Survey on Providing Security and Authentication for Devices to Achieve QOS in IOT

Mudassar M. Shaikh[1], Prof. V. V. Jog[2]

Abstract: ***The IOT (Internet of Things) is a network which connects things to the Internet for the intend of interchanging information through the information sensing devices with acceptable protocols. Sensing Devices utilize in households and smart city is now interconnected with the Internet. This interconnection provides a whole range of data (industrial context, device status, etc.) that can be collected, aggregated, and then shared in secure, and privacy-aware manner. Some essential fields such as Wireless Sensor Network and Intelligent Transport System (ITS), base nodes collect information and transmit it to the destination nodes. Destination sends commands by the relay devices to the base nodes. Thus how maintain the security of both base nodes and destination nodes in this kind of communication is a pressing problem. Instead of proposing yet another security scheme, this can be made easy if devices are identified before communication with secure routing***

Keywords: IOT (Internet of Things), Sensor nodes, Routing algorithm, Security.

1. Introduction

Internet of Things (IoT) is a part of future internet with self-organizing capabilities which will help human and connected things with the help of agreed protocols. The elements of the IoT comprise not only those devices that are already deeply rooted in the technological world (such as cars or fridges), but also objects foreign to this environment (garments or perishable food), or even living beings (plantations, woods or Livestock). By embedding computational capabilities in all kinds of objects and living beings, it will be possible to provide a qualitative and quantitative leap in several sectors: healthcare, logistics, entertainment, and so on.

In the IoT, the surrounding objects are connected into networks with each other in much form. (RFID) RF Identification, sensor technology (WSN), and some other technologies will be enclosed into a variety of applications accepted common definition of IOT is not yet defined by any standard of organization although there are various definitions of IOT. Evolution in the technology, energy constrained devices, power, storage and high power batteries have become easy to purchase at low cost. This increasing trend enabling the manufacturing and development of small scale devices with appropriate security and identification mechanism

“Things” that are connected with each other should have the following three peculiarities

1) ***Comprising Approach***: Using RFID, Sensors, obtain the object information at anytime from anywhere. Using it, information and communication systems can be embedded in the system around us. Identification and recognition of the devices and authentication and security purpose
2) ***Reliable-Transmission***: Devices which communicates with each other should transmits the data reliably by using secure routing transmission. Wireless and Wired technologies, gateway technologies are used. IOT allows and creates the communication between these devices.
3) ***Intelligent Processing***: Various technologies like (WSN) allows the data to be flow, sense, and transmit easily from devices to devices. The emerging technologies helps the IOT vision to make it works

2. Related Work

Timo Koskela, *Sami* Hakola, Tao Chenand Janne Lehtomaki[1] proposed the direct communication between two devices using cluster. Direct communication of devices reduces the work load of cluster setup and load on cluster heads. Transmission delay issues are solved by using D2D communication and instant service is achieved to devices. Examples like, YouTube, Facebook, Myspace can possibly get benefits from direct communication.

Jun Suk Kim, Jaheon Gu, and Min Young Chung [2], proposed a novel scheme for cluster based D2D group communication. The proposed scheme enables the UEs to form cluster by broadcast-based information exchange and to mediate the medium access in the cluster or between clusters to communicate each other. Through the proposed scheme, UEs can communicate with UEs belong to the same cluster or the other cluster.

Cristina Alcaraz, Pablo Najera, Javier Lopez, Rodrigo Roman [3] authors show how the integration of WSN in IOT improves the trust of users towards devices. In order to allow WSN to become an intrinsic part of the IoT in a secure way, several security challenges have been considered. Several approaches have been made to solve the security challenges by Integrating WSN in IOT.

YANG Jin-cui, PANG Hao, ZHANG Xin [4] this paper improves the two way mutual authentication Protocol by enhancing system model. Several new techniques have been added to the previous two mutual authentication protocols. It also overcomes the problems of one-way authentication protocol directly by using two way mutual authentications and secondly enhances the two way mutual authentication protocols.

Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brunig and Georg Carle, [5]proposed the two authentication with RSA algorithm. In this paper, introduce the first fully implemented two way authentication security scheme for the

Internet of Things (IoT) based on existing Internet standards, especially the Datagram Transport Layer Security (DTLS) protocol. The proposed security scheme is based on the most widely used public key cryptography (RSA)

Huansheng Ning, Hong Liu, Laurence T. Yang, [6] to design an aggregated-proof based hierarchical authentication scheme for the layered networks. I) the aggregated-proofs are established for multiple targets to achieve backward and forward anonymous data transmission; II) the directed path descriptors, homomorphism functions, and Chebyshev chaotic maps are jointly applied for mutual authentication; III) different access authorities are assigned to achieve hierarchical access control

Yijun Maoa, Jin Li, Min-Rong Chenc, d, Jianan Liue, Congge Xiee, Yiju Zhanf [7] author proposed Fuzzy identity-based encryption to provide security in IOT environment.In addition, this scheme has the advantage of tight security reduction. Thus in contrast to previous FIBE schemes with loose security reduction, this scheme needs not to enlarge the keys size and ciphertext sizes to obtain the same security level. Our scheme also enjoys the advantage of constant size of public parameters.

