IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

A Mobile Agent Based Framework for Securing Iot Network

Anubhuti[1], Harjot Kaur[2]

M.Tech, Student, Department of CSE, GNDU RC, Gurdaspur, India[1]

Assistant professor, Department of CSE, GNDU RC, Gurdaspur, India [2]

Abstract: At present, Internet of things (IOT) has become an important area of research work in which the various physical objects are connected to internet for a number of applications. Due to world-wide acceptance of the Internet of Things, security problems in it have increased. This paper presents these security issues and proposes a framework to detect the malicious node in a network using mobile agents. An algorithm is also proposed to detect malicious nodes.

Keywords: Mobile agents, multi agent systems, internet of things, attacks, Security Certificate, Insecure nodes.

1. INTRODUCTION

Agents
An agent is a computer system which when situated in some environment is capable of performing autonomous action [1], i.e. situated in an environment; a software agent can perform the required action without the interference of its owner. The owner just need to tell what to do and the agent will perform the action. A simple example of an agent can be “Air-conditioner” that can automatically adjust its temperature according to the temperature of the room. Intelligent agent is enhancement to the agent i.e. it is capable of performing flexible and autonomous action, where flexibility mean- Reactivity, Proactivity and Social-ability [2].

The reactive property of agent implies that the agent perceives its environment and react to it i.e. an agent is able to change its behaviour according to the change in environment in which it is situated. An agent has a goal-directed behaviour i.e. it works towards achieving its goals. This property of agent is known as proactivity. And the capability of an agent to communicate and co-operate with other agents to achieve its goals shows its property of social-ability.

1.1 Multi-Agent System

A multi-agent system (MAS) is a system consisting of multiple agents that are capable of communicating and negotiating with each other to achieve their desired goals. A single agent cannot provide what is desired. In order to achieve some goals, group of agents is required. It is not necessary that each agent in a Multi-agent system is directed to achieve the same goal; the agents may have their own goals to fulfil. The complex task is divided into subtasks and these subtasks are allocated to the agents in a system. The agents work towards achieving these sub-goals even if they contradict each other.
Examples of MAS include:
Air-traffic control: suppose a key air traffic control system fails suddenly, leaving flights in the locality of the airport with no aircraft control system. Luckily, autonomous air traffic control systems in nearby airports recognize the failure and deal with it.
Internet agents: agents doing searching for us in the internet. We can tell the agents what we want and they can do search for us.

1.2 Internet of Things

The concept of Internet of things is being widely used these days. As is clear from the name, Internet of Things implies connecting each and every device to the internet [3]. So, IOT can be defined as connecting every device to the internet in order to achieve the desired goals.
Internet of things is a kind of environment, in which various devices are connected through internet to each other to give various type of information [4], i.e. IOT is an environment which gathers information from various devices connected to fulfil the required goals. The thing in Internet of things can be anything like vehicle, gadgets, persons, animals, etc that has sensors, tags, actuators associated with them to gather data. Each device in it can be given IP addresses and has the ability to transfer data across network.

1.3 Security issues in Internet of Things

The concept of Internet of Things has become ubiquitous. It is spreading very rapidly day by day. As a result, number of devices to be connected is also increasing day by day due to which security issues are increased. The network is becoming more and more vulnerable to various security attacks [5]. These attacks include:

i. Privacy issue
ii. Availability and DOS issues
iii. Spoofing
iv. Eavesdropping
v. Data tampering

These can be explained as:
Impersonation/Identity Spoofing: In this attack, an unauthorized node spoofs the identity of an authorized

DOI 10.17148/IJARCCE.2016.5688

node i.e. it communicates on behalf of some other node in an unauthorized way.

i. Eavesdropping: this attack aims at keeping an eye at the data exchanged between two or more nodes. In this attack, attacker can easily have access to the exchanged data but in this case data is not tampered.
ii. Data tampering: In this case, attackers not only access the data but are also able to modify the data.
iii. Authorization and Control Access issues: This type of attack includes the gain of unauthorized access to data or any physical assets and thus damaging them.
iv. Privacy Issues: In IOT, the privacy issue is concerned with the protection of information of the individual from exposure in the IOT environment.
v. Availability and DOS attack: It refers to Denial of service attack. The victim in this attack is unable to get access to any service i.e. the attacker is able to target victim by making the assets and services partially or totally unavailable resulting in dos attack.

2. LITERATURE REVIEW

He and Sycara (1998) [6], has discussed about the secure agent society and how can it be achieved using modern cryptography. An overview of the public key infrastructure (PKI) and the agent based PKI (security agent) is given. In security agent, there is no specific certification format, rather it allow the users to define the format according to their need and the need of application. The paper also explains about the internal architecture and methodology of S.A. in RETSINA, which includes three modules: Agent editor, planner and security module which corresponds to 3 levels: Policy specification, protocol generation and operation execution. A brief overview on the KQML (knowledge query and manipulation language) is provided which includes a set of new parameters and per formatives for agent security.

