International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 7; Issue 3(J); March 2018; Page No. 11108-11112
DOI: http://dx.doi.org/10.24327/ijcar.2018.11112.1914

Research Article

SECURE ANONYMOUS ROUTING SCHEMES FOR INTERNET OF THINGS

Nagavalli S[1*]., Ramachandran G[2] and Saminathan R[2]

[1]Department of Computer and Information Sciences, Annamalai University Annamalainagar-608 002, Tamil Nadu, India
[2]Department of Computer Science & Engineering, Annamalai University Annamalainagar-608 002, Tamil Nadu, India

A R T I C L E I N F O

Article History:

Received 16th December, 2017
Received in revised form 20th January, 2018 Accepted 4th February, 2018
Published online 28th March, 2018

Key words:

IoT, Anonymous authentication, Secure routing, AVISPA

A B S T R A C T

In recent times Internet of Things (IoT) are deployed in a complex environment where the wide range of complex applications are mandatory for the services. The complex application includes various domains such as military, agriculture, healthcare, defense, monitoring, surveillance etc. In general, IoT sensors are spatially distributed and deployed in remote fashion, usually they are powered up by batteries through the external supply. Further, the security components of such devices are very minimal due to their various constrains. Hence, the major constrain of such technology fails to provide complex services where the uncertainty plays a major role. In order to addresses the above stated problem, this paper propose a novel anonymous authentication protocol. The experimental result shows that the proposed protocol is robust and the results obtained are satisfactory.

Copyright©2018 ***Nagavalli S., Ramachandran G and Saminathan R.*** *This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.*

INTRODUCTION

Internet of things (IoT) is the collection of things armed with sensors and power that enables them to deploy for the scenario of wireless networks. The main backbone of IoT is the high influence towards the day-to-day aspects of user's behavior. It enables physical devices (things) to communicate with each other's, transfers and recover data, activates events and decisions [7][10]. IoT transforms these objects to a smart model by manipulating technologies like pervasive computing, sensor networks, and Internet protocols. The device need to be suitable for customer necessity in terms of anywhere and anytime availability [16][17].

The element of IoT is signified as simple equation: *IoT = User+ Physical devices (sensors, controllers, storage) + Internet.* The common applications based on IoT includes: smart home and cities, agriculture, smart consumer wearables, smart utilizes, transport and logistics, food monitoring, tele-medicine [11]. The technologies include RFID, Near Field communications (NFC), Machine-to-Machine (M2M), Vehicular to Vehicular communications (V2V) [9] which is used to implement IoT and make the users easy and comfortable [1].

Corresponding author:* **Nagavalli S
Department of Computer and Information Sciences, Annamalai University Annamalainagar-608 002, Tamil Nadu, India

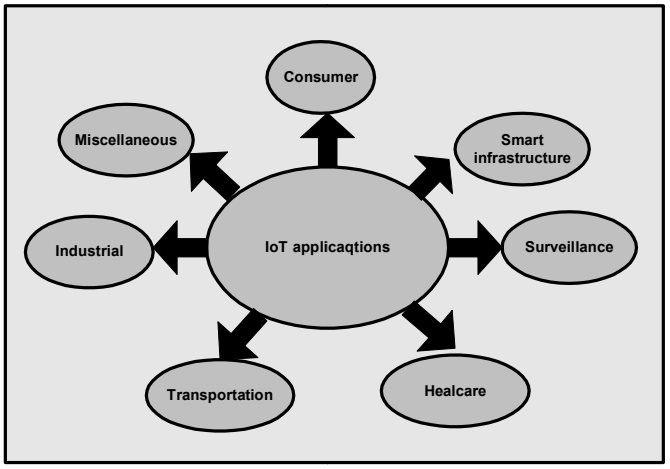

Fig 1 Applications Domains of IoT

IoT has a significant role in home and business based applications to donate the quality of life and to grow the world economy. In order to understand the possible growth and inventions, applications yet to grow to meet the customer expectations and market demands [13]. The vision of IoT is contained with wide scale of ability across multiple domains which bring challenges in data format representation, data managements and also cooperative support that manages various types of data generated from different sources beneath different administrations. Processing large scale of datasets in IoT based on statistical and computational algorithm is challenging in real-time point of view [2]. The IoT system is included number of functional blocks such as device,

communications, service, managements, security and applications.

