International Journal of Security and Its Applications
Vol. 11, No. 11 (2017), pp.53-66
http://dx.doi.org/10.14257/ijsia.2017.11.11.05

Securing Publish-Subscribe Services with Dynamic Security Protocol in MQTT Enabled Internet of Things

Adil Bashir and Ajaz Hussain Mir

Department of Electronics and Communication Engineering
National Institute of Technology Srinagar, Jammu & Kashmir, India
adilbashir.445@gmail.com

Abstract

Rapid developments in the field of embedded system, sensor technology, IP addressing and wireless communication are driving the growth of Internet of Things (IoT) in a variety of applications which include environment monitoring, smart manufacturing, e-health and smart agriculture. Due to heterogeneous and constrained nature of IoT nodes, many new security and privacy issues are introduced. IoT devices and systems collect a lot of private data about people, for example an intelligent meter knows when you are home and what devices you use when you are there. This data is shared with other devices and also stored in database or cloud server. Absence of security protocols for these resource constrained smart devices averts their widespread implementation. To address this problem, we propose a mechanism for securing application layer MQTT (Message Queue Telemetry Transport) protocol messages in IoT. The proposed security method for Internet of Things is lightweight in nature and suits well for resource constricted devices. The proposed method counters most of the likely confidentiality attacks in IoT.

Keywords*: Internet of Things (IoT), Message Queue Telemetry Transport (MQTT), MQTT-SN (for Sensor Networks), Data Distribution Service (DDS), Constrained Access Protocol (CoAP)*

1. Introduction

Internet of Things involves connecting physical objects to the internet, making them locatable and reachable remotely in the virtual domain [1, 2, 3]. Internet of Things (IoT) is regarded as the third wave of global information industry, steam-powered print technology and electronic communications being the other two in the list [4]. IoT is beginning to grow drastically, as consumers, business organizations and governments perceive the advantage of connecting inert devices to the internet. Approximately 20.8 billion connected things will be in use worldwide by the end of 2019, up 41 percent from 2017 and will reach 50 billion by 2020 [5]. The IoT will result in $1.7 trillion in value added to the global economy in 2019 [6]. IoT has distinct characteristics from those of existing Internet environments in a way that it is comprised of resource constrained devices, where the resources include CPU, memory, and battery.

To make IoT into a realization many key challenges exist, for example, security and privacy issues, client interaction, development of Application Program Interfaces (API) [7]. These challenges need to be addressed for widespread implementation and adoption of Internet of Things. Among the research challenges mentioned above, security and privacy issues are considered as obstruction for the adoption of IoT because there is no assurance that IoT will not detriment user privacy. This can be done by tailoring existing security protocols to make them suitable for resource constricted IoT nodes or develop

Received (July 10, 2017), Review Result (November 6, 2017), Accepted (November 16, 2017)

ISSN: 1738-9976 IJSIA

new protocols to protect vital sensed data from malicious users. Figure 1. Security Issues in IoT below depicts the major security challenges in IoT [8].

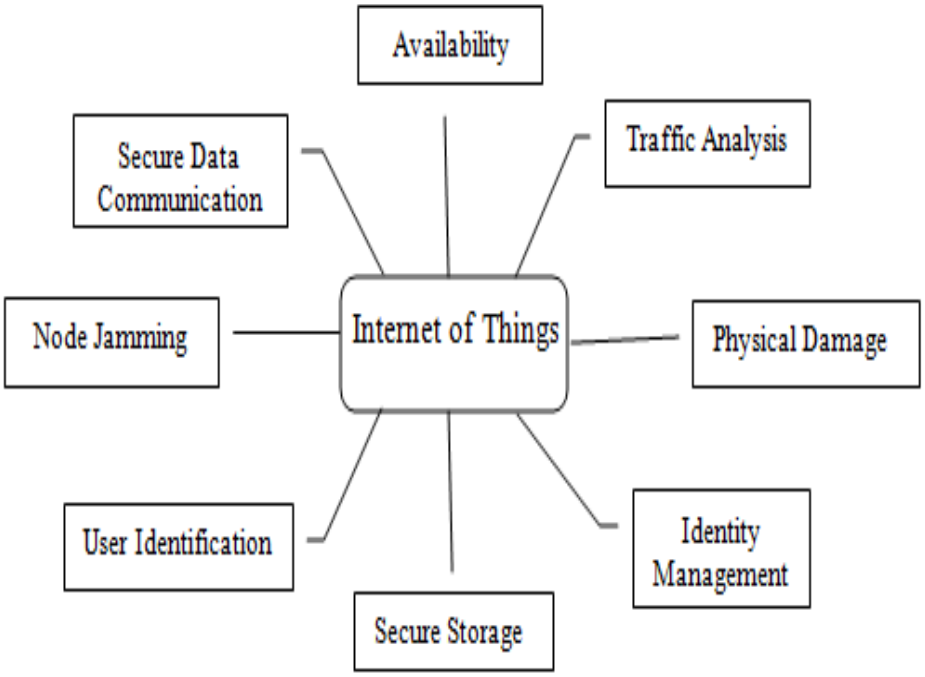

Figure 1. Security Issues in IoT

1.1. Availability

It is to ensure that illegitimate persons or devices cannot deny access or usage of IoT services to authorized users.

