Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2015 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2015

An analysis of secure MANET routing features to maintain confidentiality and integrity in IoT routing

David Airehrour
Auckland University of Technology, dairehrour@aut.ac.nz

Jairo Gutierrez
Auckland University of Technology, jairo.gutierrez@aut.ac.nz

R33. An analysis of secure MANET routing features to maintain confidentiality and integrity in IoT routing

David Airehrour
Auckland University of Technology
dairehrour@aut.ac.nz

Jairo Gutierrez
Auckland University of Technology
jairo.gutierrez@aut.ac.nz

Abstract

The Internet of Things (IoT) is fast becoming a global phenomenon and many issues are arising such as standardization, deployment of IPv6, sensors' energy requirements and security among others. However, without a secure network routing system IoT nodes will be exposed to malicious activities on the network, data compromises, privacy invasion and even acts of terrorism could be perpetrated via the teeming billions of IoT nodes. Various MANETs secure routing protocols have been proposed by researchers which could be utilized in the development of secure routing protocols for the Internet of things, thus the study of these secure MANET routing protocols will give a direction for the development and incorporation of secure routing in the Internet of Things. This paper surveys secure routing protocols in MANETs while proposing some secure MANET routing features for enshrining confidentiality and integrity in IoT routing. This paper also discusses research trends and future directions in the area of security of IoT networks.

Keywords: MANET, WSN, IoT, M2M, H2M, H2H, RFID, RPL, LLN, 6LoWPAN, 6TiSCH.

1. Introduction

With the advancement in mobile computing and wireless communications, a new paradigm known as the Internet of Things (IoT) is swiftly generating a lot of research interest and significant industrial and commercial applications. The Internet of Things (IoT) refers to the pervasive interconnectivity of various devices communicating and exchanging data with one another. These devices have built-in sensing and communication interfaces such as sensors, radio frequency identification devices (RFID), Global Positioning System (GPS), infrared sensors, laser scanners, actuators, wireless LANs and even Local Area Networks (LANs) interfaces (Zhao & Ge, 2013). These "things" can be connected to the internet and hence could be controlled and managed remotely. These devices could interact among themselves: i.e. Machine to Machine (M2M) communications by way of sending and receiving data, sensing temperature, pressure etc. while transmitting that data to other devices for further processing or corresponding actions (Xu, Ding, Zhao, Hu, & Fu, 2013). Various researchers have indicated that WSN and RFID are the main driving forces for IoT and the popularization of WSN will see the growth of IoT as there will be a proliferation of M2M devices across the globe (Xu et al., 2013). Cisco and Ericsson estimated that by 2020 there will be 50 billion devices communicating with one another (CISCO, 2013; Ericsson, 2011; Evans, 2011). The driving aim of IoT is to connect machine to machine (M2M), human to human (H2H), human to machine (H2M) while

providing ease of communication, identification, management and control among the devices (Zhao & Ge, 2013). There are numerous opportunities and benefits of IoT to mankind and these include: wildlife monitoring, environmental monitoring (pollution, water reservoir observation), e-health systems and monitoring, smart grids etc.(Park, Crespi, Park, & Kim). In essence, IoT will bring about a wide range of smart services and applications beneficial to individuals and organisations in achieving great comfort and ease in their everyday lives through the connection of machine-to-machine (M2M), human-to-machine (H2M) and human-to-human (H2H) in diverse ways, at any place and at any time (International Telecommunication Union, November, 2005; Park et al.). However, The Internet of Things currently is not without a number of interesting research challenges including: the unique identification of objects on the network, the representation and storage of exchanged messages and issues around communication protocols and security (Giusto, 2010; Gubbi, Buyya, Marusic, & Palaniswami, 2013; Xu et al., 2013). Security in IoT is quite different from Internet security and in particular routing security, for the latter is far more complicated due to the need to provide safety for the routing information and information payload that will traverse heterogeneous networks made up of billions of devices in a wireless form. It is therefore, necessary that concentrated research work for each aspect of security problems be effectively embarked upon in ensuring a stable IoT (Giusto, 2010; Zhao & Ge, 2013). In securing the routing traffic of IoT, secure MANET routing features is an area worthy of study in designing secure routing protocols for the Internet of Things (IoT).