Tripathi and Ahmed (2002) [7], explain about various paradigms for mobile agent based active monitoring of network systems. A framework for it has been discussed. This framework is implemented using AJANTA mobile agent server. It explains about various agents like monitor agent, subscriber agent, auditor agent and inspector agent. There are various interfaces like remote control interface, monitor interface, and subscriber interface that is implemented by agent. The paper also presents a set of experiments using AJANTA mobile agent system to evaluate the capabilities of mobile agents in the framework of agent. Based on network monitoring it has been found that mobile agent based network monitoring is far better than SNMP approach since it reduce network load and provides better bandwidth efficiency.

Kamangar et al. (2003) [8], discuss about the monitoring of distributed and scalable network. A brief overview on the architecture and functionality of distributed network monitoring is given. Issues of distributed network and how these can be solved using mobile agents have also been explained. It arguments on whether mobile agents are better way to monitor distributed network as compared to client-server model. It has been found that mobile agent paradigm is more efficient than client-server. Experimental results are given to verify the same.

Cecil (2006) [9], in her report first of all gives a brief overview on the importance of network monitoring and analysis. In order to improve the performance and efficiency of the network, network monitoring is must. Its main purpose is to resolve the issues of security breaches that exist within a network. Then 2 different monitoring techniques have been discussed: Router based and Non-Router based. Router based techniques does not need any installation of hardware or software since monitoring abilities in it are inbuilt and hence less flexible. In contrast, non router based is more flexible as additional software is required to be installed. Router based techniques include SNMP (simple network monitoring protocol) and RMON (remote monitoring). This paper also discusses about the active and passive monitoring of non router based technique. It has been concluded that either active or passive is not a good approach to be considered alone so their combination should be used.

Wang et al. (2007) [13] in this paper gives the brief explanation on the various attacks possible on the network like DOS, worm, Trojan horse and viruses which causes various problems to the operations in a network. This paper presents a 2-D queuing model to evaluate the performance of a system under DOS attacks. Various variants of DOS attacks exist like packet flooding attack, reflection attack and SYN flooding attack. The most common SYN flooding attack is considered here. The SYN packets consist of two packets: regular requests packets and the attack packets. The attack packets do not respond to the acknowledgement packets, leaving half-open connections in the victim's buffer. This leads to buffer overflow. A 2-D embedded Markov-Chain and a level-eliminating algorithm is also discussed. The connection loss probability and the buffer occupancy % are the basic measure of DOS attacks.

Dubal et al. (2011) [10], First gives the definition of various security related terms like cryptography, cryptanalysis, and cryptographic algorithm and about symmetric and asymmetric encryption. Various types of cryptographic algorithms like ECC, ECDH, ECDSA, DUAL RSA and MD5 have been explained. Using DUAL RSA allow at most four times faster encryption and decryption than standard RSA. It also reduces computational costs. Symmetric key techniques like ECC and MD5 are used to achieve integrity and confidentiality whereas DUAL RSA used to achieve authentication. So it has been concluded that to gain all the factors of security, it is better to use hybrid algorithm.

Lopez and Perez [11], brief introduction of IOT has been given. Various special requirements for the internet of things to work properly have also been listed, e.g.: collection of data, processing security, etc. Some approaches have been proposed that can fulfil these requirements: 1) Service oriented approach: in this case a middleware is required for two things to interact. 2) Using smart objects: capability of sensing, processing and act. Use of objects that are equipped with sensors, a processor, and actuator devices, etc. An approach has been termed for

DOI 10.17148/IJARCCE.2016.5688

the framework of the IOT : multi-agent system approach, how this approach reduces the disadvantages of a centralized system, brief description of the agent based framework components have been given like knowledge, discovering, security, decision making, etc.

Kumarasamy and Asokan (2012) [14] in the paper gives a brief discussion on DOS, DDOS attacks and different types of DOS attacks which include SYN flood, smurf attack, HTTP flood, SIP flood, etc. Defence mechanism against DOS and DDOS attack are discussed briefly. Various monitoring techniques of DOS attack include: deterministic packet marking (DPM), PPM, path identifier, pushback, MULTOPS, D-WARD, SINKHOLE and net flow. Special flow monitoring algorithm and IP trace back algorithm are also given.

