. On November 17, 2005, the International Telecommunication Union (IT U) released "I TU Internet Report 2005: Internet of Things." The publication of the report marks the imminent arrival of the Internet of Things in the world. In October 2008, the European Internet of Things Conference was held in France. In June 2009, the EU formulated and announced a 14-point action plan including standardization, research projects, management mechanisms, and an international dialogue. Japan has formulated a national development strategy for the EPC system and proposed the U-Japan plan, which will include sensor network as one of the national key strategic projects. Korea proposed the U-Korea strategy and plans to build IoT infrastructure in 2012. Singapore also announced the strategic blueprint for "Smart State 2015." China also attaches great importance to the development of the Internet of Things and has placed it at the core of its national strategy. On November 3, 2009, Premier Wen Jiabao of the State Council stated clearly in the speech “Let Science and Technology Lead China’s Sustainable Development” published at the Capital Science and Technology Conference that “We must strive to break through the key technologies of sensor networks and Internet of Things, and deploy IP early. The related technology research and development of the times has made the information network industry an 'engine' to promote industrial upgrading and the information society."

However, most researches on the Internet of Things still remain on the conceptual hype. There is no unified understanding yet. Many key technologies of the Internet of Things are still in the initial stage of development. The system structure and construction methods of the Internet of Things have not formed a unified standard. With the model, this is both a challenge and an opportunity for the informationization of the Chinese military. Therefore, the study of IoT technology and its application in the military field is of great significance to the construction of the next-generation communications network for our military.

2. The Technology of Internet of Things

The Internet of Things refers to a vast network of various information devices such as radio frequency identification (RFID) devices, infrared sensors, global positioning systems, laser scanners and other devices that are combined with the Internet. The purpose of establishing the Internet of Things is to connect all the items to the network for intelligent identification, positioning, tracking, monitoring and management. If the technology represented by computers and the Internet has changed an era (mechanization era), then new technology clusters centered on the Internet of Things and cloud computing will eventually establish another era, that is, information marked by intelligence.

The Internet of Things has a wide range of applications in civilian applications, including the nine key applications of smart industry, smart agriculture, intelligent transportation, smart grid, smart environmental protection, smart security, smart medical care and smart home appliances [2]. At the same time, the key concepts of the Internet of Things have also brought far-reaching influence to the military field and have important strategic significance. Since logistics originated from the early Internet of Things, military logistics is one of the most important applications of the Internet of Things, which greatly improves the agility and security of military logistics [3]. With the development and application of Internet of Things technology, the application of military Internet of Things is not only reflected in the field of logistics, but also reflected in military reconnaissance, environmental monitoring, unmanned combat and other aspects [4]. The impact of the Internet of Things on the military is self-evident, but to truly realize the application of all aspects, there are still many problems that need to be resolved, such as the standardization issue, the cost of capital issues, and information security issues.

The rapid development of the Internet of Things technology and its application in the military require the enrichment and deepening of the content of networking. Although the definition of the Internet of Things is not clear, the architecture of the Internet of Things is universally accepted.

The sensing layer consists of various information sensors and collection devices, including two-dimensional bar code labels and sensor gateways, RFID electronic tags and RFID sensors, access gateways, intelligent terminals, and sensor networks. The main task of the sensory layer is to identify objects and collect information. The network layer is like the brain and neural network of the Internet of Things. It mainly includes a communication fusion network, a network management center, an information center, and an intelligent processing center. The main task of the network layer is to transmit and process the information obtained from the sensing layer. In the Internet of Things, in order to achieve a wide range of intelligence, the application layer has integrated the social division of labor and industrial needs of the Internet of Things and has developed a variety of solutions. These programs combine the advantages of the Internet of Things with industrial production and management, information management, and organizational scheduling to build an intelligent industry. For example, in the military, the application layer will provide detailed solutions for military applications such as force command, weapon control, battlefield monitoring, equipment support, surveillance and reconnaissance, military logistics, battlefield medical treatment, and salvage.

3. The Applications of Internet of Things in Military

The application of the Internet of Things can be divided into monitoring, query, control, and scanning. The following is an analysis and research on the application of the Internet of Things in the military.