1.2. Traffic Analysis

Examining flow of messages in IoT network in order to obtain the information from communication patterns.

1.3. Physical Damage

Attacking the physical elements of IoT nodes, *e.g*. Node elements deterioration.

1.4. Identity Management

It deals with identifying things in IoT network and associating rights and limitations for every IoT device to use available resources. It also involves the process of identifying legitimate and illegitimate IoT nodes in a network.

1.5. Secure Storage

Designing and implementing security protocols to protect data left unattended at IoT nodes or at servers/cloud for secure storage.

1.6. User Identification

It involves developing methods for authenticating users to access IoT network by granting privileges and restricting access to unauthorized users.

1.7. Node Jamming

Attacker transmits data on same frequency as used by IoT so that error-free reception at receiver node is hindered.

1.8. Secure Data Communication

Protecting information in-transit from adversaries.

The protocols in Internet of Things are classified into four categories which include application layer protocols, service protocols, infrastructure protocols and other important protocols [9]. The application protocols used in IoT as categorized by [9] include Constrained Access Protocol(CoAP), Message Queue Telemetry Transport (MQTT), MQTT-SN (Message Queue Telemetry Transport for Sensor Networks), Data Distribution Service (DDS), Advanced Message Queuing Protocol(AMQP), Extensible Messaging and Presence Protocol (XMPP), HTTP REST, however these protocols are devoid of essential security features. From the survey on IoT application layer protocols, it has been found that MQTT and MQTT-SN are commonly used protocols than CoAP in applications like social networks, Vehicle to Vehicle communication (V2V) [10]. Authors in [11] evaluate the performance of MQTT and CoAP in terms of end-to-end transmission delay and bandwidth usage. From the comparative analysis in [11], it is observed that when the packet loss rate is low, MQTT deliver messages with lower delay than CoAP, but when the packet loss rate is high, CoAP outperforms MQTT. Similarly, the performance analysis of CoAP and HTTP is examined in [12] for energy consumption and response time.

MQTT distinguishes from HTTP in a way that it uses publish/subscribe architecture instead of request/response paradigm of HTTP [13]. Publish/Subscribe is event-driven and facilitates messages to be pushed to clients. The messages are being shared between publisher (sender) and rightful subscriber (recipient) through MQTT broker, which acts as a central point of communication. The client that pushes (publishes) a message to broker incorporates a topic into the message which acts as routing information for the broker. The client that wishes to get messages from the broker subscribes to a particular topic. Based on the subscribed topic, broker delivers all messages with matching topic to the subscriber. Therefore, the client nodes (publisher and subscriber) just talk/communicate over the topic without requiring to know each other. The publish-subscribe architecture of MQTT between clients and broker is shown in Figure 2. MQTT Publish/Subscribe Architecture.

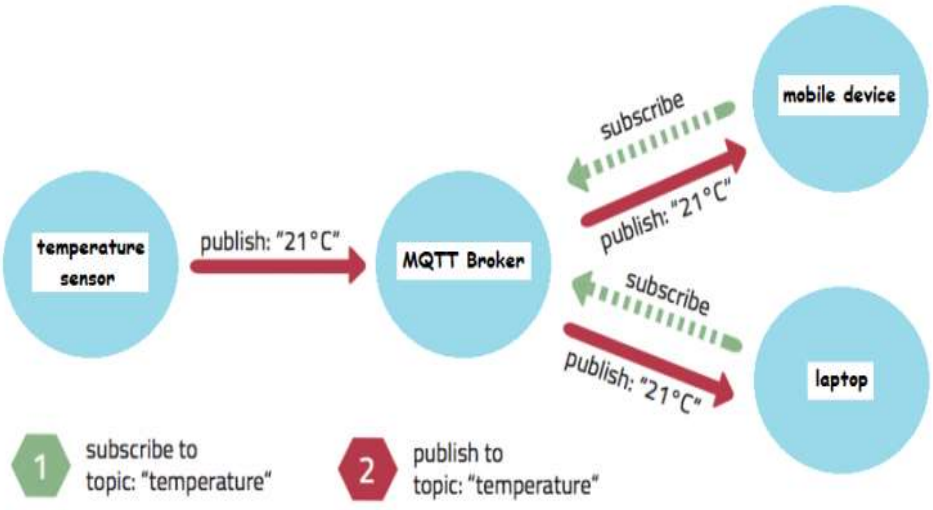

Figure 2. MQTT Publish/Subscribe Architecture

In this architecture, temperature sensor acts as publisher device that publishes sensed temperature to MQTT broker. Subscribers (mobile device and laptop) having subscribed temperature topic gets all the published messages on temperature topic from broker.

