ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Robust Scheme for Secure Communication in Internet of Things

Anjali Yeole, Sadaf Ahmedi, Kirti Madhwani, Sneha Sahijwani, Pooja Talreja

Assistant Professor, Dept. of Computer Science, Vivekanand Education Society's Institute of Technology, Chembur, India

Final year student, Dept. of Computer Science, Vivekanand Education Society's Institute of Technology, Chembur, India

Final year student, Dept. of Computer Science, Vivekanand Education Society's Institute of Technology, Chembur, India

Final year student, Dept. of Computer Science, Vivekanand Education Society's Institute of Technology, Chembur, India

Final year student, Dept. of Computer Science, Vivekanand Education Society's Institute of Technology, Chembur, India

ABSTRACT: Development of Internet of Things (IOT) has created concerns about the security of IOT. The security framework of Internet cannot provide a complete solution to all security problems. This paper attempts to provide a two-way authentication scheme followed by dynamic variable cipher security certificate in internet of things which can be applied securely in Internet of Things.The proposed paper implements the security structure on sensor layer and application layer in IOT which analyzes features of security. Based on secure hash algorithm, we present an asymmetric two-way authentication scheme between the platform and terminal combined with method of "one time one cipher" in communication process. It is a lightweight process of encryption and decryption in IOT.

KEYWORDS: IOT,two-way authentication scheme, dynamic variable cipher, platform, terminal, cooja, mote

I. INTRODUCTION

The Internet of Things (IOT) is the extension of the Internet, which refers to the interconnection and communication of everyday objects. It is generally viewed as a self-configuring wireless network of sensors whose purpose would be to interconnect all things [1] [2]. An example of an IOT object is a thermostat through which location can be determined and temperature of air conditioners and heaters can be controlled. Consumer, governmental and business trends are also pushing us toward the IOT. The nodes in IOT uses wireless network to communicate with each other for the authorized user. There are two types of node which communicate with each other. The platform node sends instructions to the terminal node. The terminal node on receiving instructions starts working and gathers necessary information which is to be transmitted back to the platform. Therefore, security becomes the major issue during communication of the IOT nodes.

The present security schemes for IOT devices uses public key cryptography in which two nodes agree upon certain key and use that key for information exchange. However, if this key is hacked then it will adversely affect the security of the system. To avoid this we need to have key which will be generated dynamically and shared between nodes for only certain period of time called session. For each session, key generated will be different and unique. The IOT nodes that are willing to communicate with each other must first authenticate themselves to each other so that identity of the node is ensured. The main purpose for proposing this scheme is to enhance the present security schemes used for IOT and eventually compare the result and performance of both - the present security protocol and the proposed protocol.

The proposed scheme is based on two-way authentication which means that the two nodes viz. platform and terminal will authenticate themselves to each other to ensure their identity. This is based on Secure Hash function. The platform and terminal must be authenticated before communication begins. Because if there is no proper authentication then attacker may attack the network to get access to confidential information illegally. This is followed by dynamic key generation algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Dynamic variable cipher security offers a safe variable key authentication protocol based on request-reply mechanism. It has characteristics like "one time one cipher", real-time performance on timestamp highly efficient data stores, the cost of computation is low. It can be used in the authentication process of other short range technologies.

II. RELATED WORK

In wireless mobile communication and wireless sensor networks many identity authentication schemes have been proposed. In [3] the authors have proposed an identity authentication scheme for wireless sensor networks, which based on elliptic curve cryptography. In [4] authors have investigated a distributed user authentication scheme in wireless sensor networks, which is based on self-certified keys cryptosystem. However, only the user nodes are authenticated in both of the above schemes. In [5] authors have presented a four entity mutual authentication technique for mobile communications which demands much computation resource.

In [6] authors have proposed a novel mutual identity authentication scheme which is based on secure hash algorithm(SHA), feature extraction and elliptic curve cryptography(ECC), this is an asymmetric mutual authentication scheme between the platform and the terminal node, which imposes light computation and communication cost. In [7] authors have proposed alightweight encryption or decryption method, using timestamp technology, timeliness in the two communicationpartners is guaranteed.

III. PROPOSED ALGORITHM I

This is a two-way authentication scheme which makes use of Secure Hash Algorithm (SHA) technique. The proposed scheme is composed of three parts:

Two-way authentication scheme

A. *Initialization:*

During the phase of initialization, some necessary information like ID of the platform and terminal, their account information, keys, random number R_N are pre-distributed among terminal and platform node.

