Survey on Security in Internet of things: state of the art and challenges

Mangal Sain, Young Jin Kang, Hoon Jae Lee

Department of Computer Engineering, Dongseo University, Busan, South Korea

mangalsain1@gmail.com, rkddudwls55@gmail.com, hjlee@dongseo.ac.kr

***Abstract*— The Internet of Things (IoT) refers to the physical devices that are embedded with Internet, electronics, software, sensors, actuators, and network connectivity. This includes many different systems, for instance, healthcare, wellbeing, smart home, building, smart meters, and so on. The Internet-based technical architecture, IP-based communication protocols, and technologies are facilitating the exchange of smart object services over the insecure channels, therefore, security and privacy of the involved stakeholder is the prime concern. In this paper we analyse available IoT security in three forms: (i) security in communication, (ii) security at application interface, and (iii) data security. This paper reviews the current IoT technologies, approaches and models and finds the security gap in existing communication technologies, application interfaces, and data security. Another focus of the paper is to provide an overview of the related work in IoT, together with the open challenges and future research directions me".**

***Keywords*— Internet of Things, Wireless sensor Networks, Security, Privacy, Trust**

I. INTRODUCTION

Internet of things (IoT) is the internetworking of the physical objects – embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. The IoT incorporates everything from a miniscule to big machines, appliances to building, body sensors to cloud computing which comprises major types of networks, for instance, distributed, grid, ubiquitous, and vehicular networks. Internet of Things (IoT) is a dynamic system connected devices through wireless or wired with self-configuring capabilities based on standard and interoperable communication where physical and virtual objects have identities, physical attributes and virtual personalities and they use intelligent interface and seamlessly integrated into the information network. The IoT incorporates everything from the body sensor to the recent cloud computing which comprises major types of networks, such as distributed, grid, ubiquitous, and vehicular.

Few years ago, the emergence of the IoT was considered with the certain degree of scepticism. A series of announcements, from the acquisition of Nest labs by google for 3.2 billon to Samsung Gear and Health-related wearables to the development of Smart Home Features into Apple's iOS, have made IoT and increasingly tangible business opportunity. Till day approx 1% of things around us is connected such Refrigerator, car washing machine, heater, air-condition, garage door, should connect but still not connected. Cisco estimated that IoT has a potential value of $14 trillion over 10 years [1].

In 2014 IoT ranked top in Gartner hype cycle for emerging technologies. With different available technologies, IoT developments may select different communication methodologies and architectures. As a shown in Table no 1, IoT systems can be developed with specific target and technology. For short range communication may select RFID, Bluetooth, ZigBee or WiFi. For industrial automation devices may prefer ZigBee and for long range communication WiMAX or Cellular technology could be the choice. Traditional security measures cannot be used directly since the smart objects are resource hungry in the terms of computation, memory and bandwidth.

IoT devices are collecting data from individuals and sharing with third parties such as voice recognition or figure print while playing video game or accessing different devices. Attacker can use these kinds of data which can pose a privacy problem for those who are unaware of the presence of the devices and have no meaningful influence over how that collected information is used [2]. IoT is still new technology which still needs to develop application standard, communication protocol as well as secure centralized data service which can be used worldwide. IoT user still using traditional security measures which are not cost effective and consumes lots of memory and time [3]. With number of increasing connected devices to the Internet, many new protocols have been developed at all layer of ISO such CoAP, RPL and IPv6 which is one of the most suitable for IoT to connect billions of device to IPv4 internet [5].

The contribution of this paper is compare in table 4 with respect to different surveys which we did in this paper as well as after comparing many ongoing projects related with security on IoT; which summaries all the latest threat to IoT. We also discussed by securing device, securing application interface and by secure data transfer an IoT can still achieve basic security requirements.

The rest of the paper is organized into four different sections as follows: Section II describes the wireless communication technologies Section III discusses how we can achieve security in Iot. In this regards we also discuss some of available research solutions. In section IV we discuss how available technology is still not enough to achieve full security in IoT. Finally, section V concludes the paper and gives us an outlook of future work.

II. WIRELESS COMMUNICATION TECHNOLOGIES

Wireless communication technologies are the backbone of IoT systems which enables connectivity between different machines as well as with different application. Communication protocol allows devices to exchange data on network and interaction with different machine. In the following Table 1, we analyse few available communication technologies as follows.

