IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Internet of Things (IOT) Standards, Protocols and Security Issues

Ahmed Mohammed Ibrahim Alkuhlani[1], Dr S.B. Thorat[2]

School of Computational Sciences, SRTM University, Maharashtra, Nanded, India[1]

Director of Institute of Technology & Management, Maharashtra, Nanded, India[2]

Abstract: The internet of things (IOT) is the new revolution of internet after PCS and Servers- Clients communication now sensors, smart object, wearable devices, and smart phones are able to communicate. Everything surrounding us can talk to each other. life will be easier and smarter with smart environment, smart homes,smart cities and intelligent transport and healthcare.Billions of devices will be communicating wirelessly is a real huge challenge to our security and privacy.IOT requires efficient and effective security solutions which satisfies IOT requirements, The low power, small memory and limited computational capabilities . This paper addresses various standards, protocols and technologies of IOT and different security attacks which may compromise IOT security and privacy.

Keywords: Internet of Things, Security, IEEE 802.15.4, 6LoWPAN, ROLL, CoAP.

I. INTRODUCTION

Recently, the idea of the Internet as a set of connected PCs is changed to a set of connected things (devices) surrounding us, such as home appliances, machines, electronics, transportation and building automation etc. The actual number ofthings in the living space is greater than the number of world population [1].

According to Cisco, there will be mostly 50 billion devices connected to the internet by 2020, creating $14.4 trillion of value at stake for companies and industries [2,3].IOT will change a number of major technological innovation and industrial development. Nowadays, more governments, enterprises and research institutions put high concentration on it[4].The major IoT emphasesis the formation of smart environments with self-control/ autonomous devices: smart homes, smart cities ,smart transport, smart healthcare, smart living, and so on [5, 6].

With the rapid increase in IoT application use, several security and privacy issues are noticed. When everything will be connected to each other, this issue will only become more risky and noticeable, and constant exposure will literally reveal additional security flaws and weaknesses. Such limitations may subsequently be exploited by hackers, and in a statistical sense all exposed flaws and weaknesses may be abused in an environment with billions of devices [7].Heterogeneity of devices (things) communication media is one of the challenging security risks that IOT will face. The different technologies such as GSM, WI-FI, UTMS, BLE, ZigBee that can be used for IOT devices communication don’t have a common standard that can be utilized for communication. The heterogeneous data structure and protocols also make content protection more complex [8].

We expect the majority of security attacks will occur at the software level because devices are connected to the IP environment, whichcurrently has most popular attacks and can at the same time cover a large number of devices and processes. From a research point of view, most new attacks are on physical signalsand in particular attacks occurs during data processing and decision making steps.

It is important to understand that any security weakness at any level affect directly the overall system security.the rest of the paper is organized as in section II an overview of the IOT enabling technologies and section III we present the IOT Standardizations of IEEE and IETF and in section IV Security requirements For The IOT and in section V conclusion and references

II. IOT ENABLING TECHNOLOGIES

A) Identification technologies:

1) Wireless Sensor Networks (WSN)
Wireless sensor networks (WSN) is built of small devices called sensors, these sensors are used to detect events and collect information from its surrounding environment these information vary depends on its need such as weather, movement, temperature, sound etc.

2) Body Sensor Networks (BSN’s)
Body sensor networks (BSN's) is wireless body network to monitor a livingbody, the sensors used in BSN are linked wirelessly in a network fashion the BSN devices can be wearable devices or implanted internally or externally in fixed position in the person's body, for example wearable devices can be a watch that monitor different activities when a person exercising, implanted devices inside the body collect information about person's health such as pulse rate, blood pressure, diabetic patients use a device to control insulin ratio in their blood . BSN devices are promising technology in healthcare area [10,11,13]

3) Radio-Frequency Identification (RFID)
RFID is an identification technology used to auto-identify objects, it’s considered as one of the most important pervasive computing technologyit doesn’t require manual intervention. RFID is based onidentifying

DOI 10.17148/IJARCCE.2015.411109

objectsremotely andretrieving data from these objects using devices called RFID tags. RFID uses the radio waves to read and gather the information using RFID readers this data is stored on a tag attached to an object .The tag memory stores the product's electronic product code (EPC) and other variable information that contains description of the product so that it can be read and traced by RFID readers anywhere. [2, 6, 12, 13].