Mobile Ad hoc NETwork (MANET) is a collection of mobile devices (called nodes) that communicate with each other without the use of infrastructure such as access points or base stations. These networks are self-configuring, capable of self-directed operations and are easily deployable; hence they are referred to as Self-Organising Networks (SONs). Nodes cooperate to provide connectivity and operate without centralized administration (Ilyas, 2003).

This paper takes a look at the need for exploiting secure MANET routing properties such as confidentiality and integrity in IoT routing. The contribution of this paper is threefold. Firstly, we introduce the subject of Internet of Things, what it is and its future trends. Secondly, the paper introduces Mobile Ad hoc Network (MANET), secure routing protocols and features that have been developed by various researchers. Thirdly, the paper argues for the need for secure routing for the Internet of Things.

2. Security and the Internet of Things

The security of information has always been an issue for mankind(Namuduri, Wan, & Gomathisankaran, July 29, 2013). How can we effectively protect information so that it does not get into the wrong hands? In the early days steganography was employed (Islam & Shaikh, 2013) in hiding important information. Today, with the introduction of computers and networks, security has taken a new dimension and its importance cannot be overemphasized. The Internet of Things promises to be both evolutionary and disruptive; however, the fundamental requirements ensuring the security of the Internet of Things (which is also a representation of any ad hoc network) remains a challenge as the important features or properties required of any good ad hoc network must consist of the following: availability, authenticity, non-repudiation, confidentiality and integrity (Mishra, 2008). This paper focuses on confidentiality and integrity in maintaining safe routes within the IoT network.

i. *Confidentiality:* Confidentiality guarantees information does not get divulged to the wrong source. In ad hoc networks, it ensures malicious nodes do not gain unauthorized access to vital routing or data information either from any legitimate node or while such information is in transit.

ii. *Integrity:* This is the assurance that data received by a destination node has not been changed in transit either through collision or via a deliberate tampering by an untrusted node while in transit and the data received was as originally sent.

3. IoT architecture

The idea on the evolution of IoT started at the Massachusetts Institute of Technology (MIT) from a work at the Auto-id center in 1999. This group was conducting research in networked radio identification (RFID) and emerging sensing Technologies (Wikipedia: The free encyclopedia, November, 2014). By 2003, 500 million devices were connected online while the population was estimated to be 6.3 billion (Evans, 2011). However, with the rapid proliferation of smart phones and tablets over the years there where about 12.5 billion devices connected online as of 2010 while the population of the world stood at 6.8 billion (Evans, 2011). The ratio of devices per person was almost one person to two devices in 2010. Today, with the increase in technological innovation and the continuous growth of smart phones, phablets and tablets the ratio is certain to be larger. In a research conducted in China (Zhang, Zhang, Yang, Cheng, & Zhou, January 14, 2009), the authors showed that the internet doubles its size every 5.32 years. With this result it is obvious that the number of devices that will be online and communicating with themselves (M2M) will be quite large and hence the need to have secure communication among the devices. Today, IoT has become a hot topic and thriving research area both in academia and industry as these technologies are set to revolutionize the way we do many things. The hierarchical model for IoT as proposed by (Miao, Ting-Jie, Fei-Yang, Jing, & Hui-Ying, 2010) is widely accepted. This model proposes a three-tier layer structure defined by its functions consisting of a perception layer, network layer and application layer. This is further explained below:

i. Perception Layer

The perception layer is the sense organ of IoT. It aims at recognizing objects and gathering information. This layer includes RFID tags, 2-D barcode labels and readers, terminals, GPS, camera, sensors and sensor network.

ii. The network layer

This layer represents the nucleus of IoT. It processes and transmits information received from the perception layer to the application layer. The network layer comprises of the following: information center, intelligent processing center, Internet network systems and network management center.

iii. The Application Layer

This layer is a fusion of IoT's socio-business requirements in order to realize the in-depth capabilities of the technology. This layer represents the confluence of IoT and industrial technology with a mix of industrial needs and machine intelligence. However, the IoT is still in its infancy and many researchers still consider it a "cloud-castle" as it is still in its formative stage and does not yet have a definite form (Miao et al., 2010). (Miao et al., 2010) advised that

for a proper understanding of IoT, the two system structure of IoT namely; *the Internet and communications network* should be analyzed in order to gain better understanding of IoT and hence create a better architecture for the Internet of Things.

