A Survey on IoT Privacy Issues and Mitigation Techniques

BIRJU TANK
GTU PG School
Ahmedabad, INDIA
Email: birjutank27@gmail.com

HARDIK UPADHYAY
GPERI
Mehsana, INDIA
Email: hardik31385@gmail.com

HIREN PATEL
SPCE
Visnagar, India
Email: hbpatel1976@gmail.com

ABSTRACT
Internet of Things (IoT) has emerged as a global network, which intelligently connects different devices or systems which are having self-configuring capabilities. The key idea is to bind or to connect miscellaneous devices or objects via wireless or wired connections along with unique addressing system and make omnipresent environment where an individual can communicate at any time with digital and physical word. It has conspicuous vulnerabilities because of increasing number of omnipresent devices. That is why for conveying data at application layer, resource constrained machines are supposed to exploit Constrained Application Protocol (CoAP) which was standardized by Internet Engineering Task Force (IETF). CoAP has previously accepted as the paradigm protocol for IoT systems. But, privacy of CoAP is yet an open Challenge. As it influences an individual's daily life it is indispensable to allow security services like authentication, confidentiality, authorization etc. This survey presents an overview of CoAP as well as current situation of security and privacy in Internet of Things that is required to be solved and discuss the further work.

Keywords
Internet of Things; CoAP; DTLS; Security; 6LoWPAN

1. INTRODUCTION
Internet of Things is playing a vital role in this modern world of technology that every smart objects are getting connected to the internet. From the smart homes and healthcare to wearables, the IoT connects almost all the facets of individual's life. Different entities can communicate and interact to provide different services. This smart nature of things lead to the many applications like smart cities, Logistics, smart agriculture, home automation, health care, military surveillance, security etc [1]. The acceptance of IoT became more appreciable and practical and was easier by applying IPv6. So the larger address space of IPv6 allows more machines to be connect through the internet. Hence, they can interact with each other. So by increasing number of omnipresent devices, it is probable to have some threats in it. In addition, machines have limited energy, processing power and computation. So it require to have secure communications between those devices for the future of IoT applications. Currently so many research is being focused on calculating security mechanisms for IoT that can resist the attacks. In this survey, we are also focuses on the privacy and security of the communication for the IoT. We have analyze the currently available solutions for the communication of different devices, as well as the proposed solutions given in the different literatures. Open privacy issues and challenges for the future work is also identified [2].

2. IoT PARADIGM
2.1 Architecture of IoT

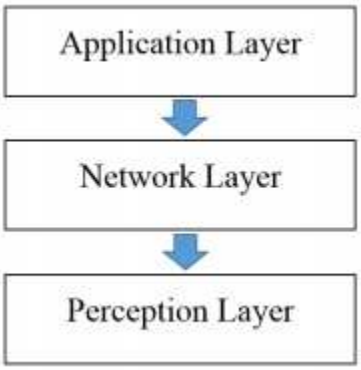

Fig. 1 Architecture of IoT

2.1.1 Perception Layer
Perception Layer is the core layer of IoT. It is also an information/data origin. The Perception Layer is like the facial skin and the five sense organs of loT, which is mainly identifying objects, gathering information. The Perception Layer includes 2-D bar code labels and readers, sensors, camera, GPS, RFID tags and reader-writers, terminals, and sensor network. Its main task is to identify the object, gathering information. All the physical world data/information related to IoT are perceived in the perception layer.

2.1.2 Network Layer
Network Layer provides transparent data transmission capability. This layer is also known as transport layer. The information/data of the perception layer is sent to next layer with the help of existing communication network. We can say that network layer is the brain of the IoT. Network layer also includes core network and access network.

2.1.3 Application Layer
Application layer is also known as Service Layer. It includes application service sub layer and data management sub layer. It is a composition of real world demand and social division. Application layer directly interacts with the users. It mostly contains UI and business logic.

ICTCS '16, March 04-05, 2016, Udaipur, India
 ISBN 978-1-4503-3962-9/16/03..$15.00
DOI: http://dx.doi.org/10.1145/2905055.2905057

2.2 IoT Protocol Stack

2.2.1 Physical Layer

IEEE Standard 802.15.4 (ZIGBEE) defines the PHY layer of the protocol stack. Zigbee is set to rule the smart home IoT market. The Zigbee networks are enabling the IoT/M2M trends and providing different utilities as well as energy services to the consumers. It mainly focuses on low-cost, low-power, low-speed communication between omnipresent devices [4].