Kun Yang, Domenic Forte, and Mark M. Tehranipoor [8] this paper proposed an RFID-enabled solution that aims at protecting endpoint devices in IoT supply chain. By taking advantage of the connection between RFID tag and control chip in an IoT device to enable data transfer from tag memory to centralized database for authentication once deployed.

Omaimah Omar Bamasag, Kamal Youcef-Toumi [9] we propose a novel continuous authentication protocol for the Internet of Things based on secret sharingscheme. This protocol provides secure and efficient authentication for frequent message transmissions in short session time intervals. The protocol introduces a novel use of secret sharing scheme, that is, the secret is used as an authenticator and the shares are used as authenticator tokens.

Sebastian Unger and Dirk Timmermann [10] Instead of searching for another security strategy, author have looked for an existing, solution that can be widely accepted related to domain as security framework for devices that are sensitive. By analyzing its concepts carefully and the parts which are suitable and necessary for IOT systems. In this paper author

Have describe the methodology and applied to derive the Devices Profile for Web Services Security (DPWSec).

3. Literature SurveyEvaluation

Table 1: Literature Survey

Author	Proposed work	Advantages	Disadvantages
TimoKoskela *et. al*	Direct communication between two devices using cluster	Direct communication reduces thetransmission delay	If one node fails it can lead to whole communication failure.
Jun Suk Kim *et.al.*	Cluster based D2D group communication	Use of cluster overcomes the problem of node failure problem	Selecting feasible device for cluster head
Cristina Alcaraz *et. al*	Integration of WSN in IOT environment	Provides ease of use of IOT devices with help of WSN devices	Deciding the topology to be used is difficult
YANG Jin-cu *et. al*	Enhanced two way mutual authentication protocol	It enhances the working of two way communication protocol which solve the old issues	Replication of each devices can lead to cost problem
Thomas Kothmayr*et.al*	Proposes two way authentication using RSA algorithm	Provides end to end security. Data updating mechanism and security involved to tackle attacks like Meet in middle	Generating key by using RSA is heavy task. Dynamic update can handle key protection against eavesdropping
Huansheng *Ning et al.*	aggregated-proof with mutual authentication	Gives Proof of authentication for devices	Attacker can overwhelm such a server by flooding it with connection requests
Yijun Maoa *et. al*	proposed Fuzzy identity-based encryption to provide security in IOT environment	Eliminate the need for certificates as used in the traditional public key infrastructure (PKI),	Need to enlarge the key size for security purpose
Kun Yang *et. al*	RFID-enabled solution that aims at protecting endpoint devices in IOT supply chain.	Enable data transfer from tag memory to centralized database for authentication once Deployed.	Providing Continuesauthentication to causes can't be done
Omaimah Omar Bamasag *et. al*	novel continuous authentication protocol for the Internet of Things based on secret sharing scheme	provides secure and efficient authentication for frequent message transmissions in short session time intervals	Problem can be raised when we are using for the multi factor or multilayer

4. Conclusion

"Things" that are connected to each other with the help of internet faces various security issues, authentication issues, data integrity, accesses policies and so on. Users are getting involved in IOT paradigm which increases the User to User, User to Machine, and Machine to Machine interactions.To this purpose, it is observe that various security measures have been done for securing devices, secure routing, and clustering concept for efficiency in communication.In this paper, we have surveyed the aspects of the IoT with emphasis on what is being done related to secure and efficient communication and what are the issues that require further research

5. Future Scope

Future work will be focus on how devices can be identified to provide required quality of service based on their working capabilities and performance regarding their storage and transmitting capabilities with respect to secure transmission.

References

[1] Timo Koskela, Sami Hakola, Tao Chenand Janne Lehtomak "Clustering Concept using Device-to-Device Communication in Cellular System"
[2] Jun Suk Kim, Jaheon Gu, and Min Young Chung "Clustering Concept using Device-to-Device Communication in Cellular System"
[3] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, "Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?",1st International Workshop on the Security of the Internet of Things (SecIoT10), pp., 2010.
[4] YANG Jin-cui, PANG Hao, ZHANG Xin "Enhanced mutual authentication model of IoT"
[5] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brunig and Georg Carle" DTLS based security and two-way authentication for the Internet of Thing" Ad Hoc Networks, 2013 Zitiert von: 47 - Ähnliche Artikel - Alle 6 Versionen
[6] Huansheng Ning, Hong Liu, Laurence T. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things", IEEE transactions on parallel and distributed systems, VOL. 26, NO. 3, pp. 657-667, MARCH 2015.
[7] Yijun Mao, Jin Li, Min-Rong Chen, Jianan Liu, Congge Xie, Yiju Zhan "Fully Secure Fuzzy Identity-Based Encryption for Secure IoT Communications" Computer Standards & Interfaces, 25 June 2015
[8] Kun Yang, Domenic Forte, and Mark M. Tehranipoor" Protecting Endpoint Devices in IoT Supply Chain"
[9] Omaimah Omar Bamasag, Kamal Youcef-Toum "Towards Continuous Authentication in Internet of Things Basedon Secret Sharing Scheme"
[10] Sebastian Unger and Dirk Timmermann "Devices Profile for Web Services Security"2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) (The International Workshop on Emerging Wireless Sensors Network Applications) Singapore, 7-9 April 2015