IoT is a technology with high claim because of its various essences, intelligence, and mobility but still they are defenseless in terms of security [14][15]. Drastically increase of IoT device due to evolving new techniques in area of electronics and computer science provide service with less human interaction. As a side effect, number of attacks has been increased in contrast with security and threats which lead to addressed them in depth to greatly develop secure smart devices [4]. Security is an ongoing research which pays attention in academic, industrial and governmental sectors. Security in term of IoT takes place in numerous cases based on technical, ethical and secrecy concerns. Set of necessities to be consider by IoT devices for considering secure connections includes: secure authentication to access data by certified person, secure data encapsulation, broadcast data with secured IoT devices, suitable secure key algorithms, physical secure sign [3]. Resources like CPU and memory management are classically constrained which is built on IoT devices is challenging in the area of energy computation mode of operation. Hence, this paper proposes a light weight authentication protocol. The proposed protocol is robust and resilience enough to have a secure exchange between the devices.

The contribution of this paper is as follows:

- A strong mutual authentication mechanism to authenticate devices at end points
- Anonymous data routing with decentralized architecture
- No generic broadcast which leads to zero knowledge proof which is practically impossible for an attacker to perform masquerading attacks.

LITERATURE SURVEY

Ayman *et al*. proposed a novel secure routing scheme [5] for IoT networks with SISLOF as a objective function. Their method utilized a modified RPL routing protocol. They measured performance of the key pre-distribution in the context of the Internet of Things when SISLOF is used as the Objective Function of the RPL routing protocol. However, the author's method fails due to the overhead of internal routing table generation. Further, it is very difficult to manage the storage space of the occupied routing tables.

Kamble *et al*. surveyed the security weakness [6] of the benchmarked routing protocol RPL which is widely used in the IoT platforms. Here the authors studied the entire weakness of the protocol and analyzed the susceptibility of the protocol under various attacks. The authors analyzed that the fundamental enabling factor for the successful deployment and use of most IoT applications.

Airehour *et al*. studied about various robust secure routing algorithms for IoT devices. In their survey they focused mainly on security that will pose a fundamental enabling factor for the successful deployment and use of most IoT applications and in particular secure routing among IoT sensor nodes thus, mechanisms need to be designed to provide secure routing communications for devices enabled by the IoT technology. Further, they analyzed the existing routing protocols and performed various tests over the protocol in order to evaluate the efficacy of the protocols.

From the literature, it is studied that the existing system suffers with incorporating End-to-End security in hardware infrastructures such as switches, routers etc. Further, the hardware components used in the present day conventional networks are deterministic packet switches which cannot be operable when there is a strategic attack. Further, the design of such hardware switches are immutable in nature which fails to adapt when there is an attack. Recent advancement in cryptographic techniques also fails due to their light weight encryption standards and the length of the verification keys used were also very long in length. However, there is no protocol reported that they ensure anonymity in their communication. Further, there is no proof that the communication cannot be interceptable by any strong attacks. Hence, there is a need for a secure anonymous communication protocol.

Anonymous Mutual Authentication Model (AMAM)

The proposed AMAM protocol consists of three main phases. First phase implicates the security assumption and design goals. Second phase enables a strong mutual authentication among each node in the network. Finally, the third phase implicates the Peer to Peer encryption protocol.