TABLE 1. WIRELESS COMMUNICATION TECHNOLOGIES

	NFC	**RFID**	**Blutooth**	**Wi-fi**	**ZigBee**	**WIRELESS HART**	**6LoWPAN**	**WiMAX**	**2.5-3.5G**
Network	PAN	PAN	PAN	LAN	LAN	LAN	LAN	MAN	WAN
Topology	P2P	P2P	Star	Star	Mesh, star, tree	Mesh, star	Mesh, Star	Mesh	Mesh
Power	Very low	Very low	Low	Low-high	Very low	Very low	Very low	High	High
Speed	400kbs	400kbs	700kbs	10-100mbs	250 kbs	250kbs	250kbs	10-110 mbs	1.8-7.2 mbs
Range	<10cm	<3m	<30 m	4-20m	10-300m	200m	800 m	50km	Cellular network
Application	Pay, get access, easy setup	Item tracking	Network for data, exchange headset	Internet, multimedia	Sensor networks, industrial automation	Industrial sensing networks	Sensor network building	Meter area broadband internet connectivity	Cellular phones and telemetry
Cost adder	low	Low	Low	Medium	Medium	Medium	Medium	High	High

NFC: Near Field communication (NFC) is a short-range, high-frequency (13.56MHz) RFID technology that allows user to exchange data and information between two NFC enabled devices. In future NFC can be one of the most used communication technology due some following reason. NFC provides easy network access and data sharing, without much lengthy process of handshaking. NFC can be configured with user intent and provide much better accessibility to device. It also provides data security at multiple level which really one of the crucial point for IoT. NFC have one of the biggest disadvantage is distance.

Texas instruments recently announce that they also working on NFC sensor transponder for Industrial, medical, wearable and many other IoT applications [5].

RFID : Radio Frequency Identification, is a technology where information stored on a microchip can be read remotely, without physical contact using energy. In RF there are several frequency ranges used including Low Frequency (LF, 125 kHz), High Frequency (HF, 13.56 MHz), Ultra High Frequency (UHF, 433 MHz, 860-960 MHz) and Microwave (2.45 GHz, 5.8 GHz). These bands, in general, do not require a license if the transmitted power is limited. Some bands can be used globally (HF) while others are specific to certain regions (UHF in US, EU, and Japan) [6].

Bluetooth: Bluetooth is based on the IEEE 802.15.1 standard. It is a low power, low cost wireless communication technology suitable for data transmission between mobile devices over a short range (8–10 m). The Bluetooth standard defines a personal area network (PAN) communication. It operates in 2.4 GHz band. The data rate in various versions of the Bluetooth ranges from 1 Mb/s to 24 Mb/s. The ultra low power, low cost version of this standard is named as Bluetooth Low Energy (BLE or Bluetooth Smart). Earlier, in 2010 BLE was merged with Bluetooth standard v4.0.

Wi-Fi: IEEE 802.11 is a collection of Wireless Local Area Network (WLAN) communication standards. For example, 802.11a operates in the 5 GHz band, 802.11b and 802.11 g operate in the 2.4 GHz band, 802.11n operates in the 2.4/5 GHz bands, 802.11ac operates in the 5 GHz band and 802.11ad operates in the 60 GHz band. These standards provide data rates from 1 Mb/s to 6.75 Gb/s. WiFi provides communication range in the order of 20 m (indoor) to 100 m (outdoor).

ZigBee: The ZigBee Alliance has developed a very low-cost, very low-power consumption, an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create PAN with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth two-way, wireless communications standard. The ZigBee network layer (NWK) supports star, tree, and mesh topologies [7]. Its low power consumption limits transmission distances to 10–100 meters line-of-sight, a defined rate of 250 Kbit/s, which is best suited for intermittent data transmissions from a sensor or input device.

WirelessHART: WirelessHART is a wireless sensor networking technology based on the Highway Addressable Remote Transducer Protocol (HART). Developed as a multi-vendor, interoperable wireless standard, WirelessHART was defined for the requirements of process field device networks. The protocol supports operation in the 2.4 GHz ISM band using IEEE 802.15.4 standard radios. Backward compatibility with the HART “user layer” allows transparent adaptation of HART compatible control systems and configuration tools to integrate new wireless networks and their devices, as well as continued use of proven configuration and system-integration work practices. It on the estimated 25 million HART field devices installed, and approximately 3 million new wired

HART devices shipping each year. In September 2008, Emerson became the first process automation supplier to begin production shipments for its WirelessHART enabled products [8].