IoT enables physical objects with sensing, communication and actuating capabilities that bring many applications but a lot of problems as well, especially in terms of privacy and security. The main problem that hinders the usage of highly secure protocols in IoT is resource constrained nature of nodes in terms of CPU, memory and energy capabilities. Another issue in these devices is that most of the devices use wireless communication, which makes it easier for an attacker to intercept messages. To address these problems, we design a security mechanism for MQTT enabled IoT nodes that is less complex in nature and consumes minimum energy for cryptographic operations and at the same time provides effective message confidentiality.

The rest of paper is organized as follows. In Section II, we discuss related works that have been carried out to secure IoT network. Section III presents security attacks in IoT. In section IV, we discuss proposed security scheme. Section V presents the details of its hardware implementation. Finally, analysis of the proposed scheme is given in section VI and section VII concludes the paper.

2. Related Work

In [14], a security protocol for IoT has been designed in which device specific master key is imprinted in the devices which is fixed or static key. Then a challenge based shuffling algorithm is used at the client and server side to make the key dynamic. The point of concern here is that how client and server choose the same challenge for shuffling the key being distant/unknown to each other. Further, the dynamic session key is left exposed for a reasonable amount of time during which an attacker can easily decipher the messages that can lead to compromisation of the entire network.

Authors have used Attribute Based Encryption (ABE) scheme to ensure security of Publish-Subscribe (Pub-Sub) architecture based IoT [15]. To encrypt messages, symmetric Advance Encryption System (AES) cryptography is used and the AES key itself is encrypted using ABE scheme. Since most of the IoT devices have limited resources and generate smaller number of data bits, therefore using highly computational AES and ABE cryptographic techniques in IoT devices is not suitable. In [16], security of published content and the privacy of client's (subscriber's) interested topics are protected using Predicate Based Encryption and CP-ABE.

A "Peer to Peer security Protocol for IoT" has been proposed in [17] in which messages are secured from malicious attacks using P2P security system. However, in this algorithm, there are a number of messages exchanged between client and authority node due to which the designed algorithm consumes lot of device energy, therefore making it energy inefficient.

An authentication and confidentiality mechanism has been designed in [18] to allow publishing clients to sign and encrypt events at the same time. The developed mechanism uses IBE (Identity Based Encryption) and ABE schemes, therefore enable efficient routing of encrypted events. On the other side, subscribers verify the signature of an event using CP/KP-ABE.

In [19], author has proposed a hybrid encryption technique for securing messages in IoT devices. However, the encryption algorithms used are AES and ECC which are computationally complex and energy draining algorithms and hence not suitable to be used for resource constrained IoT devices.

3. Classification of Security Attacks in IoT

IoT devices and network are vulnerable to various kinds of attacks because of wireless communication medium used and inherent scarce resources. It is imperative to know the types of attacks that are likely to harm IoT, so as to design appropriate solutions. Depending upon the type of resources being harmed, three broad categories of attacks have been identified which are Physical attacks, Encryption attacks and Network attacks. Each of these categories of attacks are discussed below [20].

3.1. Physical Attacks

These attacks harm the hardware components of IoT system affecting their lifetime and functionality. In this type of attack, adversary needs to be physically close to or inside IoT network to launch the attack. IoT devices suffer from the following types of physical attacks.

3.1.1. Jamming Attack

Assailant interferes with the communication frequencies of IoT devices thereby, jamming the signals and breaking down communication among nodes. The services of entire IoT network is disrupted if the communication of key nodes is jammed [21].

3.1.2. Node Tampering

In this type of physical attac, sensitive information at nodes is accessed and modified by adversary after gaining physical access of the node [22].

3.1.3. Malevolent Node Addition

The information flow among IoT devices can be intercepted by adversary after injecting false nodes in the network.

3.1.4. Physical Damage

Attacker harms the electronics and hardware components of IoT devices physically so as to disrupt the working of IoT system, thereby affecting the services and operation of IoT network and devices.

3.2. Encryption Attacks

These assaults affect IoT network by breaking down the encryption mechanisms applied in IoT system.