In military supplies, the use of Internet of Things RFID technology can enhance the management, inventory, and inquiries of materials in transportation and distribution. In this process, the RFID electronic tag on each piece of goods, the handheld RFID reader/writer inside the material supply side, the RFID reader/writer of the exit access control system on the supply side of the goods, the

RFID reader/writer on the transport vehicle, and the warehouse on the demand side of the goods RFID readers for export access control systems, handheld RFID readers in warehouses, etc. can form an RFID reader/writer network. They work under the management of an RFID middleware platform, and the person in charge of distribution can use RFID. The middleware platform interface monitors and manages the data read and written by the received RFID reader. Benefits of the system: First, the visibility of materials from shipment to transportation and storage management can be enhanced and management becomes clear, transparent, and simple and accurate. Second, the safety of material transportation and management is improved, and Reliability; Third, warehouse managers can keep track of the quantity and demand patterns of materials in inventory and provide timely and accurate material supplements. In particular, during the war, the mastery of weapons and ammunition inventories is related to operational tasks of combat units. Whether or not the accomplishment of the planned operational objectives can be achieved; fourthly, comprehensive control of the situation can reduce waste of resources and save costs. Fifth, in joint operations based on information systems, military warehouses across military regions and multiple services can be networked. Combine a regional and nationwide logistics system and provide feedback on the demand information of various combat units so as to implement material guarantees in real time and accurately so that the entire security system is efficient and orderly.

In the future, the battlefield needs to use information technology to accurately and timely grasp the dynamic information of the battlefield in order to make decisions in real time and accurately. As early as 10 years ago, the U.S. military had completed the study of “smart dust”, an ultra-miniature sensor consisting of microprocessors, radios, and wireless network software. The volumes have become grit-sized and they can carry out information collection, information processing and information transmission, and future smart dust can even be suspended in the air. In the future joint battlefield, such miniature wireless sensors, radars, air strike forces, sea strike forces, missile systems, tanks, artillery, armored vehicles, combatants, battle command information systems, operational support systems, and command can be deployed. The center and others are organically combined to form a huge military IoT. The use of aircraft or other means to spread a large number of miniature wireless sensors in the vast area of the battlefield, the micro-wireless sensor self-organizing network, you can collect, transmit, fuse battlefield information, to provide each combat unit with "all necessary" intelligence services Including theater surveillance, enemy investigation, target tracking, and enemy damage assessment. Each fire unit can transmit the shooting effect, its own status, and other conditions to the relevant command system. Through real-time analysis of the system, it can timely implement safeguards and adjust the use of firepower. According to feedback from micro-wireless sensors, weapons and equipment, and combat personnel, the information command center can timely make corresponding adjustments, deployments, and safeguards. In the coming decades, the Internet of Things will change the battlefield environment and change the forms and methods of combat.

The management of weapons and equipment is mainly to maintain and maintain the physical functions of weapons and equipment in a controlled manner. IoT-based weapons and equipment management helps to automate and intelligentize management. The main idea is to first attach the global product electronic code (EPC) to the main components of the weapon and equipment; secondly, to use RFID, 3D visualization and other technologies to monitor and locate the status of weapons and equipment in real time; Through the monitoring system, the information of all parts and components is transmitted to the information processing system through the network communication technology; Finally, the collected information is comprehensively processed and then input into the weapon equipment management expert system, and the expert system automatically gives the corresponding Management plan.

4. Trend Analysis of Military Applications of Internet of Things

As a typical M2M system, the Internet of Things will be able to perceive a variety of information terminals that humans need to connect to the ubiquitous network consisting of a fixed network, a wireless mobile network, the Internet, the broadband network, and various other private networks.

In the broad sense, the Internet of Things implements extensive communication and information exchange between machine and person (M2P), person-to-person (P2P), and person-to-machine (P2M), and fundamentally solves the problem of communication between physical entities and information systems. At the same time, according to the needs of the contact itself, it also solved some network management problems such as self-organization, dynamic routing, automatic operation, and calculation processing. It should be pointed out that the management or monitoring of the Internet of Things cannot be equated with command and control in the military field, but it provides the prerequisites for the control of things in military applications.