6LowPAN: The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks. IPv4 and IPv6 are the work horses for data delivery for local-area networks, metropolitan area networks, and wide-area networks such as the Internet. Likewise, IEEE 802.15.4 devices provide sensing communication-ability in the wireless domain. The inherent natures of the two networks though, are different. IEEE 802.15.4 nodes can operate in either secure mode or non-secure mode. Two security modes are defined in the specification in order to achieve different security objectives: Access Control List (ACL) and secure mode [9].

WiMAX: IEEE 802.16 is a collection of wireless broadband standards. WiMAX (Worldwide Interoperability for Microwave Access) standards provide data rates from 1.5 Mb/s to 1 Gb/s. The recent update (802.16 m) provides data rate of 100 Mb/s for mobile stations and 1 Gb/s for fixed stations [10].

Mobile communication: There are different generations of mobile communication standards including second generation (2G including GSM and CDMA), third generation (3G-including UMTS ad CDMA2000) and fourth generation (4G-including LTE). IoT devices based on these standards can communicate over cellular networks. Data rates for these standards range from 9.6 Kb/s (2G) to 100 Mb/s (4G) and are available from the 3GPP websites.

III. How to secure Internet of Things

Even most of traditional systems are not fully secure and it's always a concern for system how to secure them adequately. A technology which still in rely on traditional framework for development and still there is not specific standard is much more susceptible to security threat. With the expansion of the IoT market, protecting the company's data and IP is more important than ever. To make sure any IoT device is secure every developer need to follow following services [11, 12 and 13].

Authentication: The forthcoming challenge for IoT is to authenticate IoT user's authentication. With the new standard and self configuring protocol authentication becoming more complex compare to traditional approach. With the help of two factor authentication for example google's two step notification its little bit easy to control your application specially with help of mobile which stays with everyone all the time. The features that make the smart phone a powerful authentication factor are the same that will enable our watches, wristbands and thermostats to have an opinion on our identity and an ability to assert that opinion [14].

Confidentiality: In IoT message can be easily intercepted by third parties with the help of latest technology. For example if some a user accessing his homecare application from public Wi-Fi at restaurant and accessing some live video of home for third party it will be easy to access same content with same network. Therefore it's really important to have confidentiality and message need to be hidden from intermediate entities. End-to-End (E2E) message secrecy is required in the IoT. Also, the stored data such as message and personal data on IoT device should be hidden from unauthorized entities.

***Data Integrity*:** Interestingly most of research in IoT focused on privacy which is also an important ingredient of secure IoT. In any application, Integrity is much more important component compare to other such as availability because privacy may lead to some embarrassment but integrity especially if its medical device or car's breaking system can easily cost someone's life. From many years public key infrastructure (PKI) and Keyless Signature Infrastructure (KSI) are both used for data security and have complementary roles. PKI is best used for authentication and for secure communication on network. KSI can be used for integrity proof [15].

Access Control: In traditional system, access controls are only targeted to a closed system where all users are known to the system. In IoT, it should consider open and closed system where unknown party play an important role. [16, 17 and 18] are pretty good example of access control in IoT. UCON [16] have three decision factors (authorizations, obligation and conditions) and two decision properties (mutability and continuity).

A) Communication Security

Communication in the IoT should be protected by providing the security services discussed in previous section. By using standardized security mechanisms we can provide communication security at different layers. Table 2 shows an IoT stack with standardized security solution at different layers.

TABLE 2. STACK WITH SDANDARDIZED SECURITY SOLUTION

IoT Layer	IoT Protocol	Security Protocol
Application	CoAP	User-defined
Transport	UDP	DTLS
Network	IPv6, RPL	IPsec, RPL security
6LoWPAN	6LoWPAN	None
Data-link	IEEE 802.15.4	802.15.4 security

Link Layer: IEEE 802.15.4 Security: link layer. 802.15.4 link-layer security is the current state- of-the-art security solution for the IoT. The link layer security protects a communication on a per-hop base where every node in the communication path has to be trusted [19]. A single pre-shared key is used to protect all communication. In normal case if an attacker compromised one device and access to one key it means whole network will be compromised but in this

link layer as its per-hop security only one hop/device will be compromised and it can be detected at initial state. Still link-layer security is limited but it's quite flexible which operate with multiple protocols on different layers.