APPLICATION (CoAP)
NETWORK (RPL)
ADAPTION OF 6LoWPAN
MAC LAYER (IEEE 802.15.4) LoWPAN
PHYSICAL LAYER (IEEE 802.15.4)

Figure [1]: Communication Protocols in IOT

B) Networks and communication technologies:
wired and Wireless technologies (e.g., GSM, UMTS, Wi-Fi, Bluetooth, ZigBee) gives the chance of billions of devices and services to be connected [14–15]. Scalable and secured architectures designed for IoT network communication are required for secure and reliable wireless communication networks based on wireless identifiable devices and services [16].

C) Software and hardware technologies:
Research on Nano electronics devices focuses on minimizing, and increased functionality - decreasing cost in the design of wireless identifiable systems [12]. Smart devices with advanced inter-device communication will lead to smart systems with high degrees of intelligence and autonomy, enabling fast deployment of IoT application and developing new services [17].

III. IOT STANDARAZATIONS

IEEE 802.15.4 is a low power radio frequency made for constrained devices .IEEE first announced IEEE 802.15.4-2011 [20]. Later, IEEE 802.15.4e-2012 [21] new MAC Specifications with time slot channel capabilities was released in 2012 [21]. Internet Engineering Task Force (IETF) has taken the lead of developing standardization for resource constrained devices[19] established working on standardization by creating "IPv6 over Low power Wireless Personal Area Networks (6LOWPAN)" Working Group in 2007. then, IETF established "Routing Over Low Power Lossy Networks (ROLL)" in 2008 RPL the routing protocol was one of its achievements,"Constrained RESTful Environments (CORE)" in 2010, "DTLS In Constrained Environments (DICE)" in 2013 and Authentication and Authorization in Constrained Environment (ACE) working group in 2014.

A. IEEE 802.15.4
is a radio technology standard , which was defined it in 2003 under IEEE 802.15Personal Area Network (PAN) Working Group, it's designed for low-power and low data-rate applications.IOT devices are built on IEEE 802.15.4 standards. This common standard enables IOT technology and widely adapted by companies , many well-known standardization organizations are developing low-power protocol stacks based on IEEE 802.15.4, such as WirelessHART [22] ZigBee and ISA100.11a.IEEE 802.15.4 specifics both physical and MAC layers (lower layers of OSI model) the lower layers interact with the Upper layers using 6LOWPAN standards and internet protocols which make wireless (IOT) internet of thing or in another words wireless embedded internet.
Typical IEEE 802.15.4 maximum data rate of 250 kb/s and a the output power at max1 mW. packet maximum size is 127 bytes. Besides the physical and MAC layer headers, the available space for an upper layer protocol is between 86 and 116 bytes[23].Other amendments were introduced for the standard, namely IEEE 802.15.4a specifying additional PHY layers, IEEE 802.15.4c [24] to support recently opened frequency bands in China and IEEE 802.15.4d with a similar goal for Japan.

B. IETF Protocol stack for IOT
It becomes very important to study how the present approaches to standardization in IOT can be enhanced, and at the same time it gives better opportunities for the research community for understanding to contribute to the IoT field. the IETF has developed a set of protocols and standards to be openly used for accessing applications and services for wireless resource constrained networks refer to figure [2].

1) 6LoWPAN
Some estimations predict IOT smart devices will reach 50 billon device by 2020, so a scalable,stable and secure IP addressing is required for this huge number of devices. to enable wireless communication IPv6 is the only choice whereas a huge pool of ip addressesis required,its considered one of the enabling technologies of IOT. The 6LoWPAN protocol is an adaptation layer for transporting IPv6 packets over IEEE 802.15.4 links.
6LoWPAN is an ELTF standards designed with the purpose of enabling IP connectivity in resource constrained networks, the IPv6 over Low-power WPAN (6LowPAN) Working Group has been created and works on protocol optimization of IPv6 over networks using IEEE 802.15.4 links Specifically, the 6LoWPAN protocol focuses on how to apply IPv6 to the MAC and PHY layers of IEEE 802.15.4.the minimum value of maximum transmission unit (MTU) definite by IPv6 is 1280 bytes (RFC 2460) whereas the maximum frame size supported by IEEE 802.15.4 is only 127 bytes[25], in addition to significant header overheads occupied by layered protocols such as MAC layer header and security header thus IPv6 packets are too large to fit into a single 802.15.4 frame .the 6loWPAN fragment the large packets into smaller packets which can fit into 802.15.4 frames[26] the first fragment carries a header that includes the datagram size (11 bits) and a datagram tag (16 bits). Subsequent fragments carry a header that includes the datagram size, the datagram tag, and the offset (8 bits).at the destination side 6LoWPAN assemble these fragments and deliver the packet. Figure [1] shows the communication stack of IOT