B. *CA Verification:*

There is a CA center that can be used to verify the identity of both the nodes securely.

C. *Two-way authentication:*

Step 1: Platform identity authentication:

According to Fig. 1, platform will send information to terminal which will include matrix password identifier, R_N and SHA(R_{N-1} || ACN), where R_N and R_{N-1} are random numbers. R_{N-1} is the random number generated in the last session. ACN is the account which is secret and only known to the platform and the terminal node.

When the terminal node receives the request for authentication, it will compute SHA1 (R_{N-1} || ACN) using SHA1 and compare the result with the received hashed information, if they match, the platform is legitimate otherwise the platform is considered to be illegal and the terminal will deny the request.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

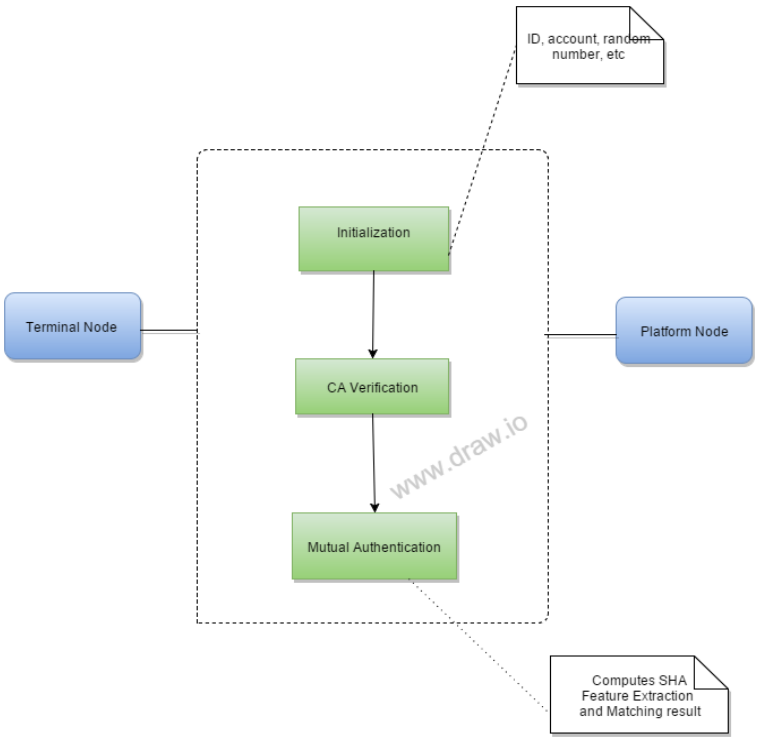

Fig 1. The Two way Authentication Scheme

Step 2: Terminal identity authentication

If the platform is authenticated, the R_{N-1} is updated with R_N, and then SHA1 will be computed followed by feature extraction. SHA1 is used to transform the authentication information (ID, account, etc.) to several messages having fixed length, and we regard these messages as non-objective image. Feature extraction will be used to compute reduced representation of the non-objective image and this will be sent to the platform.

When the platform receives the authentication information, according to the ID, it will know which terminal node want to be authenticated. Platform will then search for the corresponding information about this terminal node in its database. The platform performs same procedure as performed by the terminal and compares the result with received authentication information. If they matched, the terminal node is legitimate and authenticated. A link will be established and both will then continue the communication using dynamic cipher which is explained in our next algorithm.

IV. PROPOSED ALGORITHM II

Dynamic Cipher Key Generation

Dynamic Cipher key generation is based on the concept of one time pad. To have secure communication between two nodes (i.e. IOT device) encryption and decryption technique is used. A key Matrix is stored at clients and server location. After authentication of nodes by two-way authentication algorithm, the client sends request to server along with the coordinates of the key matrix that is stored at both the ends. The key thus used by the client is the one corresponding to the coordinates sent by the client.

Now only the server knows the key that is used for encryption. The key used for encryption is valid only for particular time period. This is achieved by setting time stamp. After the lapse of time set by the time stamp the key becomes invalid

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

and is replaced by a new key in the key matrix.

