The Internet of Things

M

Nigel Mc Kelvey
Letterkenny Institute of Technology, Ireland

Kevin Curran
University of Ulster, School of Computing and Intelligent Systems, Northern Ireland

Nadarajah Subaginy
University of Ulster, School of Computing and Intelligent Systems, Northern Ireland

INTRODUCTION

The Internet of Things (IoT) also known as Web of Things (WoT) is a concept where everyday devices - home appliances, sensors, monitoring devices - can be accessed through the Internet using well known technologies such as URLs and HTTP requests (Gomez et al., 2013). It is estimated that more than 4 billion users of mobile phones already have the ability to access the Internet. Advances in technologies are changing i.e. the way we use the Internet. Intelligent devices found in devices such as fridge's, machine's, factories and even clothes are connecting and interacting automatically on their own without human interaction by use of sensors that transmit data. It is soon expected that there will be more devices or "things" on the Internet than there will be people (Ben-Saied et al., 2014).

IoT has been emerged as one of the most important shifts of thought with regards to the future state of Internet. Its significance is described in terms of providing a different lens on how to link the Internet with real world's objects. In a more comprehensive way, IoT transforms real world objects into smart objects and connect them through Internet. In contrast with the current Internet, IoT depends on a more flexible architecture where physical objects with embedded sensors will communicate with a cloud to send and analyse data using the Internet Protocol. IoT envisions a future in which digital and physical entities can be linked, through their unique identifier and by means of appropriate information and communication technologies (Montavont et al., 2014). There are still open issues regarding 5 IP-WSN (Internet Protocol Wireless Sensor Network) features in an IoT scenario: IPv6 Adaptation, Mobility, WEB Enablement, Time Synchronisation and Security.

Before discussing how the Internet is evolving towards an Internet of Things it is important to understand how the Internet has changed from web 1.0 to web 2.0 and now to the Internet of Things we need to understand the technology and changes in society that have made this happen or even possible. Web 1.0 allowed people to communicate on a global scale by broadcasting their messages (Kalfoglou, 2012). It was focused more towards organizations than individuals. What was on the web or the content of what made up web 1.0 was not seen to be free to all user's like it is today, organizations sought to control or have ownership of this content. Web 1.0 did not allow for personal interaction. User's would have created HTML home pages listing whatever information they wanted about themselves but this information was static or read only. Anyone looking to obtain information over the web would probably have ended up paying a subscription to some on-line encyclopaedia company such as Britannica. Technologies such as JavaScript, XML, Ajax, RSS, Apache, MySQL and infrastructure improvements such as broadband has taken the power away form organizations in terms of content or ownership of information on the web and given it back to the people. Now users could create feature rich dynamic web content, allowing them to become contributors and producers of information. The emphasis was now based on the sharing of information and not ownership. Web 2.0 offers user's and communities a global stage on which they could perform, weather it be posting videos on YouTube showing off there talents or lack of talent, or web forums offering advice or solutions to

DOI: 10.4018/978-1-4666-5888-2.ch570

individual worries or problems ranging from diseases and treatments to software fixes and code solutions.

With users now having the ability to generate and post their own content. Social networking sites such as Facebook have been set up to take advantage of this by providing user's a platform on which they can interact. Social networking sites such as Facebook have changed the traditional ways people have communicated, socialised or even became friends it also expected to do the same for organizations in terms of networking and making business connections. This is due partly to the global reach of Facebook. Due to the large number of sensors, an IoT scenario deals with big volumes of data. There are three main problems that must be solved: resolution, sensitivity, and reliability. Compressed Sensing (CS) refers to the method used to reduce the number of samples collected in an IoT WSN (Kyriazis et al., 2013) Thus it is possible to create stand-alone applications that require fewer resources.

BACKGROUND

The following scenario paints a picture of what the Internet of Things is trying to achieve and how it aims to achieve this.

Scenario: *You wake up in the morning and your alarm clock goes off at the right time because it is hooked up to your calendar, which knows that you have a conference to attend that day, it then searches and figures which plane you need to get, therefore knowing what time to wake you up. In your house the heating would have been on for an hour in order to heat the water for you. You get in your car and an audio announcement lets you know that the road to the airport has been closed due to a burst water pipe which has been caused by a blockage in the water supply; your car then identifies another root to take to the airport ensuring that you get there on time.*

In this scenario all this has been taken care of for you on your behalf by sensors or systems linking to each other acting smart because they know about each other. For example your phone was able to communicate or transmit data across a network to a system in your home activating your heating; Sensors in the water supply system were alerted to a blockage which then transmitted this information across a network to the traffic control system; the traffic control system then transmit this data or information across a network to a system in your car along with an alternative route for you to take, making sure you avoid any delays and get to the airport on time.