DOI 10.17148/IJARCCE.2015.411109

2) Application Layer Protocol

the constrained application protocol (CoAP) was designed by IETF to meet certain features such as simplicity, low overhead, and multicast support in resource-constrained environments.CoAP was designed in order to extend web technology to certain requirement for small and constrained devices and low power, low bandwidth networks unlike HTTP CoAP is completely asynchronous discovery and multicast requests, CoAP is interesting mix of making the web very efficient and adding features that is important for IOT applications like subscriptions and discovery. What we need to know is that CoAP is not fully replacement for HTTP protocol it has the following features

1. Web transfer protocol for constrained devices (coap://)
2. UDP binding with reliability and multicast support
3. GET, POST, PUT, DELETE methods
4. Built-in discovery
5. Simple,4 bytes header
6. Asynchronous transaction model
7. It has strong built-in DTLS security protocol

3) Network Layer Protocol

The IETF Routing over Lossy andLow-Power Networks (RoLL) working group was established in February 2008. It focuses on routing protocols design and committed to the standardization of the IPv6 routing protocol for lossy and low-power networks (LLNs).

Standards	Purpose	Implementation	Working Group
IEEE 802.15.4	Radio frequency for constrained devices	Developed to enable wireless communication in Low energy devices	IEEE802.15
6LoWPAN	Adaption layer for allowing devices to be IP enabled	Used as an adaption layer on top of IEEE802.15.4 for IPV6 packets fragmentation and Assembly	Developed under IETF 6loWPAN Group works on protocol optimization of IPv6 over networks using IEEE 802.15.4. Specifically
CoAP	Constrained Application Protocol	It is used as HTTP protocol with extra functions for constrained devices	Developed under IETF CoRE working group
RPL	Networking Routing Protocol	Used for routing packets in lossy and low power networks	Developed under IETF ROLL working group for routing over LLNs

FIGURE [2]: Standards and protocols for IOT and its function

The first objectives of the working group were to produce a set of routing requirements to determine whether or not current available IETF routing protocols would meet the requirements specified in the routing requirement documents, the working group quickly converged on the fact that none of the existing routing protocols would satisfy the fairly unique set of routing requirements for LLNs. Thus ROLL was re-chartered to design a new routing protocol called RPL.

RPL is prescribed as a Distance Vector IPv6 routing protocol for LLNs that identifies how to build a Destination Oriented Directed Acyclic Graph(DODAG). the IP smart object networks have unique routing requirements that related to low power consumption, small form factors and communication challenges of low speed, high error rates and unstable radio waves[25]. The design of RPL routing protocol consider these requirements.RPL was designed for LLNs networks the lossyness could be unpredictable event so RPL designed to be robust to controls such issues, furthermore it is self-manage and able to heal itself without requiring manual interference.. in figure [2] shows a summary of standards and protocols and their purpose and implementation

IV. SECURITY REQUIRMENTS FOR IOT

IOT will be widely used in our lives a huge impact on social life and business environments at home, work, and in intelligent transport and healthcare thus in these crucial areas the security risks will be higher. IOT security could be compromised by several types of attacks. These attacks could be on physical level or on software level.IOT devices have different amount of memory and different computation resource capabilities when connected to the internet these devices are susceptible to attacks. A suitable security mechanisms and services should be there to protect these devices from different types of attacks.Attacks against IOT devices could be passive attacks or active attacks.The passive attacks attempts to learn or make use of information from the system but does not affect system resources where as an active attack attempts to alter system resources or affect their operation.