6LoWPAN networks: IPv6 used on sensor node to simplify the connecting task and it's quite successful especially in all LoWPAN devices [20-23]. IPv6 can be used in IoT as it also supports development for commissioning, managing, configuring and debugging networks [20]. The IETF (Internet Engineering Task Force) created the 6LoWPAN working group to define the support of IPv6 over IEEE 802.15.4 LoWPAN networks which is defined by an additional adaptation layer introduced between data link and network layers, as specified in Fig.1.

There are three different kinds of LoWPAN architectures types were defined, a) Ad-hoc LoWPAN, with no infrastructure b) LoWPAN, with one edge router and c) LoWPAN with multiple edge routers. Fig.2 illustrate security framework for 6lowPAN; which aim at bootstrapping security associations between a newly authenticated device and those want to connect to the same domain, without letting intermediary foreign entities gain any knowledge of the exchanged key material.

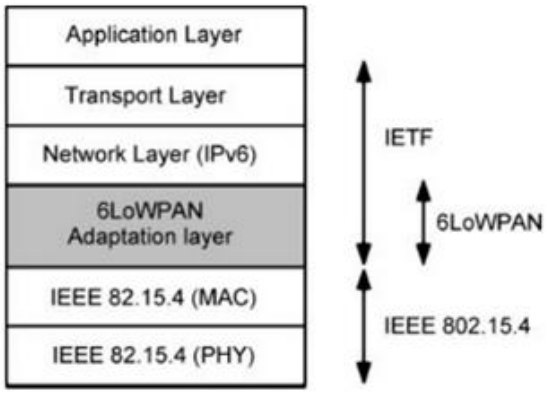

Figure 1. 6LowPAN adaptation layer [21]

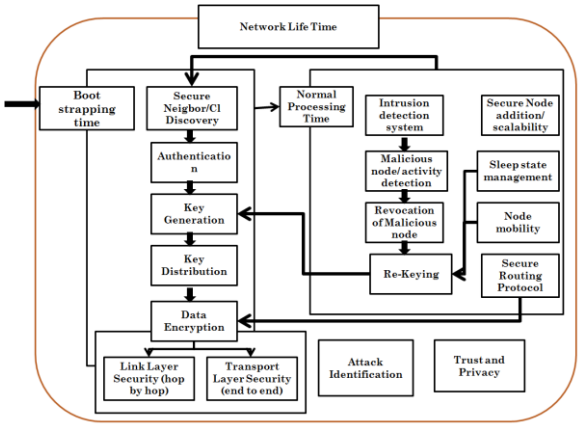

Figure 2. Security framework for 6LowPAN

As illustrate in Fig.2 initially, the joining device discovers the identities of its neighbors; it then undergoes an authentication procedure; generation of key and distribution

Network Layer: IP Security: As IoT basically implemented on internet, it use network IP Security (IPsec) provided by Network layer. IPsec provides end to end security with authentication as well as confidentiality and integrity. By operating at the network layer, IPsec can be used with any transport layer protocol including TCP, UDP, HTTP, and CoAP [24]. IPsec ensures the confidentiality and integrity of the IP payload using the Encapsulated Security Payload (ESP) protocol [25], and integrity of the IP header plus payload using the Authentication Header (AH) protocol [26]. Now in IPsec is mandatory in all IPv6 protocol means all IPv6 ready devices by default have IPsec support [27].

1905.1 Abstraction Layer: With the increase of home care solution, every device is connected with Internet made wired and wireless home networking a hot topic. To address a wide variety of application, regions, environments and topologies, multiple connectivity technologies should be used. A typical home network is shown in Fig 3. As with any network deployment, many problems need to be addressed for the network.