3.1 Secure Routing in MANETs and IoT

Designing secure and efficient routing protocols for MANETS is a primary challenge but, extremely useful in maintaining network route information and security. A lot of secure routing protocols for MANETs use multi-hop rather than single-hop routing to deliver packets to their destination. Many designs adopted for secure routing have been through the use of cryptography techniques in which the security of mobile nodes is assured by the hop-by-hop authentication among the nodes and all intermediate nodes are required to cryptographically confirm the digital signatures attached to the routing information (Djenouri, Khelladi, & Badache, 2005). In other designs, a trust metric system is utilized (Djenouri et al., 2005). Nonetheless, in all systems for secure routing, the underlying idea is to integrate more information into the routing messages, routing table data exchanges, and other security related operations which are introduced in these protocols thereby securing and enhancing how the routing information and packets are sent over the wireless channel though at a little performance cost. However, if a secure routing protocol experiences excessive overheads that make it inefficient this makes such a protocol practically useless. Table 1 gives a summary of some notable secure routing protocols that have been proposed and implemented, their secure properties (defence mechanism) and the techniques adopted.

4.0 IoT routing protocols and security

i. 6LoWPAN

6LoWPAN is an IETF-standardized IPv6 adaptation layer (data link layer) which enables IP connectivity over low power and lossy networks (Bhalaji, 2009; Internet Engineering Task Force (IETF), December, 2014). This is seen as the foundation for the network build up for the Internet of Things such as smart homes, smart cities and industrial control systems (Kantzavelou, Tzikopoulos, & Katsikas, May 29 - 31 2013). A large number of applications utilize 6LoWPAN for IP-based communication through an upper layer protocol such as the RPL routing protocol. 6LoWPAN essentially adjusts IPv6 packets into frames of 127 bytes – a frame size requirement that low power sensor devices can utilize among themselves. Also, 6LoWPAN supports the transmission of large-sized IPv6 packets on the data link layer of the IEEE 802.15.4. 6LoWPAN also provides fragmentation support at the adaptation layer. Although the system of fragmentation makes processes such as buffering, forwarding and processing of fragmented packets resource expensive on these already resource constrained devices. Rogue nodes can send duplicate, overlapping or stale fragments to disrupt the network (Hummen et al., April 17-19, 2013).

Protocols	Technique	Base Routing Protocol	Attacks Addressed	Brief Description
SEAD	Authentication and Hashing	DSDV	Various forms of DoS attacks and routing loops	It uses efficient one-way hash functions to authenticate the lower bound of the distance metric and sequence number in the routing table.
ARIADNE	MAC, Hashing	DSR	Worm hole attacks, Modification and Fabrication attacks	Using a hash chain and MAC list, verifies the integrity of the messages using roué request
SRP	Encryption	ZRP	Modification, Replay and Fabrication attacks	Establish security association using public key and then encrypt the communication using public key
SQoS	Symmetric Cryptography	Reactive routing protocol	Limit DoS attack and route overhead	This protocol utilizes symmetric cryptography which incorporates hash chains and MW-chains. The authors claimed that the combination of these two cryptographic techniques provide efficient mechanism for storing and generating values of hash chains as well as providing instant authentication and low storage overhead during routing of network traffic.
TAODV	Trust metric system and lightweight cryptography	AODV	Defense from Misbehaving nodes	Route selection is based on quantitative Route Trust and Node Trust values. Hence, a packet differential of zero indicates a perfect route and trusted link while trustworthiness decreases for growing route trust values.
ARAN	Sign the request Packet	None	Modification, Fabrication and Impersonation	Digitally signs the routing messages using private key that are verified by next node using certificates
Black hole Attack in Mobile Ad Hoc	Sequence Number Inconsistencies, Multiple Routing Paths	AODV	Black hole attack	Identifies anomalies by checking if the sequence number of subsequent sent and received messages are larger than previous values and it constructs the safest path based on multiple path information from the received multiple route replies (Al-Shurman & Yoo, 2004)
Black hole Attack on AODV-based Mobile Ad Hoc Networks	Dynamic Learning	AODV	Black Hole attack	An attack model is devised by analyzing the distribution of sequence number difference in normal and anomalous case (Kurosawa, Nakayama, Kato, Jamalipour, & Nemoto, 2007).