Security assumption and design goals

As per the regulation of the pervasive environment, the IoT devices are free and liable to move. Hence a node can move freely, leave or join the network at any time dynamically. Further, each device will hold a separate address for their public and private communication. The design goal of the proposed AMAM model is to resist the attacks from the malicious adversaries. Further, the security implication reflects that the proposed AMAM model is resistance enough to withstand the compromise and if any compromise is found within the network, the compromise should not affect the other node in terms of performance.

Mutual authentication mechanism to authenticate each nodes in the network

In this phase, a strong mutual authentication mechanism is incorporated. Here a Diffie- Hellman algorithm is used to achieve the mutual authentication. The structure of each session during their broadcast is formed as a data structure which is assumed to zero knowledge proof. Hence, identifying this data structure is a hard task. The data structure used for session broadcast is as shown below.

$$[label, session_{prikey}, next_{pubkey}, sequece, dIP$$

$$label^{-}, sIP, source\_, source\_pubkey]$$

End to end encryption mechanism with anonymous routing

In this phase, a strong end to end encryption Double Ratch*et al*gorithm is included in order to achieve the encryption link between the devices which communicates.

Access Control Systems

The proposed AMAM consists of Access Control Systems (ACS) which is responsible for keeping track of nodes. ACS are flexible permission granting system for different level of authorities based on the roles and attributes (for data transfer).

How AMAM works

The structure of the broadcast is shown above. The first field is a unique session id. It is used in the route request phase where the temporary public key of each node (second field) that relay on the packet and the third field is not used. In the route reply phase, the second field is the session private key, and the third field is the next node's temporary public key. Once the exchange is completed the join handshake is performed among the neighbors. The data in these two fields are encrypted, and their function is to find an anonymous link among intermediated nodes.

The fourth field records a random number shared between the source node and the destination node. The fifth field records the IP of the destination node. The sixth field records the session private key. The seventh field records the IP of the source node. The eighth field records the signature of the source node's IP address. The ninth field records the public key of the source node. All the data in fields 4 - 9 are encrypted by the receiver's long-term public key.

Each node sets up a route table and a spare route table after it receives a valid reply packet. These two tables have the same structure. Route table is to record the preferred neighbor node, which can relay the packet, and spare route table is to record all the other neighbor nodes.

Experimental Setup

The proposed AMAM is implemented on CENT OS with Intel Xeon processor and 28 GB RAM. The nodes are deployed independently to monitor the water tank which contains shrimps. Each node is executed to run AMAM protocol in order to ensure that each node communication is encrypted. A checksum is created and certificate pinning is also ensured in all nodes in order to verify the authenticity of nodes and to avoid the node cloning activities.

The entire framework is implemented using Python and the monitoring framework is deployed in AMAZON AWS, thus by setting up a private cloud using a 64bit Amazon Linux 2015.09 v2.0.8.

Performance analysis

In this section, the performance of the proposed AMAM is evaluated. The experimental setup of AMAM is demonstrated using 10 nodes and 2 server nodes.