3.2.1. Side channel Attacks

In this attack, the cryptographic keys used in security protocols are retrieved using techniques like Fault, Timing, Power and Electromagnetic analysis on the encryption devices of an IoT system.

3.2.2. Man-In-the-Middle Attack

The messages exchanged during key generation process are captured by attacker by which he is able know the final key shared between two communicating entities, such as in Diffie-Hellman key exchange mechanism. The attacker can then encrypt/decrypt data from sender and receiver and inject false data also.

3.3. Network Attacks

These assaults differ from physical assaults in a way that the attacker doesn't need to be physically close to devices and IoT network but can launch attacks remotely.

3.3.1. Traffic Analysis Attacks

An assailant can examine and intercept confidential messages to deduce patterns and information in communication [23]. Attacker first launches sniffing attack to obtain network information. To do this sniffing applications like port scanning, packet sniffer *etc.* are used.

3.3.2. Sinkhole Attack

The service of entire IoT network is altered by fake routing advertisement and then dropping all packets to the compromised node. Such an attack has impact on confidentiality of data as well [24].

3.3.3. Denial of Service Attack

In this attack, adversary injects false traffic to overload the network and keep channels busy. This results in disrupting the services of network.

3.3.4. Routing Information Attack

Such attacks influence routing information by creating routing loops, dropping packets, extending or shortening routes [25]. For example, Blackhole attack, Hello Attack [26].

3.3.5. Sybil Attack

In this type of attack, a malevolent node forges identity of legitimate node and thus leads to network compromisation. For example, an IoT based voting system is created where a Sybil node casts its vote more than once [27].

4. Proposed Security Mechanism

In this section, we discuss the proposed method for securing MQTT messages between publisher and subscriber from malicious users. Objective of the proposed method is to safeguard critical data from adversary by applying an energy efficient and secure algorithm. Being energy efficient algorithm, it provides the longevity of IoT devices by consuming less energy of nodes for cryptographic operations.

4.1. Network Scenario

IoT devices are intelligent devices equipped with sensing and communication capabilities by which they interact and collaborate with other smart things. Whenever an IoT device senses an event, it starts publishing the sensed information to MQTT broker. After receiving information from publisher, MQTT broker sends it to subscribers based on their subscribed topic. The subscriber may actuate an output unit to perform its assigned task and then further publishes information to other subscribers and this way chain of events start to occur. For example, an arm band (bracelet) senses sleep cycles of a person and then wakes him up gracefully at the specified time and when it happens the arm band sends messages to other devices at home and pretty sooner, the chain of events start to occur, for instance, Air conditioner (AC) turns on automatically, and then the coffee maker starts and so on. Therefore, the data sensed by bracelet is published to AC

which then initiates other events. This is represented in Figure 3. Chain of Events in IoT below.

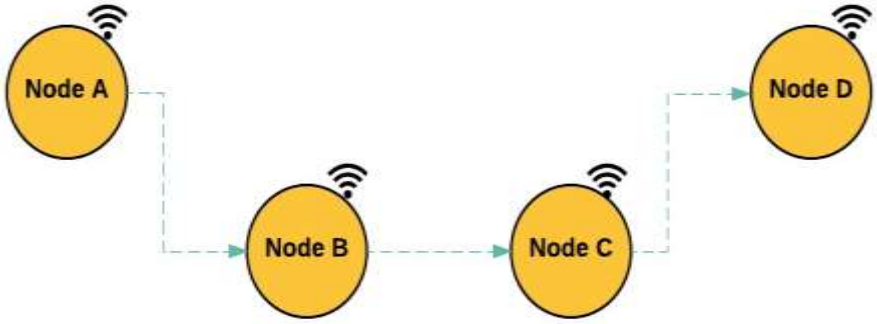

Figure 3. Chain of Events in IoT

In Figure 3, node A senses an event which is published to node B using MQTT broker. Node C gets the subscribed information only after node B has received its subscribed information and likewise the chain of events start occurring and each IoT device performs its task after receiving subscribed information on the topic from MQTT broker.

