Review on Authentication Techniques in IOT Network

Dewesh Tiwari, Ajit Kumar Tiwari

Bhabha College of Engineering, RKDF University, Bhopal, M.P. India

Abstract: This paper presents a review on the various authentication techniques in IOT Networks. With the large use of internet and automated devices, the demand of IOT is increasing day by day. Although it may also include other sensor technologies, wireless technologies, or QR codes, RFID was initially thought of as the only method of communication. The advantages of IPV6 are now integrated into IP-based protocols and technologies. The service-providing entity is now connected to nearby websites and data bases in addition to being accessed by the owner. A lot of things work together to provide ambient intelligence. Additionally, they can be remotely accessed and managed by legitimate servers other than the owner.

In light of this scenario, proper authentication and access control techniques must be implemented to ensure that only moral users can access and interact with the networks.

Thus in IOT network the main concern is of security of the data for which proper authentication and access control is needed. The paper also presents the examination of the various authentication methods used by constrained networks.

Keywords: IOT, Security, Authentication,Access Control

I. INTRODUCTION

The phrase "Internet of Things" (IoT), which was first used by Kevin Ashton [1], represents a future society in which both living and non-living physical objects will be connected to the internet and be able to communicate with one another and web service applications. The hosts in the web are represented by the entities attached to the sensors and microcontrollers. From now on, enabling the limited real-world citizens to mature into elite Internet citizens A framework that encourages acknowledging future developments and visions is created by the Internet of Things.Implanted frameworks that are constrained in terms of power, compute, and memory are typically present in physical entities that are coupled to restricted devices. These legally required devices are connected and utilize the shaky Internet services. Some sorts of security features are required because of this. The most modern security alternatives, such TLS [3] and IPsec [4], are IP-based, but they are not designed for restricted devices because communication costs are so high and expensive handshaking techniques are necessary. As a result, it is impossible to directly and effectively apply current IP-based security standards. PSK is frequently utilized in WSN due to its low resource needs for computation and verification. This strategy works well in neighbourhood and segmented setups when the key discretion is controlled by a domain administrator. PSK is widely used in WSN because it uses a small amount of resources for computation and verification. When a domain administrator controls the key discretion, this methodology works well in neighbourhood and segmented settings. In any case, key management in symmetric key-based configurations is unreasonable and impractical to modify, particularly when participants are drawn from various domains, as in the IoT scenario. This is because each host uses a unique key that must be created and deployed in advance.

The need for IOT is growing daily as a result of the widespread usage of the internet and automated devices. Although other sensor technologies, wireless technologies, and QR codes may also be used, RFID was once believed to be the only means of communication. Today's IP-based protocols and technologies incorporate IPV6's advantages. In addition to being viewed by the owner, the service-providing business is now linked to adjacent websites and databases. In order to provide ambient intelligence, many factors interact. They can also be managed and accessed remotely by trustworthy servers other than the owner.

In light of this scenario, proper authentication and access control techniques must be implemented to ensure that only moral users can access and interact with the networks.

Thus in IOT network the main concern is of security of the data for which proper authentication and access control techniques are needed which is the main concern of this paper.

The primary targets of this thesis are the examination of the various authentication methods used by constrained networks. The rest of the paper has been organized as follows: section 2 covers literature survey, section 3 covers detection of moving object, section 4 presents the experimental results, section 5 concludes the paper and references are given at the end.

II. LITERATURE REVIEW

In order to establish an experiment framework and to choose result analysis methods (i.e. performance metrics), a literature review is needed. Literature Review done and is successfully completed whose summary is given below. Exhaustive survey of published literature has been conducted to have an in depth insight of the research issues. Literature from Journals, IEEE Communication Magazines, IEEE Transactions, and from digital libraries has been found out

E. Rescorla, N. Modadugu, "Datagram Transport LayerSecurity" , discusses about the Datagram Transport Layer Security (DTLS) protocol in this document in version 1.2. Datagram protocols are given communication privacy by the DTLS protocol. Client/server applications can communicate using the protocol in a way that is intended to thwart message forging, eavesdropping, and tampering. Similar security guarantees are offered by the DTLS protocol, which is based on the Transport Layer Security (TLS) protocol. The DTLS protocol maintains the datagram semantics of the underlying transport. This document makes DTLS 1.0 compatible with TLS 1.2.