Table 1: Summary of secure routing protocols for MANET as adapted from (Islam & Shaikh, 2013)

ii. Routing Protocol for Low-power and lossy Networks (RPL)

The IETF working group discovered that routing functionalities in 6LoWPAN were very challenging due to the resource constrained nature of the nodes. The working group (ROLL WG) therefore proposed the RPL routing protocol which could cover a wide band of different link layers of low-power nodes and could be used in collaboration with other host routing devices with very limited resources. RPL operates at the network layer making it capable to quickly build up routes and distribute route information among other nodes in an efficient manner. In creating its routing table, nodes in the network are linked via multi-hop paths to other smaller units of root devices which normally collect data and coordinate activities around them. For each of these root nodes a Destination Oriented Directed Acyclic Graph (DODAG) is formed by accounting for the cost of links, the attribute of nodes and status information with an objective function for planning the optimization needs of the target setting (Evans, 2011; Yashiro, Kobayashi, Koshizuka, & Sakamura).

iii. Constrained Application Protocol (CoAP)

CoAP is an application layer or software protocol developed by the "Constrained RESTful Environments" (CoRE) working group of IETF. The protocol was developed for use in very simple electronics devices which have low bandwidth and are resource-constrained. The protocol allows these devices to communicate interactively over the Internet (RESTful interactions). Devices such as low power sensors, switches, valves etc. were the target of this application layer protocol. CoAP embodies two sub-layers: a messaging layer and a request/response layer. The messaging sub-layer is responsible for duplicate detection and reliability for packet delivery in UDP (Evans, 2011; Yashiro et al.).

5. A three-tier secure routing Internet of Things architecture

It has been projected that by 2020 there will be 50 billion devices connected together. One obvious aspect highlighted is the fact that most of the interconnectedness of the 50 billion devices will be between machines (M2M) and not human-to-machine (H2M). This however, brings a challenge in the assurance of what the machines will be processing when unsupervised or without a good security system implemented. Some security challenges include:

i. *Hackers on the prowl*: hacktivists will find the IoT as a fertile ground to perpetrate their nefarious activities as they will have an abundant of devices they could hack into if a good secure network system is not implemented.
ii. *Terrorism*: With massive amount of IoT devices deployed all over the world. There is no doubt that terrorists could and would seek to explore how they can use this new technology for their attacks.
iii. *Privacy invasion*: Again with the deployment of these devices and no adequate security system implemented this could lead to privacy invasion of individuals, corporate bodies and governments.
iv. *Public confidence*: Sequel to the issue of privacy invasion, public acceptance of the IoT will dwindle as people will feel their data could be compromised once they go online or that hackers/individuals could easily have access to their sensitive data.
v. *Security and network exposure*: According to Symantec, a software security firm, in 2012 alone security breaches were estimated at US $115 billion. Today it is estimated that there are 2.4 billion nodes online and extrapolating the figure we get $50 per node in security breaches. Extrapolating this result to 50 billion devices that will be online by 2020, results in a whooping US $2.5 trillion in security breaches. This is clearly not sustainable.

Our analysis indicates that configuring a secure routing system in the network layer of IoT becomes necessary in order to implement and have a secure IoT architecture especially during network routing. We hereby propose in figure 1 a three-tier architecture for a secure routing in IoT.