Yu et al. (2013) [12], explains that the nodes in the IOT are required to exhibit intelligent behaviour. This can be achieved by using software agents in an IOT through Agent Oriented Software Engineering. Since the inception of multi-agent systems, very few systems have been deployed. To make it as popular as web2.0, end-user developers are required. As MAS has to deal with end-users, so they can modify the MAS to better serve their needs. Many tools can be used for implementing agents, which include JADE which is used with BDI agents. Another design methodology is TROPOS. But these methodologies can be used by the researchers who are clear in the intelligent agent concepts and AOSE. Some other approaches like sketchi, XML, POSH tools and more better is goal net methodology. Some points are discussed so that more and more users participate in the modification of MAS such as easy agent features, modular design, incentive approach, etc.

shikha et al. [15] Tells about the most common attack possible on WLAN which is spoof attack. A brief introduction on the various attacks possible using spoofing like Man-in-the-Middle attack, DOS, security level rollback, synchronization attacks, power saving mode attack, ARP poisoning and AP spoofing is given along with the prevention details. Various spoof detection methods and their limitations are also discussed. Spoof detection methods include: Sequence Number Gap (SNG), sequence number rate analysis (SNRA), forge resistance relationship method (FRR), received signal strength (RSS), FRR-RA and beacon spoofing detection. It has been concluded that RSS and FRR-RA methods are better than others. The paper also presents the analysis and results in two different test case scenarios.

Palanivelu and Vijayalakshmi [16] explain about WSN and threats to Wireless Sensor Networks like Denial-of-Service, integrity, eavesdropping, etc is given. A method is proposed which involves the use of Mobile Agents to identify a malicious node. It provides the description of the middleware used in the work proposed. A middle-ware based agent topology for WSN security is proposed. Simulation results are also presented.

In paper [2] (2014), it has been told about the limitations and deficiencies of the IOT and how the use of agents in IOT can resolve these issues. A three layer architecture of IOT have been explained which includes perception layer, network layer and application layer. Definition and the various properties and types of agents have been given like autonomous, flexible, ability to learn, negotiate, etc.

Sathyamoorthi et al. [17] in this paper proposed a framework to detect malicious nodes in a wireless sensor networks (WSN). Wireless Sensor Networks consists of hundreds or thousands of sensor nodes. Energy is very precious resource for sensor nodes. The paper explains about WSN and gives brief architecture of sensor nodes. A brief intro on security in WSN and approaches to detect malicious node is given. The approaches are: multipath forwarding, neighbour monitoring approach, acknowledgement based approach and node categorization and ranking algorithm. It presents the problem definition and proposed system. A Stop Transmit and Listen (STL) scheme is proposed to find the malicious node. For every few seconds every node stops their transmission to detect malicious nodes as they are not aware of non transmission times. How malicious node is removed is also discussed.

Limitation: It detects only malicious nodes and does not tell anything about the type of attack occurred at each node.

Bekara (2014) [18] gives the introduction on internet of things, smart grid and IOT based smart grid is given. Several protocols proposed by IETF (Internet Engineering Task Forces) for their efficient integration at different layer to the internet are described which includes 6LowPAN, RPL, CoAP, etc. The two flows: Electric flows and Informational flows in smart grid are discussed. The description of the smart grid conceptual model and the general view of the Advanced Metering Infrastructure (AMI) are given. Various security issues like spoofing, eavesdropping, data tampering, DOS, etc are defined. It also includes several challenges need to be considered when dealing with security algorithm like scalability, mobility, deployment, etc.

Abomhara and Koien (2015) [19] in this paper presents introduction on Internet of Things (IOT), IOT devices and services. The various attacks possible on IOT are cyber-threats, security and privacy issues, eavesdropping, Denial of Service, physical attacks, reconnaissance attacks, spoofing, etc. It also tells about various security threats and vulnerabilities. The primary security goals like confidentiality, integrity, authentication and authorization, auditing and non-repudiation are also introduced. Finally, the classification of possible intruders as individuals and organised groups are explained.

3. PROPOSED FRAMEWORK

In the IOT, it is very important to detect the security of the various node connected to the internet so that the malicious attacks, if any, may be avoided. Here we have given a proposed framework for the security in IOT using mobile agents, which are capable of identifying the insecure nodes and according to the label of insecurity; the required action may be taken.

The framework consists of three types of agents.

There is a monitoring agent which is also a Mobile Agent. It will perform two functions:

DOI 10.17148/IJARCCE.2016.5688

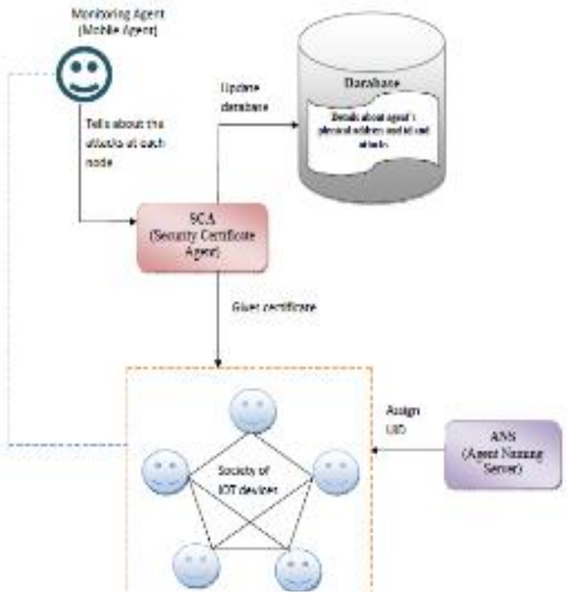
1. It will monitor each node and check whether it is secure or not and gives this information to security certificate agent.
2. If there is an attack it will give this information to IOT devices

Agent Naming Server will assign a unique identity to each node in a network. i.e. each node has unique id associated with it.