4.2. Method

- Publisher has data to be transmitted to subscriber(s). Publisher generates a key 'K' with which data is encrypted using lightweight cryptographic algorithm such as CLEFIA [28], PRESENT [29] or invertible logical operation i.*e.* XOR. Our method employs XOR operation being simple and lightweight in nature.
- K is generated using Pseudo-Random Number Generator (PRNG) that is designed using system time. 'K' is dynamic in a way that it changes its value periodically after some time interval. Whenever an attacker comes close to conjecture the value of K, it gets changed, hence rendering the value of K as doubtful for adversary.
- Designed method provides best security services to MQTT enabled IoT devices in both cases *i.e.* when data is left unattended at IoT nodes and when data is in-transit. In the first case, sensed data is protected from attackers by repeating encryption-decryption cycles at random time intervals to encrypt data at nodes by newly generated dynamic key, till the data is published to broker. During the interval in which data is left exposed, *i.e.* the time between decryption and re-encryption of data, it is ensured that no attacks occur and a safe time interval is maintained, the details of which is presented later in this section. In the second case *i.e.* data in-transit, the sensed information is encrypted using a random key generated by PRNG, thereby making it difficult for adversary to guess the value of key 'K' at a particular instant of time.

4.3. Algorithm

XOR operation has been chosen as an encryption operation because it is computationally simple to perform, but is not itself secure enough to prevent vital information from attacks, thus the key 'K' is made dynamic by changing its value periodically to reduce the chances of various attacks like brute force attack. The algorithm used for encrypting sensed information at publisher device is:

Algorithm A:

Step 1: Use system time dependent Pseudo-Random Number Generator (PRNG) to generate a random number (T_1) by applying seed X_1 (T_1 acts as an encryption key).
Step 2: Encrypt data (P_1) sensed by IoT node using T_1.

$$C_1 = P_1 \text{ XOR } T_1$$

Step 3: Publish C_1 to MQTT broker.
The algorithm that is used at subscriber side is:

Algorithm B:

Step 1: Use system time dependent Pseudo-Random Number Generator (PRNG) to generate a random number (T_1) by applying seed X_1 (T_1 acts as decryption key).
Step 2: Decrypt C_1 using T_1.

$$P_1 = C_1 \text{ XOR } T_1$$

Subscriber decrypts the message received from MQTT broker and performs the assigned task based on the message contents and can further publish for other subscribers in the chain of event scenario as defined in section 4.1 above. If the subscriber wants to publish messages further, Algorithm A is repeated to encrypt messages before publishing to broker as shown below in steps 3-5.
Step 3: Use system time dependent Pseudo-Random Number Generator (PRNG) to generate a random number (T_2) by applying seed X_2 (T_2 acts as an encryption key).
Step 4: Encrypt data (P_2) using T_2.

$$C_2 = P_2 \text{ XOR } T_2$$

Step 5: Publish C_2 to MQTT broker.
If the node is left unattended, Algorithm A and Algorithm B are executed after random intervals till the data is published.

4.4. Safe Time Interval Calculation

Calculating the time period during which sensitive information is left exposed is shown in this section and the method adopted is similar to that in [30]. The key length of 'K' is taken as 128-bit, so as to diminish the probability of brute force attack and to reduce time gap. Therefore, number of possible values of:

$$K= N = 2^{128} * (1 \div 2) = 3.40*10^{38} * (1 \div 2)$$

'N' also represents the number of conjectures needed by an assailant to guess the value of 'K' using brute force method. Hence, the probability that the assailant conjectures value of 'K' is:

$$K = G = 1 \div (3.40\times 10^{38}\times (1 \div 2))$$

Therefore, it is found that the possibility of predicting the value of 'K' is very low. Assume that, an assailant takes time 't' to make one guess operation, then the time 'T ' needed to make 'N' conjectures is

$$T= 3.40\times 10^{38}*(1 \div 2) * t$$

Hence, the time-gap after which 'K' should be altered is 'T'. The time period during which the value of K is changed and the information is left unencrypted, a safe time warp, will practically be T-x, where 'x' is the time taken to change K and re-encrypt the data.

5. Implementation

An experimental setup is developed to implement the proposed mechanism and algorithm which consists of IoT nodes as publisher-subscriber and Raspberry Pi as MQTT broker. The view of IoT node is shown in Figure 4. IoT Node below.