1. Attacks on privacy

Information can be easily gathered through remote access mechanisms our privacy is one of the important goals for IOT security researchers, the IOT devices distributed nature make it tempting for attackers to get some information

Thefollowing are the most common attacks on user privacy [28]:

Eavesdropping and passive monitoring: This is most common and easiest method of attack on data privacy, If messages are not protected by cryptographic mechanisms, an attacker could easily understand the content. especially if the data obtained by the attacker is important and contains personal information

Traffic analysis: the attacker can make ansuccessfulattack on privacy by combining eavesdropping with traffic analysis. The attacker could recover the location, and identity of communicating hosts furthermore the attacker

DOI 10.17148/IJARCCE.2015.411109

could observe the frequency and length of messages being exchanged Through effective traffic analysis, an attacker can identify certain information with special roles and activities on IoT devices and data.[29]

2. Physical attacks

This sort of attack tampers with hardware components. Due to the distributed nature of IoT devices and most devices typically operate in outdoor environments unattended, which are highly susceptible to physical attacks. [30].

3) Denial-of-Service attack (DoS)

The majority of IOT devices have small memory and limited computation resources; they are thus vulnerable to resource and network exhaustion attack. Attackers can send a lot of requests to be processed by specific things so as to deplete their resources.DoS attacks can cause jamming in the communication channel, thus breaking down the communication channel between nodes. Network availability can also be disrupted by flooding the network with a large number of packets, consumption of computational resources like bandwidth, memory, disk space, or processor time

4) Packet Fragmentation Attack

To enable the transmission of large IPv6 packets over constrainedlink layer technologies such as IEEE 802.15.4 [26]the 6LoWPAN provides fragmentation support at the adaptationlayer. IEEE 802.15.4 frame size is 127 byte whereas the IPV6 MTU maximum transmission unit is 1280, so when transmitting large packet through IEEE 802.15.4 constrained link we need to fragment large packet into smaller once to occupy the IEEE 802.15.4 frame size. 6LoWPAN provides fragmentation support at the adaptationlayer. However, the design of the 6LoWPAN fragmentationmechanism renders buffering, forwarding and processingof fragmented packets challenging on resource-constraineddevices. Specifically, malicious or misconfigured nodes maysend duplicate or overlapping fragments [18].

Due to the lack of authentication at the 6LoWPAN layer, recipients are unable to distinguish these undesired fragments from legitimate ones for packet reassembly. Moreover, reassembling nodes have to optimistically store fragments of a packet and depend on a timeout mechanism to discard incomplete packets. This, however, may cause the constrainedmemory of a node to be occupied with incomplete packets due to missing fragments. Thus, lossy links as well as malicious or misconfigured nodes can block the processing of newly received fragmented packets by spuriously occupying buffer resources.[18]

5) Limited Channel Capacity

The channel rate of IEEE 802.15.4 is only 250 kb/s in the 2.4 GHzband, which limits the scalability and application traffic load of the IoT. For example, experiment results show that the CC2420 radio can only support around 100 40-byte packets/s.

V.CONCLUSION

This survey provides a brief overview of IOT standards and protocols The IEEE 802.15.4 and it conjunction with 6LoWPAN to provide internet connection for constrained devices we also provide an overview of some IOT protocol such as the application protocol CoAP and the routing protocol RPL. We have discussed the current IOT security and privacy issues. IOT privacy and security are still hot research area that involves many aspects, like hardware design, the concept of nanotechnology which will increase the functionality of devices simultaneously with reducing the cost and size of the device which will help in developing a robust cryptographic mechanism. Current Internet IOT standards and protocols are still need to be improved these standards still face the obstacle that these devices share some common features such as low energy, limited memory and small computational capabilities.

REFERENCES

[1] Omar Said, MehediMasud, Towards Internet of Things: Survey and Future Vision, International Journal of Computer Networks (IJCN), Volume (5) : Issue (1) : 2013

[2] O. Mazhelis, H. Warma, S. Leminen, P. Ahokangas, P. Pussinen, M. Rajahonka, R. Siuruainen, H. Okkonen, A. Shveykovskiy, and J. Myllykoski, “Internet-of-things market, value networks, and businessmodels : State of the art report,” 2013.[3] O. Vermesan and P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River Publishers, 2013.