F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-levelsensornetwork simulation with cooja," in *Local* Simulators for wireless sensor networks discusses a valuable tool for system development. However, current simulators can only simulate a single level of a system at once. This makes system development and evolution difficult since developers cannot use the same simulator for both high-level algorithm development and low-level development such as device-driver implementations. We propose cross-level simulation, a novel type of wireless sensor network simulation that enables holistic simultaneous simulation at different levels. We present an implementation of such a simulator, COOJA, a simulator for the Contiki sensor node operating system. COOJA allows for simultaneous simulation at the network level, the operating system level, and the machine code instruction set level. With COOJA, we show the feasibility of the cross-level simulation approach.

E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl, "Home networking with ieee 802. 15. 4: a Developing standard for low-rate wireless personal area networks" discusses Software Defined Networking (SDN) centralizes network control to improve network programmability and flexibility. Contrary to wired settings, it is unclear how to support SDN in low power and lossy networks like typical Internet of Things (IoT) ones. Challenges encompass providing reliable in-band connectivity between the centralized controller and out-of-range nodes, and coping with physical limitations of the highly resource-constrained IoT devices. In this work, we present Whisper, an enabler for SDN in low power and lossy networks. The centralized Whisper controller of a network remotely controls nodes' forwarding and cell allocation.

To do so, the controller sends carefully computed routing and scheduling messages that are fully compatible with the protocols run in the network. This mechanism ensures the best possible in-band connectivity between the controller and all network nodes, capitalizing on an interface which is already supported by network devices. Whisper's internal algorithms further reduce the number of messages sent by the controller, to make the exerted control as lightweight as possible for the devices. Beyond detailing Whisper's design, we discuss compelling use cases that Whisper unlocks, including rerouting around low-battery devices and providing runtime defense to jamming attacks. We also describe how to implement Whisper in current IoT open standards (RPL and 6TiSCH) without modifying IoT devices' firmware. This shows that Whisper can implement an SDN-like control for distributed low power networks with no specific support for SDN, from legacy to next generation IoT devices. Our testbed experiments show that Whisper successfully controls the network in both the scheduling and routing plane, with significantly less overhead than other SDN-IoT solutions, no additional latency and no packet loss.

N. Kushalnagar, G . Montenegro, C . Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks describes This document investigates potential application scenarios and use cases for low-power wireless personal area networks (LoWPANs). This document provides dimensions of design space for LoWPAN applications. A list of use cases and market domains that may benefit and motivate the work currently done in the 6LoWPAN Working Group is provided with the characteristics of each dimension. A complete list of practical use cases is not the goal of this document. This document is not an Internet Standards Track specification; it is published for informational purposes.

We discuss the characteristics of the constrained devices and the network in which they operate in the first section. A brief overview of pertinent cryptography requirements is then highlighted. Finally, we discuss the Datagram Transport Layer Security (DTLS) protocol**.**

III. METHODOLOGY

There are two methods for authentication in constrained networks. One is Centralizedapproach and another is Delegation Based Approach. Here we have discuss both of them

1. Centralizedapproach

Symmetric-key secure M2M communication methodologies are effective and appropriate for constrained networks. On the other hand, the flexibility of the key administration is a common problem as a result. A single key must be shared by two entities in order to communicate. Therefore, before the actual deployment, an entity must be preoccupied with the entire key individuals with whom it wishes to communicate. Scalable and advanced key distribution techniques are introduced to address this issue. A key distributor is used here, which is only a central server performing the function of key agreement. The restricted entities are focused on using a secure key to communicate safely with the central server. Small domains can use this, and it requires a high level of trust in the key distributor. Building confidence between key distributors from different domains, however, might be difficult when two entities present in two different domains seek to communicate. Here, the key distribution procedure in sensor networks is simplified. Here, each entity is given a polynomial share P(; b) derived from a discrete symmetric polynomial P. (a; b). Therefore, a secret key P(1; 2) that is used for communication can only be used by nodes that have a polynomial share.

2. Delegation Based Approach

Methodologies based on delegation provide ways to delegate computationally escalating work to more powerful devices. For instance, public-key operations used in session setup are typically delegated. One of these delegation methods is the Server-based Certificate Validation Protocol (SCVP) [19]. Here, a trusted server is given the challenging responsibility of creating a certificate path or validating a certificate. Clients don't need to worry about the specific method for authentication acceptance, which enables them to have a clear justification. On the other hand, this necessitates that the SCVP server be trusted, much like a neighbourhood programme.