6. Secure routing in IoT: research challenges

The Internet of Things (IoT) is swiftly unfolding with an increasing number of devices getting linked up to the internet each day. We see various heterogeneous devices getting networked together and communicating with one another. An example is in a household where PCs, game consoles, tablets, mobile devices, TVs and even refrigerators are getting connected to the internet (Ungurean, Gaitan, & Gaitan, 2014). While this is good news for investors and manufacturers this however, opens up a new range of challenges in IoT, namely: data and network security of

IoT. Current research findings show that IT security threats for 2013 and 2014 are threats that subsist only with the presence of a network and they include: botnets, malware, Denial-of-Service (DoS) attack on financial services and Distributed Denial of Service (DDoS) attack, web-based malware, android malware and Spam (Mc Afee Labs, 2014; Sophos Limited, 2013, 2014). The IoT topology which is mostly an M2M communication network has the capacity to be hijacked by intruders and used to maliciously infiltrate a network and perpetrate a range of attacks. A fundamental research challenge is the lack of a standard and secure framework for the communication of these heterogeneous devices across platforms. Network security threats will pose a great challenge to public acceptability of the IoT if they are not addressed as quickly as possible. The threat situation is very fluid and the entire IoT topology is open to attacks if not given the necessary attention. Accordingly, we do not advocate the adoption of any secure routing protocols of MANET into IoT sensor nodes but an adaptive or improved version that will suit IoT nodes without impacting negatively on them.

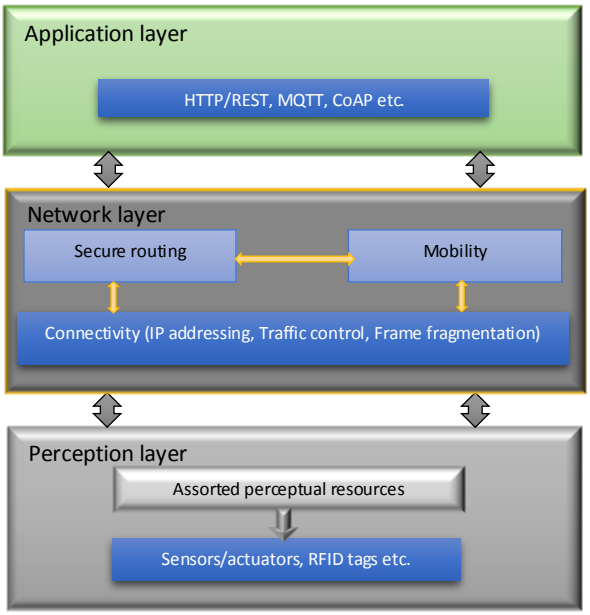

Figure 1: A three-tier secure routing Internet of Things architectural layer

7. Conclusions

We are close to having billions of devices online and talking to each other in a fashion that is not known to humans. This is a whole new paradigm and its implications are yet to be fully understood. This new technological landscape brings both benefits and attendant problems. It will be a good practice to pre-empt some of the attendant problems by putting in place measures to address them. One of such issues is secure routing in IoT. It will be good adopting a secure routing approach to secure network traffic from being compromised by malicious nodes on the

network. The effect of such compromises could even cause public apathy towards a full acceptance of the Internet of Things. As noted in (Evans, 2011) efforts to promote and secure the IoT will have to come from businesses, governments, standards organizations, and the research community while working together as a team in making IoT a success and the "next big thing" after the Internet.

References

Al-Shurman, M., & Yoo, S.-M. (2004). Black Hole Attack in Mobile Ad Hoc Networks Symposium conducted at the meeting of the Annual Southeast Regional Conference

Bhalaji, N. (2009). Reliable Routing against Selective Packet Drop Attack in DSR based MANET. *Journal of Software, 4*(6).

CISCO. (2013). *The Internet of Everything (IoE): Connections Counter*. Retrieved December 2, 2014, 2014, from http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342

Djenouri, D., Khelladi, L., & Badache, A. N. (2005). A survey of security issues in mobile ad hoc and sensor networks. *Communications Surveys & Tutorials, IEEE, 7*(4), 2-28. doi:10.1109/COMST.2005.1593277

Ericsson. (2011). More than 50 billion connected devices: Driving forces. Retrieved from http://www.akos-rs.si/files/Telekomunikacije/Digitalna_agenda/Internetni_protokol_Ipv6/More-than-50-billion-connected-devices.pdf

Evans, D. (2011). The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Retrieved from http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Giusto, D. (2010). *The Internet of things: 20th Tyrrhenian workshop on digital communications*. New York: Springer.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660. doi:http://dx.doi.org/10.1016/j.future.2013.01.010

Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H., & Wehrle, K. (April 17-19, 2013). 6LoWPAN Fragmentation Attacks and Mitigation Mechanisms*Association of Computing Machiner (ACM).* Symposium conducted at the meeting of the WiSec 2013, Budapest, Hungary.