Fig. 2 IoT Protocol Stack [3]

2.2.2 Adaptation Layer (6LowPAN)

6LowPAN allows the IPv6 packets to be transferred over the standardized PHY and MAC layer which are broadly applicable to the IoT. To make this possible, 6LowPAN aims at the process of header compression because TCP/IP header size is too large for 802.15.4. So without compression it is not possible to transmit any packet. Another focus of 6LowPAN is on handling the packet fragmentation and reassembling. 1280bytes of Maximum Transfer Unit is required by IPv6, whereas 802.15.4 has 128 bytes of frame. So fragmentation is required to handle this mismatch [5].

2.2.3 Network Layer

The more number of potential devices are getting connected to the IoT network. It is expected to have 20 billion devices connected by 2020. IPv4 is not capable enough to fulfil the needs of IoT. So IoT networks need to use IPv6 to increases the number of addresses from 32bits to 128bits. But the problem is we cannot directly use IPv6, so it requires some modification to use it.

2.2.4 Transport Layer

How we are connecting our local network to the internet is an important task in designing the IoT devices. Transport layer plays an important role in this. Protocols of transport layer provides the reliability of the overall network. TCP is mainly use for the communication between humans and web like emails, web browsing etc. Whereas now a days UDP gains significance in sensor networks. UDP is best suited for the real-time applications in IoT [6].

2.2.5 Application Layer

So many protocols are available for communication at the application layer. But those protocols are too heavy for the IoT networks. So Internet Engineering Task Force (IETF) designed one light weight protocol called Constrained Application Protocol (CoAP) for the communication at application layer in IoT. It is mainly designed for the small, low-power and constrained devices. As the requests and responses are exchanging asynchronously, the use of CoAP is relatively easy [7].

3. RELATED WORK

Privacy and Security are probably the most challenging issues in the IoT, and considerably they have been discussed in many papers. In this section we have identified the issues or challenges for privacy in IoT and currently available solutions for that. Yet the concept IoT privacy and security are not fully defined and having various definitions in various literatures [16]. Though the security issues like integrity and availability are major concerns, Privacy issues like Protection of data and Security of information are also the complimentary requirements for IoT networks. As there are many vulnerabilities in traditional networks, IoT also facing different attacks on network [9] which affects the different functionalities of IoT and degrades the services provided by the IoT networks.

Initially the issue identified in IoT was privacy in end-to-end and in group communication [11]. For that authors in [11] proposes a solution with two approaches i.e. tunneling of DTLS-TLS and key management. The message is encrypted with two keys and sent by sender. In between the proxy takes the first key and decrypts the packets and forward it to the receiver. But the drawback is what if the proxy wasn't trustworthy. So this can be disadvantageous for the constrained networks and for low memory devices. And another problem for group communication is that DTLS and TCP doesn't support multicast [11]. So the solution is needed to secure multicasting in IoT networks.

CoAP protocol have binding with DTLS to secure the CoAP packets with few necessary configurations that is suitable for the constrained environment. DTLS also guarantees [8] the integrity, non-repudiation, confidentiality and authentication at application layer using CoAP. As IoT uses UDP as a transport layer protocol, unreliability of UDP communication is one of the problem faced by IoT networks. By enhancing this area, authors in [15] came up with a solution. They uses datagram transport layer security (DTLS) for authenticated and confidential communication. They compresses the DTLS header in according to reduce overhead using 6LoWPAN mechanism. They reduce the energy consumption and response time of network as compare to the traditional CoAP. They implemented this solution in OS for IoT and tested it in real hardware. The results are effectively shows that the solution is more efficient as compare to traditional/Uncompressed CoAP/DTLS. Since, the observation says that energy required for communication is greater than energy required for computation. So practical implementation of this may not reduce the amount of energy proposed in this solution.

Another issue with using traditional HTTP protocol in constrained network is Overhead and complexity. So this is one of the strong reason to develop new protocol for Constrained networks i.e CoAP [10]. CoAP reduces the overhead in the network so that required bandwidth also decreases. This kind of data reduction increases the reliability of network. The reason behind this is reduction of link layer fragmentation. That also reduce the latency in low-power wireless networks like 802.15.4. Another problem discussed in [10] is privacy and security in the end-to-end communication. That problem is solved by the handshake phase of the DTLS which is used for channel security and authentication. Authors of the [10] discusses the four security modes, based on configuration, for the IoT devices. Those are NoSec, RawPublicKey, Certificate and PreSharedKey. But the observation says that this approach cannot be better adapted for embedded devices. And also in order to defend

latest attacks, protocols are continuously being upgraded and updated.

