THE SECURE AUTHENTICATION MECHANISM TO INCREASE THE SECURITY OF IOT DEVICES.

Navneet Khubber
Research Scholar
Haryana Engineering College, Jagadhri, Haryana (India)

Abstract

The Internet of Things (IoT) states to the use of intelligently connected devices and schemes to leverage data assembled by embedded sensors and actuators in machines and extra physical objects[1]. But the clocks of IoT devices are not well synchronized due which security gets compromised. In this research work, the time lay technique will be proposed which will synchronize the clocks of the IoT devices and also establish secure channel from source to destination for data transmission and thereby improving the security of the network.

Keywords - Internet of Things(IoT), Time lay, Base station(BS), Radio Frequency Identification(RFID)

Introduction

We are living in a digital world where potentially every object is becoming digital, mobile and connected via the internet. These waves of technological changes will bring not only huge opportunities, but also new risks. These waves of technological changes will combine the reach of the Internet with a ability to directly control and manage machines, devices and the infrastructure of the physical world.

The Internet of Things (IoT) can be defined as the ability of objects of everyday use to connect to internet and exchange information. IoT system provides an interconnected environment where objects have digital presence and can also communicate with each other and people. [2]. With the advent of IPv6 and the wide arrangement of Wi-Fi networks, IoT is growing at a precariously fast pace, and researchers estimate that by 2020, the number of active wireless connected procedures will exceed 40 billion.[3]While IoT is expected to offer many benefits ranging from smart homes, smart cities, healthcare surveillance, smart wearable devices etc., adding insecure devices to a network can have serious consequences. Security in IoT is fundamentally linked to the ability of users to trust their environment. Therefore, an added level of security related to data encryption, data authentication etc. is required.

Security and Privacy Issues in IoT

The internet is extended to physical world with the help of IoT technology due to which various security and privacy issues have risen. The internal properties of IoT as well as the differences of this technology against other traditional networks are mainly the reasons of causing such issues. In order to attack the IoT systems, several adversaries have come up. The examination of various security issues as per the information flows and potential adversarial points of control is very important in order to protect the system from various attacks. The four security and privacy issues that are found more often are mentioned and described below:

- Authentication and physical threats: Mostly within the public regions most of the highly distributed IoT devices are deployed such as RFID tags as well as wireless sensors. Thus, the management as well as vulnerability of these devices from physical attacks becomes more difficult. For instance, a malicious sensor might display some other location other than where it actually is. Also, a malicious person might move the sensor installed in one environment to complete different scenario. Thus, the authentication of IoT devices becomes important due to which the devices need to be recognized and with respect to correct topological address the device’s association is to be verified.

- Integrity: Data integrity has become a concern due to the presence of unattended scenario for IoT devices. A self-supported manner is followed during the operation of most of the devices once they are deployed. In comparison to the supervised wired network, the tampering of data is performed very earlier since there is very little or no maintenance required at all [5]. The quality of data that is gathered by IoT devices is assumed to be very low and might also be corrupted due to the natural loss of calibration or perturbation. Thus, there is huge amount of noise present within the data and its spoofing and forging becomes very easy.
- Confidentiality: There is a wireless communication mode utilized amongst the devices as well as gateway. Due to this reason, the confidentiality of data comes to a risk. For instance, within the wireless networks, a major issue that arises is eavesdropping. Due to the presence of resource-constrained types of low-end devices that constitute most of the parts of IoT devices, the confidentiality of the data that is to be transmitted is not easy. The IoTs are active sensors or passive RFID tags that include very limited number of resources and capabilities and thus are very different from that of traditional wired and wireless networks. A higher barrier is provided with the help of storage and other properties of IoT device with the help of which the important operations are performed along with assurance of confidentiality of data.
- Privacy: In case when the IoT networks are integrated with global internet in order to provide monitoring and interaction with real world, the leakage of information is possible. The data might be accessible to various organizations and domains present on Internet through the connection of real world objects and information [6]. However, here the chances of exploitation and attacks are higher since the information is exposed to several users amongst which many might be malicious.