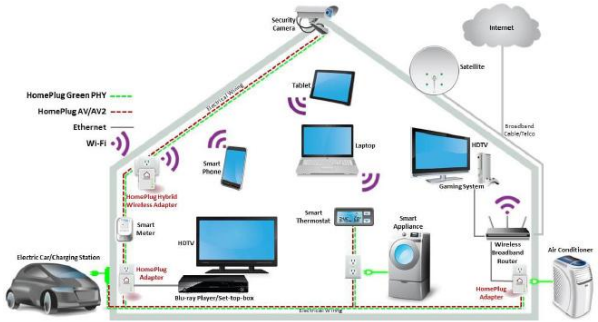

Figure 3. Hybrid home network

The design of IEEE 1905.1 is flexible and scalable to accommodate future home networking technologies. The 1905.1 Abstraction Layer (AL) supports interface selection for the transmission of packets arriving from any interface or application. The 1905.1 layer does not require modification of the underlying home networking technologies and hence does not change the behaviour or implementation of existing home networking technologies. An abstraction layer is used to exchange Control Message Data Unit (CMDU) among 1905.1 compliant devices

B) Data Security

Securing communication is really important in IoT but most of application developer forgets about securing data which is generated from all IoT devices. Most of devices in IoT are small and doesn't have enough constraint due to limited size to secure them from security threats related with hardware. There are several solutions exists but due to different communication technology only one solution may not be enough to secure everything.

There are number of article proposed secure storage solution [28, 29, 30, 31]. Codo [28] is a security extension for the Coffee [32] file system in the Contiki OS [33].

In [34] I. E. Bagci proposed a secure storage and communication framework which is based on IPv6/6LoWPAN protocols. IPv6/6LoWPAN defines IPsec/ESP (Encapsulating Security Payload) that provides encryption and authentication of transmitted data packets. The author uses cryptographic methods and data formats which is defined by ESP for data processing before storage. In this architecture they also need to store header information along with data which also need cryptographic processing. This encrypted data must be stored in ESP compatible over network which they achieve by using IPsec as a base for communication and storage, and the existing key exchange mechanisms defined for IPsec can be reused for the storage element of the framework.

IV. DISCUSSION

There are many companies who are working towards security standards and providing better interface where user can get secure communication, secure access to device and secure data transfer and storage. For manufacturers, vendor and industry IoT technology need a specific standard which be considered as priority. In Table 3 we summarize some of available IoT security project which targeting IoT enabled technology.

In [35] author proposed solutions provide E2E security for web based application exploiting DTLS. In IoT most of the hardware has limited capability and DTLS handshake is still acceptable solution. For a secure communication author used IPsec which is mandated by IPv6.

TABLE 3. AVAILABLE IoT SECURITY PROJECTS

	35	**36**	**37**	**38**	**39**	**40**	**41**	**42**
Authentication	Yes	No	Yes	No	Yes	yes	Yes	Yes
Privacy	Yes	Yes	Yes	Yes	Yes	yes	Yes	Yes
Access Control	Yes	Yes	Yes	Yes	Yes	yes	Yes	Yes
API security	Yes	Yes	NO	Yes	No	No	No	No
Data Security	No	Yes	Yes	Yes	Yes	Yes	No	Yes
Mobility	No	Yes	Yes	Yes	No	No	No	No
Middleware	No	No	No	No	Yes	Yes	No	No

In [38], author developing a secure and smart application for pervasive information systems. Their basic target is smart health, smart city, smart shopping etc which directly related with IoT. Their main target is to develop distributed profile which can be integrated with user profile along with secure data and privacy.

iCore project [39] target is to address two key issues: In context of IoT, first is how to abstract the technological heterogeneity that derives from the vast amount of heterogeneous objects. Another is to consider the views of different users/stakeholders for ensuring proper application provision, business integrity and therefore, maximize exploitation opportunities.

Japan-Eu ICT Corporation working together on the future internet, whose basic target is to find common global standard to secure communication, secure information and energy efficient standard [41].

To handle security challenge in IoT, security needs to be design in device. With device security, the risk of data theft and unauthorized access can be reduced. Especially for the medical device if data is stolen it can lead to some serious consequences. Manufacture should build inbuilt security features in device. Moreover the device security should be updated time to time. Building security in device alone will not provide full security in IoT but it definitely reduce the risk. In IoT, security needs to be address throughout its cycle. Secure booting, proper access control, secure authentication and secure application interface need to develop to make sure whole process is secure in IoT.

As we discussed in previous section that Internet was only designed for communication and not for millions of devices to connect together. In future the number IoT device will be increase and its all depend on how to manage device security on every stage. Therefore it is paramount to find specific standard and mechanism to get security in the IoT.