At present there are systems or sensors in place that can tell when there is a blockage in the water supply, knows if certain roads are blocked and can control the heating in your house all of which transmits data accordingly. But the fact is these systems are isolated systems on their own. Connecting these isolated systems together and creating what is referred to as a system of systems, which allows for all this information to be shared among all relevant systems is one of the major problems facing the Internet of Things in becoming a smarter more intelligent web. Another problem facing the Internet of Things is that if every object e.g. car's, house's, water supplies, clothes, factory's and so on are to be connected to the Internet then surely they will all need to have their own uniquely identifiable IP (Internet Protocol) address, that is a hell of a lot of IP addresses. Currently the Internet works on the network layer standard of IPv4 which is slowly but surely running out of available IP addresses and it is not expected to be able to cater for all the extra IP addresses that will be generated by the Internet of Things.

The Internet Protocol (IP) and IPv6

The Internet Protocol (IP) specifies the format of packets, also called *datagrams,* and the addressing scheme. Most networks combine IP with a higher-level protocol called *Transmission Control Protocol (TCP)*, which establishes a virtual connection between a destination and a source. Today's Internet works on the network layer standard of IPv4. IPv4 is a 32-bit address protocol that was developed in the 70's. IPv4 was thought to offer enough addresses for the future, but with the increased number of Internet user's and the lower cost of "always on" broadband, now with the Internet of Things becoming a reality addresses are beginning to run out. To extend the number of addresses for network devices, a new protocol was required (Dinakaran & Balasubramanie, 2012).

In 1994 the Internet Engineering Task Force (IETF) decided to adopt the new protocol of IPv6. IPv6 is not a new and improved version of IPv4 but rather a totally

new set of Protocols (Sinclair, 2014). Internet Protocol version 6 also known as IPv6, is the latest generation protocol for Internet networking. Like IPv4 this protocol operates at the network layer of the OSI model. It offers better security, addressing and a host of other features to support large global networks compared to its predecessor IPv4. IPv4 provides 2 to the power of 32 address spaces, or just fewer than 4.3 billion addresses, whereas IPv6 offers 2 to the power of 128 addresses, which gives 3.4 X 10^{38}. IPv6 addresses are backward compatible with IPv4 (Ren et al., 2006). The IPv6 protocol has been designed with scalability and extensibility in mind. This will allow many different type's of devices other than PCs, to more easily join the Internet in the future, e.g. Mobile phone's, PDA's, monitoring or censoring devices found in houses, water supplies, clothes, car's and factories. The way IPv6 assigns addresses allows for easier allocation of addresses to mobile devices. It also helps as it allows these devices to move around and keep their IP address, which means applications don't need to shut down and restart to get a new address when they switch between different networks. The main disadvantage of IPv6 implementation for the Internet of Things is going to be the cost involved of transferring from IPv4 to IPv6 (Li et al., 2013).

While IPv6 has been around for quite a few years, older I.T. and security workers may need to be educated further on its implementation and how it operates. Both software and equipment may need to be upgraded in order for the smooth transition to IPv6. IPv6 can be deployed in a number of different ways either; IPv6 only network, Duel Stack or Tunnelling. Below is a brief description of each. As the name suggests only operates on the IPv6 protocol, this means the network can only communicate with other IPv6 networks or duel stack networks. This means it can't communicate with an IPv4 network without a translation mechanism. Upgrading all nodes on the network at once would be an immense task; therefore it is unlikely that IPv6 only networks will operate independently without IPv4, for some time to come (Modares et al., 2014).

In a dual-stack configuration each network node is able to receive and forward packets using both IPv4 and IPv6. With dual stack IPv6 devices and services can be tried and tested without disrupting the IPv4 network. This still requires that all nodes are upgraded to operate both IPv4 and IPv6, which would also be a very large task for any network (Zagar et al., 2007).