Though CoAP is uses DTLS for the security, there are many problems with using it directly in IoT domain. In DTLS, we have to send six handshake messages, before sending ciphered data, to exchange key blocks. As packets are fragmented into 127byte MTU size, it causes delay and loss of data in the network, which generate overhead in the constrained network. And such devices can be vulnerable to the DoS attacks also. So authors in [14] came up with proposed solution to this. In that they separated the encryption phase and handshake phase under DTLS by using SSM (Secure Service Manager). As the handshake is performed in SSM, the problem of delay and loss of data can be solved. And also devices are performing the encryption phase only, the chances of DoS attacks can be reduce. But the drawback of this approach is that the constrained devices and SSM should be virtually connected via pre-shared key though it is physically separated. So it requires continuous virtual connection between device and SSM.

In the next paper [12], the authors discusses the lightweight security scheme for the IoT applications. Current solutions like DTLS is not as effective because of its exorbitant handshaking, too large cipher suite process and PKI (Public Key Infrastructure) based authentication. So to overcome these problems, authors in [12] proposes a lightweight security scheme. They used AES (Advance encryption Standard) 128bit symmetric key algorithm. They came up with Auth-Lite and CoAPsLite approach. Auth-Lite enables the lightweight authentication mechanism and CoAPs-Lite enables lightweight security for the CoAP. They achieved that by modifying header of CoAP which is briefly discussed in [12]. But this approach is application specific. This approach can only be used in vehicle tracking systems. So for other application this approach may or may not be helpful.

As the previous work has drawback of expensive handshaking. The author of [13] came with solution to this problem. They proposes an alternative cross-layer approach for optimization of handshaking between the end-points. The proposed method divides the responsibility of communication in two phase such that application layer performs session establishment and transport layer performs the transfer of message into the secure channel. Proposed lightweight solution also defends conventional IoT attacks like cipher text attack, Denial of Service (DoS) attack and replay attack. This system can easily be include with existing system without any significant changes in current system and with minimum additional code. But the observation says that this solution is light weighted only for unicast. This approach cannot work with multicast. So lightweight multicast security solution is yet an open challenge [17].

Having these many lightweight approaches for CoAP, still heavy weight of DTLS being a considerable problem. DTLS headers are too long to get fit in a single MTU (Maximum Transmission Unit). So focusing on the need of minimization of communication overhead, authors in [18], [19] presented their approach on how to overcome these kind of problems. To get reach to this objective authors in [15], [25] have proposed 6LowPAN header compression for DTLS. They have reduced a number of security bits up to 62% [20]. To continue with this approach, authors in [21], [22] have presented a security scheme based on RSA. Their implementation was focused on achieving high interoperability and low overhead. But RSA consumes very large amount of energy which is introduced by computational overhead of DTLS handshake. Other approaches [23], [24] have proposed the performance of handshake using ECC-based cryptography. But the results of all these approaches are showing very high energy consumption.

4. CONCLUSION

In the context of IoT, It is very hard to differentiate the concept of Privacy and Security. This survey reported the current state of solutions available for privacy as well as security. It is clear that security body of IETF depends on DTLS as quality protocol for security. As DTLS provides security solutions by ensuring confidentiality, key management and integrity, combination of CoAP and DTLS may also help to reduce many privacy issues in IoT by applying different discussed approaches. Current research is very much focused in reducing the header size of DTLS and the number of message transfers for the handshake to make CoAP communication lightweight and reliable. Our future work will focus on mitigation approach for the CoAP based on above criteria. We hope that our efforts will be helpful to the new IoT based development.

5. REFERENCES

[1] R. Benabdessalem, M. Hamdi, Tai-Hoon Kim, A Survey on Security Models, Techniques, and Tools for the Internet of Things 7th International Conference on Advanced Software Engineering & Its Applications, 978-1-4799-7761-1/14 2014 IEEE.

[2] J. Granjal, E. Monteiro, and J. S Silva, Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues IEEE Communication Surveys & Tutorials, VOL. 17, NO. 3,2015.