V. CONCLUSIONS

With the emergence of the IoT it requires customized security and privacy on each level. IoT involves different communication technologies which still require a common communication standard. By developing secure middleware researcher can integrate IoT and communication technology. The main goal of this paper is to provide a better understanding of security approaches in IoT as well as current technologies and models, in order to discover what challenges need to be met to make secure communication in IoT.

ACKNOWLEDGMENT

This research was financially supported by the Ministry of Trade, Industry and Energy(MOTIE) of the Republic of Korea and Korea Institute for Advancement of Technology(KIAT) through the Regional Specialized Industry Development Program(Grant Number : R0005598).

This work is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (Grant number: NRF-2011-0023076).

REFERENCES

[1] J. Bradley, “The Internet of Everything: Creating Better Experiences in Unimaginable Ways,” Nov 21, 2013, http://blogs.cisco.com/ioe/the-internet-of-everything-creating-better-experiences-in-unimaginable-ways/#more-131793

[2] Wilton, Robin. CREDS 2014 - Position Paper: Four Ethical Issues in Online Trust. Issue brief no. CREDS-PP-2.0. Internet Society, 2014

[3] Karen Rose, Scott Eldridge, Lyman Chapin “Understanding the Issues and Challenges of a More Connected World" in WWW.INTERNETSOCIETY.ORG, October 2015.

[4] Gont, F., "Security Assessment of the Internet Protocol version 6 (IPv6)", UK Centre for the Protection of National Infrastructure.