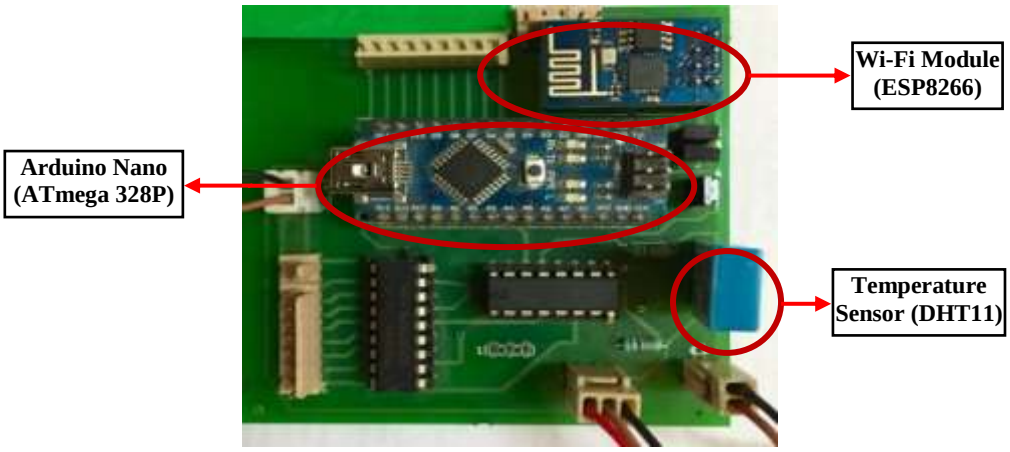

Figure 4. IoT Node

The PCB diagram shown in Figure 4 above represents IoT node which has a temperature sensor attached to it in addition to the arduino nano as one of the essential components and is equipped with Wi-Fi device for communication purpose. This is used as client IoT device which acts as publisher and subscriber. Raspberry Pi is used as MQTT server (broker) which receives published messages on the given topics from publishers and relays them to rightful subscribers. The view of MQTT broker is shown in Figure 5. Raspberry Pi2 Model B.

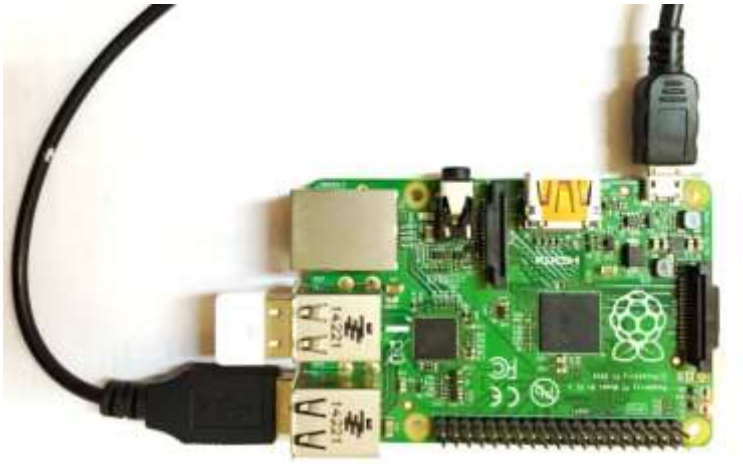

Figure 5. Raspberry Pi2 Model B

The microcontroller (Atmel Mega 328P) on the arduino board is programmed using arduino programming language (embedded C functions) in arduino software (IDE) to implement MQTT client and the proposed security method. Block diagram of the client node is shown in Figure 6. Block diagram of node.

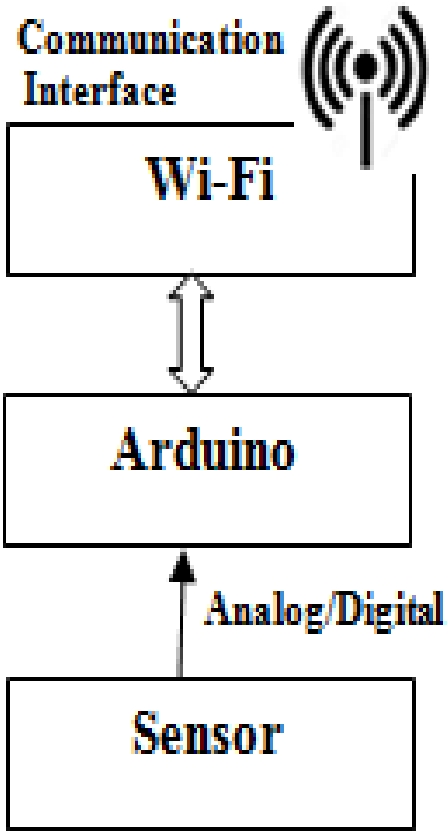

Figure 6. Block Diagram of Node

6. Analysis of Proposed Scheme

6.1. Security Analysis

A compromised node is added to IoT network that acts as an attacker. The brute force algorithm is implemented in it so as to check the vulnerability of our proposed algorithm to brute force attack. The temperature sensor attached to IoT node senses temperature which is then encrypted by dynamic key 'K'. This encrypted information is consistently sent to adversary node which then tries to decrypt the information by launching brute force attack. The information is sent after the interval T (time gap between the $(n+1)^{th}$ encryption and n^{th} encryption).

From the experimentation, it has been found that the attacker is unable to decrypt the information even once as the key 'K' gets changed dynamically. The key size can be made large to increase T, *e.g.* an adversary able to process 10^6 decryptions per second takes 10.01 hours to conjecture the correct key [31].