Command and control in the military field means that the command and control entity issues a series of commands or instructions to the command and control object according to judgments and decisions. The object performs corresponding actions or activities according to the instruction, and finally completes the task assigned by the subject. On the one hand, the subject's decision-making process includes the complex process of analyzing, judging, comparing, planning, optimizing and evaluating; on the other hand, the activities or actions performed by the object are reversible and controlled and can be stopped or released.

The Internet of Things does not have a high level of control capability. After loading application systems such as expert decision-making, evaluation optimization, and behavior control, it only gives them “wisdom” and has the control capabilities of “Smart World”. Similarly, in military applications, intelligence terminals, complex computing software, and expert decision-making systems can also be embedded to give the “wisdom” to the Internet of Things and realize the development from things to materials.

The move from material to material control is a potential trend in the military’s military use of the Internet of Things. It is also an internal requirement and meets the actual needs and objective laws of military informatization construction. Controllability is a fundamental principle in the military field. Whether it is personnel, weapons, sensors, or safeguard resources, it must be continuously controllable in combat operations. Code control, precision control, and safety control are all designed to make control behavior more reliable. As mentioned above, the achievements, capabilities, and levels of current military information construction have been able to solve the problems of communication, sensing, identification, positioning, timeliness, navigation, and security. It should not be difficult to realize the Internet of Things, but it is just a matter of time. Therefore, for the military, it is not enough to target only things. Since human beings entered the information age, information technology has been continuously expanding human vision and thinking, bringing with it many unanticipated "long-tail effects", and physical control should be an inestimable consequence of the Internet of Things [5].

On the basis of the Internet of Things, if various intelligent decision-making units, control feedback units and agile control terminals are embedded on objects for specific applications, action control over natural objects can be achieved, and the level and level of command and control can be extended or refined. Go on. Among them, it includes not only the control of people but also the control of things. At the same time, it is also possible to achieve leapfrog control, self-organizing control, and loop autonomy. At present, in the “smart earth” and other foreign research projects, some simple concepts of physical control have been proposed. For example, on-board sensors replace the driver to control the car to slow down or turn off the engine in dangerous moments. The sensors in the refrigerator control the food according to the type and shelf life. These controls are simple control actions performed by the control agency after being judged according to predetermined rules. In military applications, it is possible to conduct more complex control actions, allowing the “control” to self-learn and make decisions through an expert system, and effectively control the state or behavior of “controlled” applications, especially in some applications. Dangerous, bad environment, complicated calculation, or high-intensity combat operations play an important role. The military-based command and control based on the Internet of Things will have a wider scope, greater flexibility, more distinctive distributed features, and more accurate, detailed, and secure command and control activities.

5. Conclusion

As the main driving force of the information technology revolution, the Internet of Things faces historical opportunities in its industrial development and its application in the military. At the same time, the application of the Internet of Things in the military field is an inevitable requirement for the development of military informatization. As a new concept, the military Internet of Things is still in the stage of exploration on the battlefield. In particular, some standardization issues and information security issues have not yet been resolved. However, we have reason to believe that the military will show its tremendous influence in the future battlefield.

References

[1] Wang Baoyun. A Survey of Internet of Things Technology [J]. Journal of Electronic Measurement and Instrument, 2009, 23(12) : 1-6.

[2] Ren Fengyuan, Huang Haining, Lin Yi. Wireless sensor networks [J]. Chinese Journal of Software, 2003, 14(7): 1282-1291.

[3] Wang Shengkai, Kong Ning. Application Prospect of Internet of Things Technology in Military Field [J]. Internet of Things Technology, 2012, 2(9): 62-65.

[4] Shen Subin, Fan Quli, Zong Ping, et al. Research on the architecture and related technologies of Internet of Things [J]. Journal of Nanjing University of Posts and Telecommunications, 2009, 29(6): 1-11.

[5] Zhou Haitao. Technology, Application and Development of Ubiquitous Network [J]. Telecommunications Science, 2009, 25(8): 97-100.