	1	2	3	4	5	6	7	8
1	2eqa	1wsx	3eds	1eqa	1ews	1xcv	2sdx	5red
2	1qaz	2wsd	2dcv	4dax	5tre	3wsx	7uyt	3ew1
3	2wqa	4waz	6ebv	4fds	6ter	3sxv	2dew	1ewt
4	6yhg	4rfd	3ert	3ewa	9iuy	7uyv	9oiu	2wqz
5	5ret	9iuy	7uyh	3xcv	7uyj	3edw	5rew	4rew
6	3wsa	7uyn	6trc	4rev	5fer	1qab	4rfd	2wsz
7	9ikj	7ytr	5trf	6oil	3dlo	7ujt	8iuy	5tre
8	2wsa	3wsa	8red	7red	6tre	4efr	6tre	8iuy

Table 1. Key Matrix

The client encrypts the data using the key. Encryption can be done by any technique according to client's choice. The client then sends the encrypted data to server. The server will now decrypts the data according with the key whose coordinates are shared by client. Hence there is secure communication between client and server. The key used by the client is deleted and replaced by a new key in the matrix. The new key is generated by appropriate randomize function. Since, the system is developed with respect to IOT devices, the size of the key matrix is kept as small as possible.

Thus the system diagram is shownin Fig. 2:

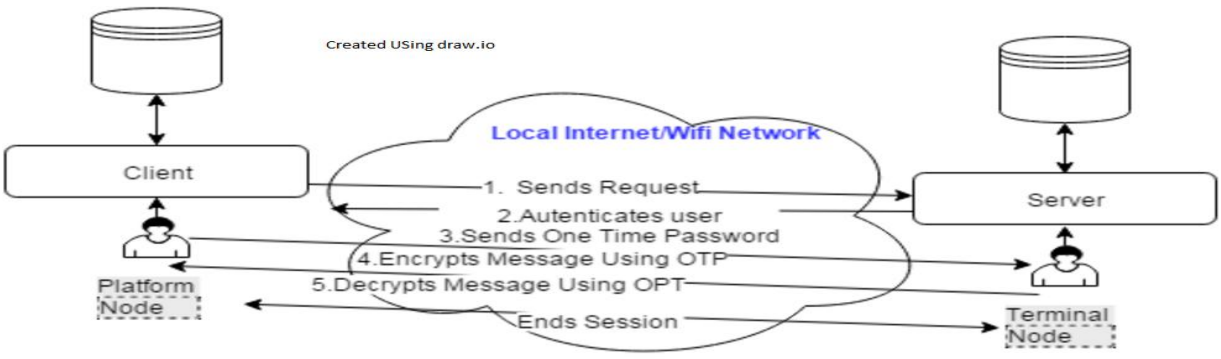

Fig 2. System Diagram

V. SIMULATION RESULTS

The work done till now is simulated in Contiki OS using COOJA simulator which is an open source simulator for IOT devices. The network Fig. 3 shows six motes i.e. nodes. Mote 1 is the server and rest are clients. The portion in green color depicts the radio environment and the range of the server. The mote which is highlighted using two red concentric circles is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

the mote which is active at particular time. The arrow connecting two motes depicts communication link between two motes. The mote output is shown in Fig 4. It shows time, mote id and the message which is transmitted from one mote to another mote during that time. From the mote output in Fig 4. the performance of the motes in wireless network can be analyzed. Further work includes introducing authentication and encryption-decryption using dynamic cipher within coojaand eventually comparing the performance of the present scheme and proposed scheme. The issue here is that cooja provides limited space for storage. Therefore, size of the key matrix required in dynamic cipher should be small. The storage space required by the key matrix are 8*8*8=256 Bytes. The communicating parties will randomly generate a coordinate from 1 to 16 bit length. Then according this coordinate, we will get a random password, and it's length can be 4 Bytes to 256 Bytes, so there are be 64!=1.26*1089 password in theory.