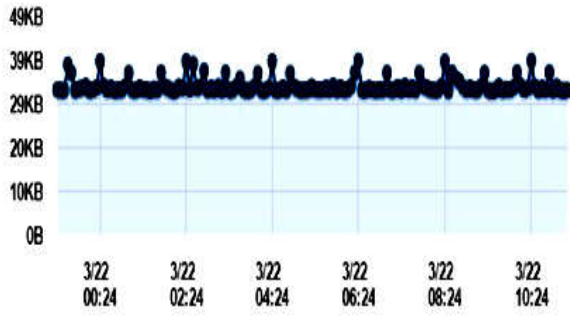

Fig 2 CPU utilization in percentage

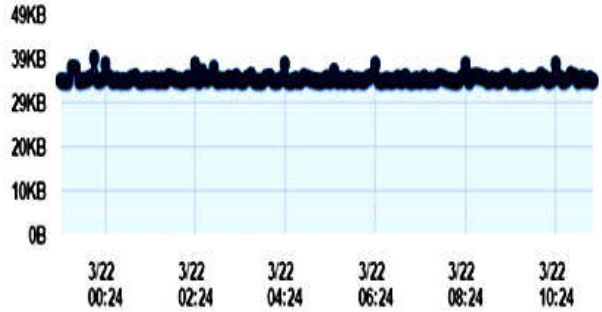

Fig 3 Max Network IN *in* bytes

Amazon Web Service (AWS) is a collection of remote computing services [12]. AWS offers infrastructure (IaaS) with provision for Amazon EC2 (Elastic Compute Cloud) instances. EC2 instances basically provision VMs that can run any software application. They are offered in different sizes and types from "t1.micro" to "h1.4xlarge" with one core and 612 MB of memory to 16 cores and 60 GB of memory. Any types of instances can be launched in Amazon Machine Images (AMIs) which contains preconfigured OS, software packages, libraries and tools based on user choice.

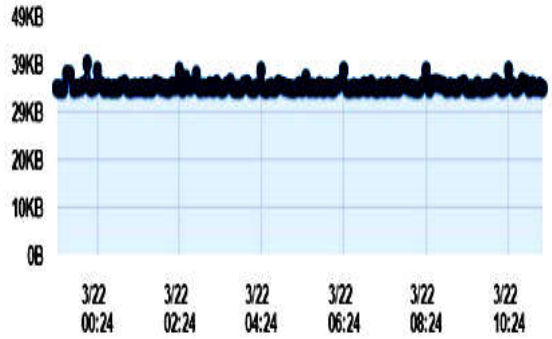

Fig 4 Max Network IN *out* bytes

In AWS, the health of environment and CPU Utilization, and calculated Maximum Network IN and Maximum Network OUT are monitored. To find the availability of EC2 instances, the load balancers periodically sends requests to EC2 instances. These tests are called health checks. The health check status of the instances is positive, and at the time of health check it is InService. The status of the instances is unhealthy, and at the time of health check it is OutOfService.
As shown in Fig. 2, Fig. 3 and Fig. 4, the environment health is monitored by health check codes for 10 hours and reported as OK. Hence, the novel secured dual authentication protocol is proven safe in the cloud environment. CPU utilization was monitored for 10 hours and the usage calculated shows that less than 15% of resource got consumed for the protocol deployment. Maximum Network IN and OUT is calculated. Time taken for calculation in 10 hours from 00.24 am to 10.24am for both IN and OUT Maximum network time. Result shows that monitoring of the environment health, CPU utilization and Max Network up and down times is fine, and the entire configuration is deployed successfully to the new cloud environment.

Protocol Verification

Further to verify the authenticity of the proposed AMAM, the protocol is formally verified using AVISPA tool. This tool is widely used for analysis and verification of internet security protocols. High-Level Protocol Specification Language

(HLPSL) [8] is used for verifying the security properties of the protocol which is integrated with four different back-ends; all the back-ends as mentioned here performs the security analysis of the protocol. In HLPSL, each entity is defined in a separate role and it is described in the initial state of the transaction. Three basic roles are defined as Node with common system properties, Token Authority, Base station and Cloud Server. During the security analysis of HLPSL, the result of the protocol will be verified whether it meets them or not. Fig. 5 and Fig. 6 show the actual protocol simulation and verification for both the normal execution scenario and attack scenario.