FUTURE RESEARCH DIRECTIONS

There is an increased exposure to remote hacks but the IoT opens up many privacy implications. The sheer scale of deployment of these limited-function embedded devices in households and public areas can lead to unique attacks. There is also the worry of the domino effect where if one device becomes 'owned' - it can easily spread to the remainder of the cluster. The privacy issues arise due to the data collection mechanisms which may lead to user profiling and identification of individuals in unforeseen use case scenarios. The utmost care needs to be taken when deploying IoT devices with regards their lifecycle, data collection mechanisms and overall security protocols. Manufacturers do seem to be increasingly considering the correct forms of cryptographic algorithms and modes needed in particular for IoT devices. There is an international ISO/IEC 29192 standard which was devised to implement lightweight cryptography on constrained devices. There was a need for this as many IoT devices have a limited memory size, limited battery life along with restricted processors. Traditional 'heavy' cryptography is difficult to deploy on a typical sensor hence the deployment of many insecure IoT devices. Sony is one manufacturer who have created a novel block cipher called CLEFIA which supports up to 128 bit keys. Other embedded device stream ciphers include Salsa20/12 and Trivium. The research however is still early days. There is a real need for manufacturers to monitor their networks 24-7, looking for potential intrusions and unusual activity on the network. One such example is Detica who has some very sophisticated tools that can identify network intrusions (González García et al., 2014).

Tunnelling is the most likely approach to implementing IPv6 for the Internet of Things, as it requires only the edge nodes of a network to be IPv6 enabled. It works by encapsulating the IPv6 packet as a payload within an IPv4 packet. This provides a more cost effective way of upgrading to IPv6 as only the edge nodes need to be compatible, then as time goes on IPv6 machines and applications can be purchased, as and when they are required. Even though work began on IPv6 over 15 years ago, there were very few networks of any size running the protocol up until the last few years. Only Mobile telecommunication providers had begun using IPv6 to allocate addresses to mobile phones, as IPv4 would never be able to assign addresses to the millions of mobile phones that are sold each year. Most

organizations that have enough address spaces aren't willing to implement it, because of the costs involved. Up until 2003 there were no major corporations or organizations committing to the IPv6 cause. Then in the summer of 2003 the American Department of Defence announced that it would only purchase IPv6 compliant technologies with the goal of being fully IPv6 compliant (Su et al., 2014).

Today Asia is leading the way in IPv6 implementation. China, Japan, South Korea and Taiwan are the major players in the research and the development of IPv6 networks. China has already started to build large multi-level network platforms, which use IPv6 to connect to each other. It is known as China Next Generation Internet (CNGI). The network was launched in 2006, with operating speeds of 2.5 to 10 gigabytes per second on the network (Fleshbourne, 2004). The Internet of Thing is expected to revolutionize the consumer market as the Internet grows to become the number one economic tool that customers will depend on. It is predicted that customers will depend completely on a network made up of services and that business will depend solely on the future Internet to provide these services. It is expected that electronic devices will be at the heart of the future Internet thus making the Internet of Things the very core of the future Internet, with the Internet of Thing there will be a lot of systems or sensors found in cars, machines and products which will be monitored and connected directly through services to business systems and business operations in order to provide higher visibility which will inturn lead to improvements in business operations in such things as manufacturing and production i.e. farming (Ondemir and Gupta, 2014). Sensors found in such things as products will transmit data in real time on inventory levels, how long it takes the product once it leaves the factory to when it appears on the shelves of shops thus identifying bottle necks or delays in the supply chin all of which can lead to more efficient business process. Sensors found in medical devices such as pace makers will transmit data back to the hospital on the condition of the patient thus identifying problems before it is too late. These sensors could also transmit data back to the manufactures on the performance of the device, helping them make improved and more efficient devices in the future. Sensors in the ground could transmit data back to farmers on the soil conditions, thus helping farmers know when the best time to plant or harvest their crops are, this will maximize how farmers make use of their land.

CONCLUSION

Although we have seen the Internet evolve from web 1.0 to the Internet of Things, the future Internet is going to be as much about the ownership of information as web 1.0 was, with organizations trying to control or own the information that will be generated by all these sensors and devices found in the Internet of Things. While the benefits of the Internet of Things are clear to see in how they can improve business process by providing higher visibility and making the web more efficient, I can't help but wonder will it get to a stage in society that people will no longer have the skills or ability to organise themselves or others. Will we as a society just expect devices or systems to arrange and organize everything on our behalf and to just point us in the right direction? By allowing this are we ourselves becoming objects much the same as what cars, clothes and factories are in this linked up system of systems that is the Internet of Things. Maybe this is the price society pays for advances in technology, it's not that long ago that people where predicting that texting on mobile phones would be the end of the English language as proper grammar and spelling would be lost on the new generation. I don't believe this to be the case, this is evolution much the same as going into a shop and buying meat out of a freezer, the need or necessity has been replaced with a easier or much more convenient option, that is not to say that you can't go out and catch your own animals and butcher them if you want.