Ilyas, M. (2003). *The handbook of ad hoc wireless networks*. Boca Raton: CRC Press.

International Telecommunication Union. (November, 2005). *ITU Internet Reports: The Internet of Things*. Retrieved from http://www.itu.int/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf

Internet Engineering Task Force (IETF). (December, 2014). IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch). Retrieved from https://datatracker.ietf.org/wg/6tisch/charter/

Islam, N., & Shaikh, Z. A. (2013). Security Issues in Mobile Ad Hoc Network In S. Khan & A.-S. K. Pathan (Eds.), *Wireless Networks and Security: Issues, Challenges and Research Trends* (pp. 49-56). Heidelberg, Germany: Springer-Verlag Berlin Heidelberg. doi:10.1007/978-3-642-36169-2

Kantzavelou, I., Tzikopoulos, P. F., & Katsikas, S. K. (May 29 - 31 2013). Detecting Intrusive Activities from Insiders in a Wireless Sensor Network using Game Theory Symposium

conducted at the meeting of the Association of Computing Machinery (ACM) PETRA 2013, Island of Rhodes, Greece. doi:http://dx.doi.org/10.1145/2504335.2504350

Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. *International Journal of Network Security, 5*(3).

Mc Afee Labs. (2014). 2013 Threats Predictions. Retrieved from http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf

Miao, W., Ting-Jie, L., Fei-Yang, L., Jing, S., & Hui-Ying, D. (2010, 2010). Research on the architecture of Internet of Things*IEEE.* doi:10.1109/ICACTE.2010.5579493

Mishra, A. (2008). *Security and Quality Of Service In Ad Hoc*
Wireless Networks. Cambridge, UK: Cambridge University Press.

Namuduri, K., Wan, Y., & Gomathisankaran, M. (July 29, 2013). Mobile Ad Hoc Networks in the Sky: State of the Art,Opportunities, and Challenges Symposium conducted at the meeting of the Association of Computing Machinery (ACM), ANC 2013, Bangalore, India.

Park, S., Crespi, N., Park, H., & Kim, S.-H. (2014). IoT routing architecture with autonomous systems of things*IEEE.* doi:10.1109/WF-IoT.2014.6803207

Sophos Limited. (2013). Security Threat Report 2013. *1.13*. Retrieved from https://www.sophos.com/de-de/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf

Sophos Limited. (2014). Security Threat Report 2014. 2-22. Retrieved from http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf

Ungurean, I., Gaitan, N.-C., & Gaitan, V. G. (2014, 2014). An IoT Architecture for Things from Industrial Environment*IEEE.* doi:10.1109/ICComm.2014.6866713

Wikipedia: The free encyclopedia. (November, 2014). Radio-frequency identification *Radio-frequency identification*: Wikipedia.

Xu, G., Ding, Y., Zhao, J., Hu, L., & Fu, X. (2013). Research on the Internet of Things (IoT). *Sensors & Transducers, 160*(12), 463.

Yashiro, T., Kobayashi, S., Koshizuka, N., & Sakamura, K. (2013). An Internet of Things (IoT) architecture for embedded appliances*IEEE.* doi:10.1109/R10-HTC.2013.6669062

Zhang, G.-Q., Zhang, G.-Q., Yang, Q.-F., Cheng, S.-Q., & Zhou, T. (January 14, 2009). Internet Growth Follows Moore's Law Too. *PhysOrg*. Retrieved from http://phys.org/news151162452.html

Zhao, K., & Ge, L. (2013, 14-15 Dec.). A Survey on the Internet of Things Security Symposium conducted at the meeting of the Computational Intelligence and Security (CIS), 2013 9th International Conference on doi:10.1109/CIS.2013.145