[5] https://connectedworld.com/nfc-transponder-for-enabling-iot/

[6] Shain Armstrong " RFID Basics: How RFID Tags Work" last accessed from http://blog.atlasrfidstore.com/rfid-tag-basics on november 24, 2011
[7] *"ZigBee: Brief Introduction". Noor Ul Mushtaq. Retrieved 2016-11-05.*
[8] Wireless Devices in Process Manufacturing last accessed from http://www.arcweb.com/market-studies/pages/wireless-devices-for-process-industries.aspx
[9] Park, S.; Kim, K.; Haddad, W.; Chakrabarti, S.; Laganier, J. (March 2011). IPv6 over Low Power WPAN Security Analysis. IETF. I-D draft-daniel-6lowpan-security-analysis-05. Retrieved 10 May 2016.
[10] P.P. Ray" A survey on Internet of Things architectures", Journal of King Saud University - Computer and Information Sciences, 8 October 2016
[11] Hong Yu, Jingsha He, Ting Zhang, Peng Xiao, and Yuqiang Zhang. Enabling end-to-end secure communication between wireless sensor networks and the internet. World Wide Web, pages 1–26, 2012.
[12] Oscar Garcia-Morchon, Sye Loong Keoh, Sandeep Kumar, Pedro Moreno-Sanchez, Francisco Vidal-Meca, and Jan Henrik Ziegeldorf. Securing the ip-based internet of things with hip and dtls. In Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, pages 119–124. ACM, 2013.
[13] Javier L´opez and Jianying Zhou. Wireless Sensor Network Security. IOS Press, 2008.
[14] Richard E Smith. Authentication: from passwords to public keys. Addison-Wesley Longman Publishing Co., Inc., 2001.
[15] http://www.mtsi-us.com/blog/part-hardening-pki-ksi/
[16] J. Park, R. Sandhu, Towards usage control models: Beyond traditional access control, in: SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies, ACM, New York, NY, USA, 2002, pp. 57-64.
[17] J. Park, Usage control: A uni¯ed framework for next generation access control, Ph.D. thesis, George Mason University, Fairfax, VA, USA.
[18] X. Zhang, Formal model and analysis of usage control, Ph.D. thesis, George Mason University, Fairfax, VA, USA (2006).
[19] A. Cui and S. J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan," in Proceedings of the 26th Annual Computer Security Applications Conference. ACM, 2010,pp. 97–106. Austin, TX.
[20] Naveen Sastry and David Wagner. Security considerations for ieee 802.15. 4 networks. In Proceedings of the 3rd ACM workshop on Wireless security, pages 32–42. ACM, 2004.
[21] Mulligan G. The 6LoWPAN architecture. Proceedings of the 4th Workshop on Embedded Networked Sensors (EmNets'07). ACM: New York, 2007; 78–82.
[22] Hui J, Culler D. IP is dead, Long live IP for wireless sensor networks. Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys). ACM: New York, 2008; 15–28.
[23] Durvy M, Abeillé J, Wetterwald P, O'Flynn C, Leverett B, Gnoske E, Vidales M, Mulligan G, Tsiftes N, Finne N, Dunkels A. Making sensor networks IPv6 ready. Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems. ACM: New York, 2008; 421–422.
[24] S. Kent and R. Atkinson. Security architecture for the internet protocol, 1998. http://www.ietf.org/rfc/rfc2401.txt.
[25] S. Kent. IP Authentication Header. RFC 4302, 2005. http://tools.ietf.org/html/rfc4302.
[26] S. Kent. IP Encapsulating Security Payload. RFC 4303, 2005. http://tools.ietf.org/html/rfc4303.
[27] R. Atkinson. Security Architecture for the Internet Protocol. RFC 1825 (Proposed Standard), August 1995. Obsoleted by RFC 2401.
[28] I. E. Bagci, M. R. Pourmirza, S. Raza, U. Roedig, and T. Voigt, "Codo: Confidential data storage for wireless sensor networks," in 8th IEEE International Workshop on Wireless and Sensor Networks Security (WSNS 2012), October 2012.
[29] N. Bhatnagar and E. L. Miller, "Designing a secure reliable file system for sensor networks," in Proceedings of the 2007 ACM workshop on Storage security and survivability, 2007, pp. 19–24.
[30] J. Girao, D.Westhoff, E. Mykletun, and T. Araki, "Tinypeds: Tiny persistent encrypted data storage in asynchronous wireless sensor networks," Ad Hoc Netw., vol. 5, pp. 1073–1089, September 2007.
[31] W. Ren, Y. Ren, and H. Zhang, "Hybrids: A scheme for secure distributed data storage in wsns," in Proceedings of the 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing - Volume 02, 2008, pp. 318–323.
[32] N. Tsiftes, A. Dunkels, H. Zhitao, and T. Voigt, "Enabling large-scale storage in sensor networks with the coffee file system," in Proceedings of the 2009 International Conference on Information Processing in Sensor Networks. IEEE Computer Society, 2009, pp. 349–360.
[33] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors," in Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, 2004, pp. 455–462.
[34] I. E. Bagci, S. Raza, T. Chung, U. Roedig and T. Voigt, "Combined secure storage and communication for the Internet of Things," *2013 IEEE International Conference on Sensing, Communications and Networking (SECON)*, New Orleans, LA, 2013, pp. 523-531.
[35] R. Weber, Accountability in the Internet of things, Comput. Law Secur. Rev. 27(2011) 133–138.
[36] Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, Utz Roedig. Securing Communication in 6LoWPAN with Compressed IPsec. In Proceedings 7th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS '11), June 27-29 2011, Barcelona, Spain.
[37] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, M. Spirito, Demo: An ids Framework for Internet of Things Empowered by 6lowpan, Berlin, Germany, 2013, pp. 1337–1339.
[38] BUTLER Project. <http://www.iot-butler.eu>.
[39] iCORE Project. <http://www.iot-icore.eu>.
[40] National Science Foundation Project. http://www.nsf.gov
[41] EU-Japan Project. <http://www.eurojapan-ict.org/>.
[42] FIRE EU-Korea Project. <http://eukorea-fire.eu/>.

Mangal Sain received the M.Sc. degree in computer application from India in 2003 and the Ph.D. degree in computer science in 2011. Since 2012, he has been an Assistant Professor with the Department of Computer Engineering, Dongseo University, South Korea. His research interest includes wireless sensor network, cloud computing, Internet of Things, embedded systems, and middleware. He has authored over 30 international publications including journals and international conferences.

Young Jin Kang
2013: BS at Dongseo University, Republic of Korea
2015: MS at Dongseo University, Republic of Korea
2015 ~ current: doctor´s course Dongseo University, Republic of Korea

Research Interests: Wireless Sensor Networks, Cryptography and Network Security, Side Channel Analysis

Hoon-Jae Lee received his BS, MS, and PhD. degrees in Electrical Engineering from Kyungpook National University, Daegu, South Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information and Communication Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His current research interests include developing secure communication system, side-channel attack, and ubiquitous sensor network/radio frequency identification security.