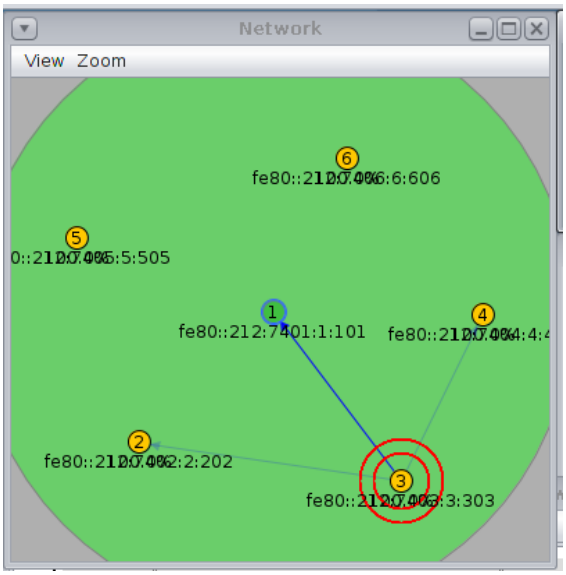

Fig 3. Nodes simulation network

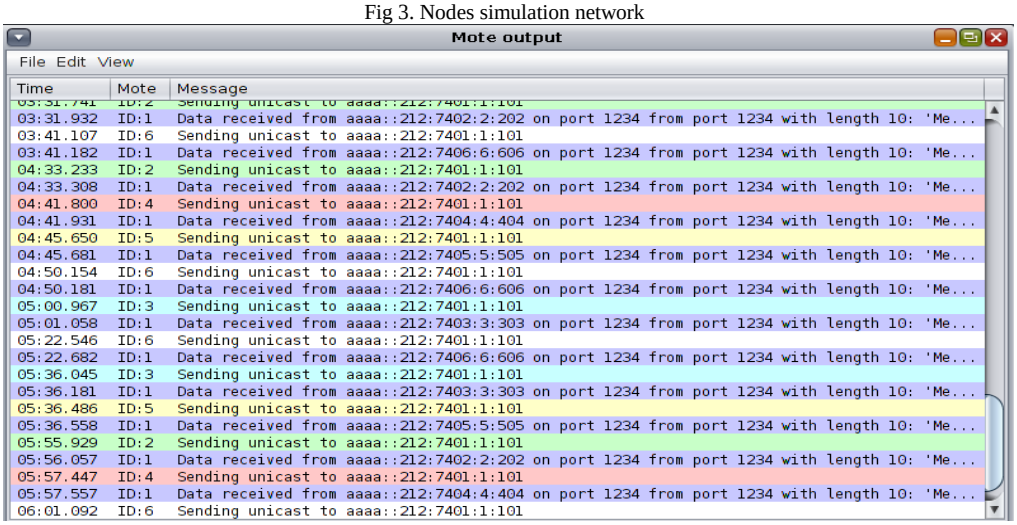

Fig 4. Nodes Output

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

VI.CONCLUSION

Secure communication between nodes by nodes authentication and dynamic cipher generation ensures safe and secure communication between nodes by implementing two-way authentication scheme between terminal node and platform which imposes light communication and computation cost. The authenticated parties then communicate using the lightweight encryption-decryption technique. This system helps to carry out secure communication between IoT devices. It not just takes care of its security but also its space. The system can be developed in Contiki operating system and can be simulated in Cooja. The system can be used by different IOT devices to carry out secure and safe communication.

REFERENCES

1. R. Kranenburg, "The Internet of Things: A critique of ambient technology and the all-seeing network of RFID," http://www.networkcultures.org/networknotebooks, 2008.
2. G. Zhao, J. Wang, J. Luo, X. Long, "Applicability of elliptic curve cryptography on Internet of Things," International Conference on Computer and Automation Engineering, 2011, vol.1, pp. 174-177.
3. Z. Benenson, N. Gedicke, O. Raivio, "Realizing robust user authentication in sensor networks,: in: Real-World Wireless Sensor Networks(REALWSN), 2005.
4. C. Jiang, B. Li, H. Xu, "An efficient scheme for user authentication in wireless sensor networks," in:21st International Conference on Advanced Information Networking and Applications Workshops, 2007, pp. 438-442.
5. C. Koner, P. Bhatacharjee, C. T. Bhunia, "A novel four entity mutual authentication technique for 3-G mobile communications," International Journal of Recent Trends in Engineering, 2009, vol.2, no. 2, pp.111-113.
6. G. Zhao, X. Si, J. Wang, X. Long, T. Hu, "A novel mutual authentication scheme for Internet of Things," 2011, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5973767.
7. Wen, Q, "Application of dynamic variable cipher security certificate in Internet of Things", 2012, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=666454sss