[4] XuXiaohui School of computer, Wuhan University,Study on Security Problems and Key Technologies of The Internet of Things, 978-0-7695-5004-6/13 $26.00 © 2013 IEEE DOI 10.1109/ICCIS.2013.114

[5] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

[6] D. Yang, F. Liu, and Y. Liang, “A survey of the internet of things,” ICEBI-10, Advances in Intillegant Systems Research, ISBN, vol. 978, pp. 90–78 677, 2010.

[7] M. Covington and R. Carskadden, “Threat implications of the internet of things,” in Cyber Conflict (CyCon), 2013 5th International Conference on, 2013, pp. 1–12.

[8] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, ShiuhpyngShieh, IEEE Fellow Department of Computer Science National Chiao Tung University Hsinchu, Taiwan,IoT Security: Ongoing Challenges and Research Opportunities,978-1-4799-6833-6/14 $31.00 © 2014 IEEE DOI 10.1109/SOCA.2014.58

[9] TengXu, James B. Wendt, and MiodragPotkonjakComputer Science DepartmentUniversity of California, Los Angeles “Security of IoT Systems:Design Challenges and Opportunities”978-1-4799-6278-5/14/$31.00 ©2014 IEEE

[10] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[11] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelffl´e, “Vision andchallenges for realising the internet of things,” Cluster of EuropeanResearch Projects on the Internet of Things, European Commision, 2010.

[12] A. de Saint-Exupery, “Internet of things, strategic research roadmap,” 2009.

[13]A. M. Riad, “A survey of internet of things,” 2013. [Online]. Available: http://www.researchgate.net/publication/257957332 A Survey of Internet of Things

[14] L. Tan and N. Wang, “Future internet: The internet of things,” in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, vol. 5. IEEE, 2010, pp. V5–376.

[15] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, “Identity authentication and capability based access control (iacac) for the internet of things,” Journal of Cyber Security and Mobility, vol. 1, no. 4, pp. 309–348, 2013.

[16] D. Bandyopadhyay and J. Sen, “Internet of things: Applications and challenges in technology and standardization,” Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.

[17] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhaueret al., “Internet of things strategic research roadmap,” O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, et al., Internet of Things: Global Technological and Societal Trends, pp. 9–52, 2011.

[18] René Hummen, Jens Hiller, Hanno Wirtz, Martin Henze, Hossein Shafagh, Klaus Wehrle Communication and Distributed Systems, RWTH Aachen University, Germany,”6LoWPAN Fragmentation Attacks and Mitigation Mechanisms”

[19] IETF, "The Internet Engineering Task Force", IETF [Online]. Available:http://www.ietf.org

[20] 802.15.4-2011:IEEE Standard for Local and Metropolitan Area Networks- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), Institute of Electrical and Electronics Engineers Std.

[21] 802.15.4e-2012: IEEE Standard for Local and Metropolitan Area Net-works - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC Sublayer, Institute of Electrical and Electronics Engineers Std.

[22] J. Song et al., “Wirelesshart: Applying Wireless Technologyin Real-Time Industrial Process Control,” Proc. IEEE RTAS, 2008, pp. 377–86.

[23] Zhengguo sheng, oranglelabs, Beijing“A Survey on theietf protocolsuite for the Internet of things: standards, challenges, andopportunities”IEEE Wireless Communications • December 2013

[24] IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 15.4:Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendment 2,3

[25] Montenegro G. et al., Transmission of IPv6 Packets over IEEE802.15.4 Networks, RFC 4944, 2007.

[26] Hui J., Thubert P., Compression Format for IPv6 Datagramsover IEEE 802.15.4-based Networks, RFC 6282, 2011.

[27] JP Vasseur, Cisco Fellow, Cisco Systems Navneet Agarwal, Technical Leader, Cisco Systems “The IP routing protocol designed for lowpower and lossy networks Internet Protocol for Smart Objects (IPSO) Alliance”

[28] H. Ning, H. Liu, and L. Yang, “Cyber-entity security in the internet of things,” vol. 46, no. 4, pp. 46–53, 2013.

[29] A. Armando, “Deliverable d2. 1: The high level protocol specification language,” Technical Report IST-2001-39252, http://www. avispaproject. org/delivs/2.1/d2-1. pdf, Tech. Rep., 2003.

[30]S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT), ser. Communications in Computer and Information Science. Springer Berlin Heidelberg, 2010, vol. 89, book section 42, pp. 420–429. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-14478-3 42

DOI 10.17148/IJARCCE.2015.411109