Related work

Daemin Shin el al(2016) highlighted the issue of routing and secure channel establishment from source to destination. To establish secure path and handle mobility IPv6 Proxy is used which handles mobility and also provides secure channel between two parties. But IPv6 is complex and increases network delay at the time of encryption and decryption .[7]

B.VinayagaSundaram(2015) proposed that major security issues occur only when nodes are connected to the internet. So instead of connecting the devicesseparately to the internet, a common access point can be setup from which the nodes can get access to the internet. So network security can be applied to the single access point.A cryptographic algorithm(RC-5,AES etc.) is devised for ensuring security within the Wireless Sensor Network.This algorithm is devised in such a way that it is suitable for sensor nodes. Sensor devices have limited memory size, processing speed and energy supply. [8]

J. Granjal et.al (2015)proposed that the architecture of IoT devices has IP-based communication protocols that provide the connectivity of devices as per the required applications. It was realized that there was a need of presence of such communication technologies in the areas where information sensing was very important. Keeping in context the goals of ensuring efficiency, reliability and internet connectivity, the various applications of IoT systems are proposed [9]. The communications being held within these systems was ensured to be protected which might only provide the usage of such applications more frequent. If the privacy or security was not assured, the users might not opt for their usage.

C. Mahapatra et.al (2016)stated that the systems that enable the various actions to be performed on the real time sensors as well as virtual online sensors are known as the IoT system. These systems help in sensing, collecting, storing, processing and transmitting the required data from the sensors. The main aspects here are the energy efficiency as well as the robust data delivery within these systems. In [10], the active RFID tags that were based on cluster head determination as well as energy harvesting of the IoT systems are proposed. As per the results it is seen that the IoT based WSN heterogeneous systems provide enhancement in the case of energy efficiency and data delivery. There is a great improvement seen through the simulation results achieved here. The energy consumption models have been formulated here as per the sensor nodes that were sent to the base station by the gateway nodes. The simulation depicted considerable improvement in lifetime of network and data delivery to the base station(BS).

table: summary of various security techniques

Author	Year	Technique	Outcome
Daemin Shin	2016	Proxy Mobile IPv6	PMIPv6 handles mobility and also provides secure channel between two parties
B.VinayagaSundaram	2015	Encryption and Hash based Security	Known cipher text attack is not possible because of the large key length (128 bits)
C. Mahapatra	2016	Data aware energy Efficient distributed clustering protocol (DAEECI)	substantial improvement in lifetime of network and data delivery to the BS
Rahul Godha	2014	Tagging Mechanism for access control	The tags will be kept private within the centralized and it should not be shared with any other devices.

Conclusion

The IoT is the decentralized network in which the devices can sense information and upload that information to the server. But IoT suffers from major security issues. The proposed work provides the solution to the problems which are mobility management and secure channel establishment from source to destination. Time lay techniques is proposed to synchronize the clocks of the network.To provide end-to-end encryption and to implement soft handoff, technique of elliptic curve cryptography and angle of trajectory is applied in the network. The proposed improvement leads to increase security of the network and reduce packetloss in the network.

References

[1] Internet of Things and data analytics handbook/edited by HwaiyuGeng.

[2] IoT connected world: security and privacy.

[3] techcrunch.com/why-iot-security-is-so-critical/ Ben Dickson(2015).

[4] B. Guo, Z. Yu, L. Chen, X. Zhou, and X. Ma(2016), "MobiGroup: Enabling Lifecycle Support to Social Activity Organization and Suggestion with Mobile Crowd Sensing", IEEE Transactions on Human-Machine Systems, vol. 46, no. 3, pp. 390-402.

[5] Guo, D. Zhang, Z. Wang , Z. Yu, and X. Zhou(2013), "Opportunistic IoT: Exploring the Harmonious Interaction between Human and the Internet of Things", Journal of Network and Computer Applications, vol. 36, no. 6, pp. 1531– 1539.

[6] Namiot and M. Sneps-Sneppe(2013), "Social Streams based on Network Proximity," 2013, International Journal of Space-Based and Situated Computing, vol. 3, no. 4, pp. 234-242.

[7] Daemin Shin, Vishal Sharma, Jiyoon Kim, Soonhyun Kwon, and Ilsun You (2016), "Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks"

[8]B.VinayagaSundaram, Ramnath.M, Prasanth.Mand VarshaSundaram.J (2015), 3rd International Conference on Signal Processing, Communication and Networking (ICSCN).

[9] J. Granjal, E. Monteiro, and J. Silva(2015), "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," in Proc. of IEEE on Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312.

[10] C. Mahapatra, Z. Sheng and V. Leung(2016), "Energy-efficient and Distributed Data-aware Clustering Protocol for the Internet-of-Things", in Proc. of IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), vol. 1, pp. 1-6.