In the event that there are any untrusted SCVP servers, the customer may assign less fundamental tasks, such as obtaining disavowal information via a CRL method. SCVP uses a MAC or a digital signature to protect the integrity of the questions and answers. A key agreement method, such as Diffie-Hellman (DH), is used to compromise the key used to create the MAC. This implies that clients must push themselves and carry out extravagant public-key-based operations. This methodology also develops overhead outside constrained networks for handshaking operations. Because of the necessity of transmitting a chain of certificates during a handshake, this results in significant transmission overhead due to the length of certificates. However, the constrained devices need additional protocol capabilities related to SCVP. Another delegation-based IoT strategy. The concept states that the public-key-based operations are transferred to a far more efficient device, such as the Gateway (GW). They suggested the strategy, which asserts that the GW is the end point and incorporates the Internet Key Exchange (IK) session establishment process. The constrained devices are given over the session key after being computed by the GW. From this point forward, the entities use this session key to secure communication.In this technique, the GW is regarded as having a high level of trust. As a next step element, the GW with the session key can now access the plain text in communication. Thus, it possesses the hidden power to change messages. As a result, the node-to-node security is compromised, albeit in some applications, this may be acceptable. For instance, the GW is widely trusted in the mechanical industries, and this scheme can be effectively used in those fields. Another scenario in which the individual cell phone serves as the GW for severely constrained devices is the Body Area Network (BAN). In this case, a high level of confidence is given to the individual cell phone.In any case, the IoT vision generally does not have access to a reliable GW all the time. The network in the scenario of the smart city has constrained devices made by various manufacturers. These devices do not necessarily provide the GW with a strong sense of trust, which could come from a different type of administrative support.

IV. CONCLUSION

The literature survey that has done during the research work gives us an idea of various authentication techniques used in constrained networks. Here we have presented a review work on authentication techniques of IOT network and has given two authentication strategies which when used for authentication will give a secure and efficient network.

REFERENCES

1. K. Ashton, "That internet of things thing," *RFiD Journal*, Vol. 22, no. 7, pp. 97–114, 2009. Friedman Mattern. Hundert JahreZukunft,Visionen zum, Available: http://link.springer.com/Chapter/10.1007%2F978-3-540-71455-2 18.
2. 2. T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246, IETF," August 2008, Available: http://tools.ietf.org/html/rfc5246
3. S. Frankel, S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. RFC 6071, IETF," February 2011, Available: http://tools.ietf.org/html/rfc6071.
4. F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *Local Computer Networks, Proceedings2006 31st IEEEConferenceon*. IEEE, 2006, pp.641–648.
5. Z. Shelby,et al., "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). RFC 6775, IETF," November 2012, Available: http://tools.ietf.org/html/rfc6775
6. E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl, "Home networking with ieee 802. 15. 4: a developing standard for low-rate wireless personal area networks," *IEEE Communications magazine*, vol. 40, no. 8, pp. 70–77, 2002.
7. N. Venkatesh, "Ultra-low power 802.11 n Wi-Fi–wireless connectivity for the internet of things.," *Low-Power Wireless as White Paper, Last visited on*, vol. 16, p. 2013, 2010.
8. S. Bluetooth, "The Bluetooth core specification, v4. 0," *Bluetooth SIG: San Jose, CA, USA*, 2010.
9. N. Kushalnagar, G. Montenegro, C . Schumacher, " IPv6 over Low-Power Wireless Personal Area Networks(6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919, IETF," August 2007, Available: http://tools.ietf.org/html/rfc4919.
10. G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944.
11. A. Dunkels, B. Gronvall, and T. Voigt, "Contiki-a light weight andflexible operating system for tiny networked sensors," in *Local Computer Networks, 2004. 29th Annual IEEE InternationalConferenceon* IEEE, 2004, pp.455–462.
12. A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks," *Wireless networks*, vol. 8, no. 5, pp. 521–534, 2002.
13. O. G. Morchon and H. Baldus, "Efficient distributed security for wireless medical sensor networks," in *Intelligent Sensors, Sensor Networks and InformationProcessing, 2008. ISSNIP 2008.International Conference on*. IEEE, 2008, pp. 249–254.
14. T. Freeman, A. Malpani, D. Cooper, and R. Housley, "Server-based certificate validation protocol (scvp)," 2007
15. R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, "Secure communication for smart iot objects: Protocol stacks, use cases and practical examples," in *World of Wireless, Mobileand Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*. IEEE, 2012, pp. 1–7.