IPv6 offers a great deal of improvement compared to IPv4. The new protocol not only offers more addresses for use in the Internet of Things, it also has a host of new improved features which will not only improve the functionality and reliability of the network, but it also gives increased security (in the form of encryption). IPv6 does offer lower run-time costs, lower maintenance and management costs, better connectivity, faster speeds and increased mobility. However, major organizations and businesses are showing a reluctance to change to the new protocol not only because of the costs involved, but because of new security concerns which could come about from the implementation of a new protocol. With the Internet of Things now

becoming a reality, organizations that do not make the switch to IPv6 will be left behind as IPv6 is as much the future of the Internet as the Internet of Things is.

On the security/privacy aspect, the public should be concerned as there is evidence to date that many IoT roll-outs have neglected the end-to-end security aspect. We know that a core reason for this is that many of the embedded devices do not simply have enough computing power to implement all the relevant security layers and functionality necessary. There is then the actual heterogeneity of devices and the lack of industry or defacto standards for connecting the IoT. Invasion of privacy is one real concern. The IoT will lead to an increased collection of information on individuals. In for instance, collecting information relating to an individual, that individual may become more easily identifiable. There is a real possibility that an individual's habits, location, interests and other personal information may be easily tracked. There are sophisticated data mining software in use which can reveal uncanny accurate information on previously 'anonymous' data. This also leads to concerns relating to identity thief. When it comes to privacy, there may be of course fairly low risk exposure of data such as the IoT tracking our food purchases etc but we must also be aware that it could expose more damaging details such as religion. We may also see a mission creep, namely in the repurposing of data concerning individuals. A lot of these deployments will be commercial and data collected may be sold onwards to third parties in ways not even initially thought of. There is still no agreed protocol for access to public data when it comes to law enforcement authorities or other intelligence agencies. There is also a real possibility that unscrupulous individuals can commit a crime by manipulating the data captured by the meter. There is a possibility that a hacker could compromise a smart meter to find out about a home owners' peaks of use to learn when they are likely to be out. On a larger scale however, there is a threat whereby smart meters which are connected to smart grids could be attacked leading to complete failure of the system. In fact, it is an ideal attack from rogue nations or terrorist organisation as once the electricity if cut -off then pretty much every aspect of life in that region is affected.

ACKNOWLEDGMENT

The authors would like to acknowledge the contribution of Paul Mc Keever in the creation of this work.

REFERENCES

Ben Saied, Y., Olivereau, A., Zeghlache, D., & Laurent, M. (2014). Lightweight collaborative key establishment scheme for the Internet of Things. *Computer Networks*, *64*(8), 273–295. doi:10.1016/j.comnet.2014.02.001

Dinakaran, M., & Balasubramanie, P. (2012). Network mobility (NEMO) security: Threats and solutions. *Journal of Theoretical and Applied Information Technology*, *35*(1), 77–82.

Fleshbourne, D. (2004). IPv6 rollout in 2005 for China and Japan - Neowin.net. IPv6 rollout in 2005 for China and Japan - Neowin.net. Retrieved from http://www.neowin.net/news/main/04/03/18/ipv6-rollout-in-2005-for-china-and-japan.

Gómez, J., Huete, J., Hoyos, O., Perez, L., & Grigori, D. (2013). Interaction System based on Internet of Things as Support for Education. *Procedia Computer Science*, *21*, 132–139. doi:10.1016/j.procs.2013.09.019

González-García, C., Pelayo G-Bustelo, B. C., Pascual Espada, J., & Guillermo C. F. (2014). Midgar: Generation of heterogeneous objects interconnecting applications. A Domain Specific Language proposal for Internet of Things scenarios. *Computer Networks*, *64*(8), 143–158. doi:10.1016/j.comnet.2014.02.010

Kalfoglou, Y. (2012). Web 1.0, Web 2.0, Web 3.0. Retrieved from http://www.kalfoglou.info/web123_.htm.

Kyriazis, D., & Varvarigou, T. (2013). Smart, Autonomous and Reliable Internet of Things. *Procedia Computer Science*, *21*, 442–448. doi:10.1016/j.procs.2013.09.059

Li, G. S., Jiang, Q., & Ma, C. G. (2013). Improvements on a mobile IP registration protocol featured with user anonymity. *Advanced Materials Research*, *765-767*, 1027–1030. doi:10.4028/www.scientific.net/AMR.765-767.1027

Modares, H., Moravejosharieh, A., Lloret, J., & Salleh, R. (2014). A survey of secure protocols in Mobile IPv6. *Journal of Network and Computer Applications*, *39*(1), 351–368. doi:10.1016/j.jnca.2013.07.013