6.2. Performance Analysis

6.2.1. Time Complexity

The time complexity defines the time taken by an algorithm to perform its task. Using the concepts from Analysis of Algorithms, the time complexity of the designed algorithm is calculated below:

$$T(n) = 6 * O(1) + 2 * O(11) + 8 * O(10) + 4 * O(1)$$

As T is small, therefore the time complexity becomes constant. It implies that the encryption time taken by proposed algorithm is constant.

6.2.2. Storage Requirements

The storage requirement of the implemented security algorithm is found to be approximately 322 bytes which is a small value and is affordable by IoT nodes. Due to less storage requirements, there is a provision to increase the key size to make the algorithm stronger against attacks.

7. Conclusion

The constraints in IoT devices and the nature of wireless communication system pose critical security and privacy concerns. Complex symmetric cryptographic protocols such as AES have been used in the literature but implementing these protocols for IoT involves lot of overhead. Most IoT devices have limited resources that include computational power, storage space and battery capabilities, therefore, it is impractical to employ asymmetric cryptographic schemes such as RSA, ECC for IoT nodes.

The proposed scheme considers inherent constraints of IoT nodes and provides lightweight cryptographic solution to secure messages from malicious users in IoT network. Based on the analysis of implemented algorithm, it is concluded that the proposed model is efficient in terms of storage space and security and is resilient to brute force attack. The implemented cryptographic algorithm has low computational overhead and thus consumes less energy for encrypting the data. Since 80% of the node energy is utilized in communication tasks and most of the security algorithms need to exchange extra messages in key establishment phase, therefore consuming significant node energy. However, the proposed scheme saves this energy by reducing such an overhead. Therefore, the developed security solution delivers better security and also consumes feeble amount of node energy, hence improving the IoT device lifetime.

As part of our future work, we continue to work on security aspects of MQTT using dynamic key cryptography such as using lightweight algorithms CLEFIA [28] or PRESENT [29] instead of XOR operation. Improving random number generator is another opportunity to make this algorithm more efficient such as generating random signal from physical sources of white noise in transistors or from thermal noise.