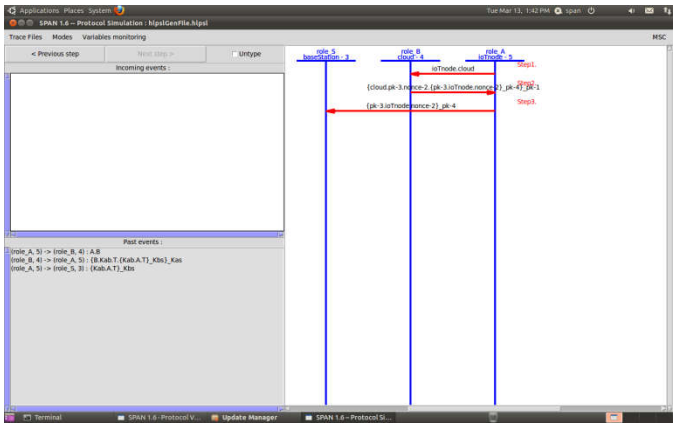

Fig 5 Protocol Simulation (AMAM) in AVISPA

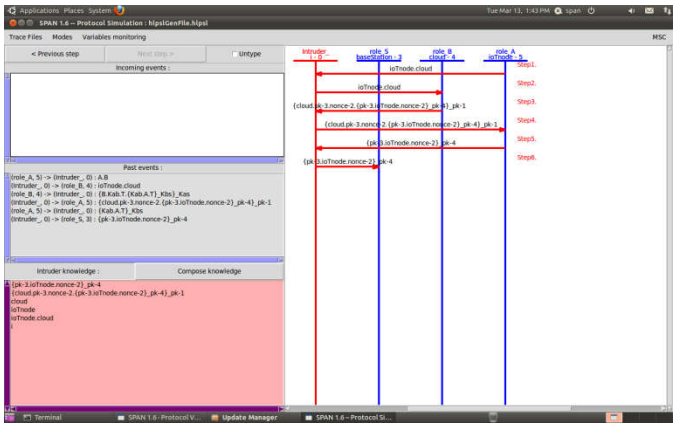

Fig 6 Composing Intruder Knowledge

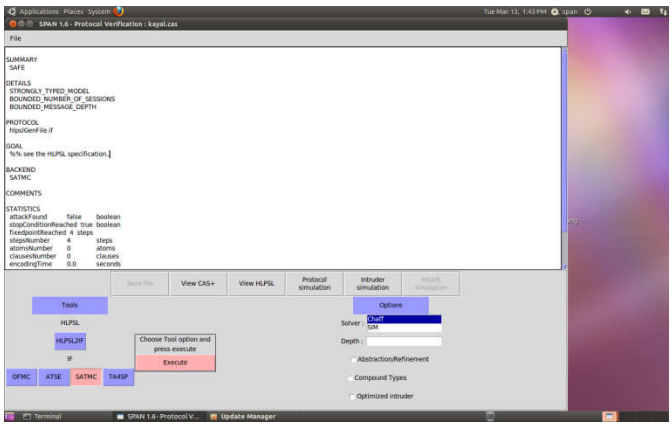

Fig 7 Protocol Verification with various Execution Logic

Model validation: Attacker Knowledge

Fig. 7 shows the protocol resilience analysis. The analysis of the proposed AMAM is performed using the protocol validation and tested over various scenarios.

1. The roles are validated using legitimate nodes.
2. Secondly, an artificial intruder knowledge is incorporated and the attacks possessing the impersonation of all the characters - legitimate nodes, cloned nodes, worm hole etc are incorporated.
3. Finally, intruder plays the role of any Owner in one of them.

From the analysis, it is observed that for all above mentioned scenario the AVISPA does not report any attack. Hence, it is realized that the proposed AMAM is authentic and the protocol is safe for all the mentioned scenarios. The proposed AMAM is light weight and with stands in all situation without compromising the performance.

CONCLUSION

From the advancement of the technology, various technological services, it is authorized that the total number of devices and their communications can be increased in upcoming years. In order to combat the threats which are arising with the IoT services an efficient light weight system is always mandatory and should be accompanied in all the devices.

In this work, a novel light weight anonymous authentication protocol is proposed, implemented and validated. The proposed AMAM is optimal enough to withstand with high resilience and capable to achieve a secure communication between the devices. Further, the authenticity of the protocol is validated using a formal language verification tool called AVISPA. The results obtained from AVISPA confirmed that the proposed AMAM is robust. Further, in future the protocol can be scaled to a larger unit which could be the extension of this work.