Montavont, J., Roth, D., & Noël, T. (2014). Mobile IPv6 in Internet of Things: Analysis, experimentations and optimizations. *Ad Hoc Networks*, *14*, 15–25. doi:10.1016/j.adhoc.2013.11.001

Ondemir, O., & Gupta, S. (2014). Quality management in product recovery using the Internet of Things: An optimization approach. *Computers in Industry*, *65*(3), 491–504. doi:10.1016/j.compind.2013.11.006

Ren, K., Lou, W., Zeng, K., Bao, F., Zhou, J., & Deng, R. (2006). Routing optimization security in mobile IPv6. *Computer Networks*, *50*(13), 2401–2419. doi:10.1016/j.comnet.2005.09.019

Sinclair, B. (2014). Finally, IPv6's killer app: The Internet of Things, zdnet, Retrieved on March 25, 2014, from http://www.zdnet.com/finally-ipv6s-killer-app-the-Internet-of-things-7000027644

Su, J., Cao, D., Zhao, B., Wang, X., & You, I. (2014). ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of Things. *Future Generation Computer Systems*, *33*, 11–18. doi:10.1016/j.future.2013.10.016

Žagar, D., Grgić, K., & Rimac-Drlje, S. (2007). Security aspects in IPv6 networks – implementation and testing. *Computers & Electrical Engineering*, *33*(5–6), 425–437. doi:10.1016/j.compeleceng.2007.05.008

ADDITIONAL READING

Chabanne, H., Urien, P., & Susini, J. F. (2011). *RFID and the Internet of Things*. London: ISTE.

Chaouchi, H. (2010). *The Internet of Things*. London: Wiley-ISTE.

Gubbi, J. Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems. The Netherlands: Elsevier.

Hersent, O., Boswarthick, D., & Elloumi, O. (2012). *The Internet of Things: Key Applications and Protocols*. Chichester, West Sussex: Wiley.

Michahelles, F. (2012, October 24-26). In Proceedings of 2012 International Conference on the Internet of Things (IOT). Piscataway, NJ: IEEE.

NIC. (2013). *Disruptive Technologies Global Trends 2025. U. S. National Intelligence Council*. NIC.

Pfister, C. (2011). *Getting Started with the Internet of Things*. Sebastapool, CA: O'Reilly Media, Inc.

Uckelmann, D., Harrison, M., & Michahelles, D. (2011). *Architecting the Internet of Things*. Berlin: Springer. doi:10.1007/978-3-642-19157-2

Weber, R., & Weber, R. (2010). *Internet of Things: Legal Perspectives*. Berlin: Springer. doi:10.1007/978-3-642-11710-7

Zhou, H. (2013). *The Internet of Things in the Cloud: A Middleware Perspective*. Boca Raton: CRC Press, Taylor & Francis Group.

KEY TERMS AND DEFINITIONS

Cloud Computing: Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources.

Cloud Service Providers: Cloud Service Providers offer an opportunity for organisations to make resources available online. These resources can range from extensive customer relationship management (CRM) software to the relatively widespread online email access.

Internet Protocol version 4 (IPv4): Is the fourth version in the development of the Internet Protocol (IP) Internet, and routes most traffic on the Internet. However, a successor protocol, IPv6, has been defined and is in various stages of production deployment.

Internet Protocol version 6 (IPv6): Is the latest version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the

Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.

Protocol: An agreed-upon set of rules that facilitates the exchange information between two computers or devices. A protocol includes formatting rules that specify how data is packaged into messages. It also may include conventions like message acknowledgement or data compression to support reliable and/or high-performance network communication.

Quality of Service: This is a measure of network performance that reflects the network's transmission quality and service availability. QoS can come in the form of traffic policy in which the transmission rates are limited which guarantees a certain amount of bandwidth will be available to applications.

Router: A device or setup that finds the best route between any two networks, even if there are several networks to traverse. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create WANs.

Universal Resource Identifier (URI): The string (often starting with http) comprises a name or address that can be used to refer to a resource. It is a fundamental component of the World Wide Web.

Wide Area Network (WAN): A network connecting computers within very large areas, such as states, countries, and the world.

Web Service: A Web Service is a software component that is described via WSDL and is capable of being accessed via standard network protocols such as but not limited to SOAP over HTTP. It has an interface described in a machine-processable format.

Web 2.0: The transition of websites from isolated information silos to sources of content and functionality, thus becoming a computer platform serving web applications to end users. Also a social phenomenon referring to an approach to creating and distributing Web content itself, characterized by open communication, decentralization of authority, freedom to share and re-use and "the market as a conversation.