References

[1] R. Roman, P. Najera and J. Lopez, “Securing the internet of things”, Computerhttp://dx.doi.org/10.1109/MC.2011.291, vol. 44, no. 9, **(2011)**, pp. 51–58.
[2] R. Roman, J. Zhou and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things”, Computer Networkshttp://dx.doi.org/10.1016/j.comnet.2012.12.018, vol. 57, no. 10, **(2013)**, pp. 2266–2279.
[3] S. Sicari, A. Rizzardi, L. Grieco and A. Coen-Porisini, “Security, privacy and trust in internet of things: the road ahead”, Computer Networkshttp://dx.doi.org/10.1016/j.comnet.2014.11.008, vol. 76, **(2015)**, pp. 146–164.
[4] C. Qinglin, “Review of Research on the Internet of Things”, Software Guide, vol. 9, no. 5, **(2010)**, pp. 6-7.
[5] Stamford and Conn., http://www.gartner.com/newsroom/id/3165317, **(2015)**.
[6] J. Greenough, http://www.businessinsider.in/The-Internet-of-Things-Will-Be-The-Worlds-Most-Massive-Device-Market-And-Save-Companies-Billions-Of-Dollars /articleshow/44766662.cms, **(2014).**
[7] A. Kanuparthi, R. Karri and S. Addepalli, “Hardware and embedded security in the context of internet of things”, Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles, **(2013)**, pp. 61-64.
[8] S. Barber, P. Mahalle, A. Stango and N. Prasad, “Proposed security model and threat taxonomy for the internet of things”, Recent Trends in Network Security and Applications, Springer Berlin Heidelberg, **(2010)**, pp. 420-429.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Communications Surveys & Tutorials, vol. 17, no. 4, **(2015)**, pp. 2347-2376.
[10] E. G. Davis and A. Calveras and I. Demirkol, "Improving packet delivery performance of publish/subscribe protocols in wireless sensor networks", Multidisciplinary Digital Publishing Institute, vol. 13, no. 1, **(2013)**, pp. 648–680.
[11] D. Thangavel, X. Ma, A. Valera, H. X. Tan and C. K. Y. Tan, "Performance evaluation of MQTT and CoAP via a common middleware", Proceedings of IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, **(2014)**, pp. 1-6.
[12] W. Colitti, K. Steenhaut, N. De Caro, B. Buta and V. Dobrota, "Evaluation of constrained application protocol for wireless sensor networks", Proceedings of IEEE Workshop on Local & Metropolitan Area Networks (LANMAN), Chapel Hill, NC, **(2011)**, pp. 1-6.
[13] http://www.hivemq.com/blog/how-to-get-started-with-mqtt.
[14] S. Mishra, "Network security protocol for constrained resource devices in Internet of things", Proceedings of Annual IEEE India Conference (INDICON), New Delhi, **(2015)**, pp. 1-6.
[15] X. Wang, J. Zhang, E. M. Schooler and M. Ion, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT", Proceedings of IEEE International Conference on Communications (ICC), Sydney, NSW, **(2014)**, pp. 725-730.
[16] P. Pal, G. Lauer, J. Khoury, N. Hoff and J. Loyall, "P3S: A Privacy Preserving Publish-subscribe Middleware", Proceedings of the 13thInternational Middleware Conference, ser. Middleware, **(2012)**, pp. 476–495.
[17] H. Zhang and T. Zhang, "Short Paper: 'A peer to peer security protocol for the internet of things': Secure communication for the sensible things platform", Proceedings of 18th International Conference on Intelligence in Next Generation Networks, Paris, **(2015)**, pp. 154-156.
[18] M. A. Tariq, "Non-functional Requirements in Publish/Subscribe Systems", Ph.D. dissertation, Universitat Stuttgart, Fakultat Informatik, Elektrotechnik und Informations technik, Germany, **(2013)**.
[19] M Xin, "A Mixed Encryption Algorithm used in Internet of Things Security Transformation System", Proceedings of International conference on cyber-enabled distributed computing and Knowledge Discovery, DOI 10.1109/CyberC.2015.9, **(2015)**.
[20] I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges", IEEE Symposium on Computers and Communication (ISCC), Larnaca, **(2015)**, pp. 180-187.
[21] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs", IEEE Communications Surveys & Tutorials, vol. 11, no. 4, **(2009)**, pp. 42-56.
[22] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks", Communications of the ACM47, no. 6, **(2004)**, pp. 53-57.
[23] B. Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy", Proceedings of International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, **(2011)**, pp. 709-712.
[24] V. Soni, P. Modi and V. Chaudhri, "Detecting Sinkhole attack in wireless sensor network", International Journal of Application or Innovation in Engineering &Management, vol. 2, issue 2 **(2013)**, pp. 29-32.
[25] D. Wu, G. Hu and G. Ni, "Research and Improve on Secure Routing Protocols in Wireless Sensor Networks", Proceedings of IEEE International Conference on Circuits and Systems for Communications, Shanghai, **(2008)**, pp. 853-856.
[26] M. A. Hamid, M. Mamun-Or-Rashid and C. S. Hong, "Routing security in sensor network: Hello flood attack and defense", IEEE ICNEWS, **(2006)**, pp. 2-4.
[27] [27]J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses", Proceedings of 3rd international symposium on Information processing in sensor networks, **(2004)**, pp. 259-268.
[28] Sony Corporation CLEFIA official webpage.http://www.sony.net/Products/cryptography/clefia/.
[29] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin and C. Vikkelsoe, "PRESENT: An Ultra Lightweight Block Cipher", Workshop Cryptographic Hardware and Embedded Systems (CHES 07), LNCS 4727, Springer, **(2007)**, pp. 450-466.
[30] A. Bashir and A. H. Mir, "An energy efficient and dynamic security protocol for wireless sensor network", Proceedings of International Conference on Advanced Electronic Systems (ICAES), *Pilan*i, **(2013)**, pp. 257-261.
[31] Cryptography and Network Security Principles and Practice 4th Edition, William Stallings, **(2005)**, pp. 66, table 22.

Authors

Adil Bashir, he received his Bachelor of Technology (B.Tech) in Computer Science and Engineering from Islamic University of Science and Technology, Jammu & Kashmir, India in year 2011. He has done his Master of Technology (M.Tech) in Communication and Information Technology from National Institute of Technology (NIT) Srinagar, India in 2013. Presently he is a research scholar at NIT Srinagar in the Department of Electronics and Communication. His research interests are Internet of Things, Wireless Sensor Networks, Embedded Systems and Network Security.

Ajaz Hussain Mir, he has done his Bachelor of Engineering (B.E) in Electrical Engineering with specialization in Electronics & Communication Engineering (ECE). He did his Master of Technology (M.Tech) in Computer Technology and PhD both from IIT Delhi in the year 1989 and 1996 respectively. He is Chief Investigator of Ministry of Communication and Information Technology, Govt. of India project: Information Security Education and Awareness (ISEA).

Presently, he is Professor in the Department of Electronics & Communication Engineering at NIT Srinagar, India. He has been guiding PhD and M.Tech thesis in Security and other related areas and has a number of International publications to his credit. His areas of interest are Biometrics, Image processing, Security, Wireless Communication and Networks.