[3] N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler M. Palattella, Standardized protocol stack for the internet of (important) things, Proceedings of IEEE, (2012) 1-18

[4] Zigbee and the Internet of Things [Online]. Available: http://www.telegesis.com/our-markets/internet-of-things/

[5] 6LowPAN: Adaptation Layer Technical Overview [Online]. Available: https://communities.cisco.com/servlet/JiveServlet/downloadBody/52715- 102-1-88316/FAN002 6lowpan.p 1

[6] Xi Chen, Constrained Application Protocol for internet of Things April 2014. [Online]. Available: http://www.cse.wustl.edu/

[7] Shelby Z. (2013, June) Constrained Application Protocol (CoAP). Document. [Online] Available: https://tools.ietf.org/html/draft-ietf-corecoap-18

[8] T. Alghamdi, A. Lasebae, M. Aiash, Security Analysis of the Constrained Application Protocol in the Internet of Things, 978-1-4799- 2975-7/13/ 2013 IEEE

[9] Abomhara, Mohamed, and Geir M. Koien. "Security and privacy in the Internet of Things: Current status and open issues." Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on. IEEE, 2014.

[10] Keoh, Sye Loong, Sahoo Subhendu Kumar, and Hannes Tschofenig. "Securing the internet of things: A standardization perspective." Internet of Things Journal, IEEE 1.3 (2014): 265-275.

[11] Brachmann, Martina, Oscar Garcia-Morchon, and Michael Kirsche. "Security for practical coap applications: Issues and solution approaches." GI/ITG KuVS Fachgesprch Sensornetze (FGSN). Universitt Stuttgart (2011).

[12] Ukil, Arijit, et al. ”Lightweight security scheme for IoT applications using CoAP.” International Journal of Pervasive Computing and Communications10.4 (2014): 372-392.

[13] Bhattacharyya, Abhijan, et al. ”LESS: Lightweight Establishment of Secure Session: A Cross-Layer Approach Using CoAP and DTLSPSK Channel Encryption.” 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, 2015.

[14] Park, Jiye, and Namhi Kang. ”Lightweight secure communication for CoAP-enabled Internet of Things using delegated DTLS handshake.” Information and Communication Technology Convergence (ICTC), 2014 International Conference on. IEEE, 2014.

[15] Raza, Shahid, et al. ”Lithe: Lightweight secure CoAP for the internet of things.” Sensors Journal, IEEE13.10 (2013): 3711-3720.

[16] G. Baldini, D. Rotondi IoT Governance, Privacy and Security Issues European Research Cluster on the internet of things [Online].Available:http://www.researchgate.net/publication/275540220

[17] A. Rahman and E. Dijk. Group Communication for CoAP (draft-ietfcore-groupcomm 25).

[18] K. Hartke, Practical Issues with Datagram Transport LayerSecurity in Constrained Environments draft-hartke-dice-practicalissues-01, DICE Internet-Draft, April 2014. [Online]. Available: http://tools.ietf.org/html/draft-hartke-dice-practical-issues-01

[19] S. Keoh, S. Kumar, and Z. Shelby, Proling of DTLS for CoAP-based IoT Applications draft-keoh-dice-dtls-prole-iot-00, Internet-Draft November 2013. [Online]. Available: http://tools.ietf.org/html/draft-keoh-dice-dtlsprole-iot-00

[20] Capossele, Angelo, et al. ”Security as a CoAP resource: an optimized DTLS implementation for the IoT.” Proceedings of ICC 2015, IEEE (2015).

[21] T. Kothmayr, A Security Architecture for Wireless Sensor Networks based on DTLS, Masters thesis, Universitat Augsburg, December 2011.

[22] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, and G. Carle, DTLS based security and two-way authentication for the Internet of Things, Elsevier, Ad Hoc Networks, vol. 11, no. 8, pp. 2710 2723, 2013.

[23] Granjal, Jorge, Edmundo Monteiro, and Jorge Sa Silva. ”On the effectiveness of end-to-end security for internet-integrated sensing applications.” Green Computing and Communications (GreenCom), 2012 IEEE International Conference on. IEEE, 2012.

[24] Granjal, Jorge, Edmundo Monteiro, and Jorge Sa Silva. ”End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication.” IFIP Networking Conference, 2013. IEEE, 2013.

[25] Raza, Shahid, Daniele Trabalza, and Thiemo Voigt. ”6LoWPAN compressed DTLS for CoAP.” Distributed Computing in Sensor Systems (DCOSS), 2012 IEEE 8th International Conference on. IEEE, 2012.