Reference

1. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, In *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.
2. V. Gazis, “A Survey of Standards for Machine-to-Machine and the Internet of Things”, In *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 482-511, First quarter 2017. doi: 10.1109/COMST.2016.2592948
3. Diego M. Mendez, Ioannis Papapanagiotou, Baijian Yang, “Internet of Things: Survey on Security and Privacy”, *Computer Research Repository*, 2017.
4. Mosenia and N. K. Jha, “A Comprehensive Study of Security of Internet-of-Things”, In *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586-602, Dec 2017. doi: 10.1109/TETC.2016.2606384.
5. E. Hajjar, G. Roussos and M. Paterson, “Secure routing in IoT networks with SISLOF”, *2017 Global Internet of Things Summit (GIoTS)*, Geneva, pp. 1-6, 2017.
6. Kamble, V. S. Malemath and D. Patil, “Security attacks and secure routing protocols in RPL-based Internet of Things: Survey”, *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)*, Pune, pp. 33-39, 2017.
7. M. Asplund and S. Nadjm-Tehrani, “Attitudes and Perceptions of IoT Security in Critical Societal Services”, In *IEEE Access*, vol. 4, pp. 2130-2138, 2016.

8. S. Sen, J. Koo and S. Bagchi, "TRIFECTA: Security, Energy Efficiency, and Communication Capacity Comparison for Wireless IoT Devices", In *IEEE Internet Computing*, vol. 22, no. 1, pp. 74-81, Jan/Feb. 2018.
9. L. Parne, S. Gupta and N. S. Chaudhari, "SEGB: Security Enhanced Group Based AKA Protocol for M2M Communication in an IoT Enabled LTE/LTE-A Network", In *IEEE Access*, vol. 6, pp. 3668-3684, 2018.
10. N. N. Dao, Y. Kim, S. Jeong, M. Park and S. Cho, "Achievable Multi-Security Levels for Lightweight IoT-Enabled Devices in Infrastructureless Peer-Aware Communications", In *IEEE Access*, vol. 5, pp. 26743-26753, 2017.
11. N. N. Dao, Y. Kim, S. Jeong, M. Park and S. Cho, "Achievable Multi-Security Levels for Lightweight IoT-Enabled Devices in Infrastructureless Peer-Aware Communications", In *IEEE Access*, vol. 5, pp. 26743-26753, 2017.
12. K. Yang, D. Blaauw and D. Sylvester, "Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey", In *IEEE Micro*, vol. 37, no. 6, pp. 72-89, November/December 2017.
13. W. L. Chin, W. Li and H. H. Chen, "Energy Big Data Security Threats in IoT-Based Smart Grid Communications", In *IEEE Communications Magazine*, vol. 55, no. 10, pp. 70-75, October 2017.
14. S. M. Cheng, P. Y. Chen, C. C. Lin and H. C. Hsiao, "Traffic-Aware Patching for Cyber Security in Mobile IoT", In *IEEE Communications Magazine*, vol. 55, no. 7, pp. 29-35, 2017.
15. H. Sedjelmaci, S. M. Senouci and T. Taleb, "An Accurate Security Game for Low-Resource IoT Devices", In *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9381-9393, Oct. 2017.
16. M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi and A. Alamri, "Toward end-to-end biomet rics-based security for IoT infrastructure", In *IEEE Wireless Communications*, vol. 23, no. 5, pp. 44-51, October 2016.
17. W. Yu and S. Köse, "A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks", In *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 11, pp. 2934-2944, Nov. 2017.

How to cite this article:

Nagavalli S., Ramachandran G and Saminathan R (2018) 'Secure Anonymous Routing Schemes for Internet of Things', *International Journal of Current Advanced Research,* 07(3), pp. 11108-11112.
DOI: http://dx.doi.org/10.24327/ijcar.2018.11112.1914

****