Security Certificate Agent is responsible for giving security certificate to each node in a network to ensure security. This will ensure authentication, data integrity, non repudiation, etc. three types of certificates can be assigned:

1. Type A- if the node is secure;
2. Type B- insecure node but can be secured;
3. Type C- if the node is damaged fully and need to be removed from the network.

3.4 Proposed Framework



Simulation algorithm steps

```
1. Start.
2. Let S be an IOT society.
3. Let A be set of agents in society.
4. Let IOT = [$I_{1,} I_{2,} ......., I_n$]
5. Let SCA be Security Certificate Agent.
6. Let MA be Mobile Agents.
7. Let MA1 be Mobile Agent 1.
8. Let MA2 be Mobile Agent 2.
9. Let ANS be Agent Naming Server.
10. Let UID be unique id assigned to each IOT device by ANS.
11. Let security-attacks represent the type of attack on a node.
12. Let $\partial_p > 0$ be a threshold value set to measure connection loss probability small enough to indicate network security status.
13. Let $\partial_b > 0$ be a threshold value set to measure buffer occupancy %.
14. Let RSS be the Received Signal Strength. The transmission power and frame distribution pattern forms the basis of RSS.
15. Set value of security-attacks = “Null”.
16. Procedure ATTACK-DETECTION ALGORITHM(A)
17. ASSIGN-UID(IOT)
18. For each IOT device [$I_{1,} I_{2,} ......., I_n$] do
19.    ANS → Assign UID
20. End for
21. End ASSIGN-UID
22. ATTACK-DETECTION(IOT)
23. For each IOT device [$I_{1,} I_{2,} ......., I_n$] do
24.      Locomote MA.
25.      MA will examine :
26.      If the connection loss probability $P_{loss}$ is large, then
                        Security-attacks = “DOS”
27.               i.e. if
28.                    $P_{loss <} \partial_p$ , no DOS attack
29.                    $P_{loss >} \partial_p$ ,  DOS attack
30.          End if
31.          If buffer occupancy % is larger than $\partial_b$ , then
32.                 Security-attacks = “DOS”
33.          End if
34.          If change in RSS value of frames,
35.                   Security-attacks = “Spoofing”
36.          End if
37.          If a certificate of a node is issued by some other CA(not by legitimate CA)
38.           then     Security-attacks = “eavesdropping”
39.          End if
40.       If more than one type of attack, Security-attacks = “Miscellaneous”
41.       End if
42.    End for
43. End ATTACK-DETECTION
44.  ASSIGNING-CERTIFICATE(IOT,SCA)
45. If attack detected
46.   MA1 informs IOT and MA2.
47.   MA2 informs IOT.
48.   Similarly, MA2 informs IOT and MA1.
49.   MA1 informs IOT.
50. End if
51.   MA informs SCA.
52.   For each IOT
53.         SCA → certificates
54.       Certificate A = secure node
55.       Certificate B = nodes in danger
56.       Certificate C =  insecure node
57. End ASSIGNING-CERTIFICATE
58.   REMOVE-NODES(IOT)
59.    If node → Certificate C
60.         Remove node.
61.    End if
62.  End  REMOVE-NODES
63. End procedure
64.  Stop
```

DOI 10.17148/IJARCCE.2016.5688

4. CONCLUSION

In this paper, we have presented a framework to detect the security attacks on the nodes in the Internet of Things. In this framework, the mobile agent is controlling the various sevices of the nodes. The framework detects the malicious node and after having detected them, the node, if cannot be secured, be removed from the network.

REFERENCES

[1] G. Weiss, A Modern Approach to Distributed Modern Approach to Artificial Intelligence, Cambridge, Massachusetts: The MIT Press, 1999.

[2] A. M. Mzahm, M. S. Ahmad and A. Y. C. Tang, "Enhancing the Internet of Things (IoT) via the Concept of Agent of Things (AoT)," Journal of Network and Innovative Computing, vol. 2, no. ISSN 2160-2174, pp. 101-110, 2014.

[3] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey," computer networks, pp. 2787-2805, 14 may 2010.

[4] "What is Internet of Things (IoT)?," Wednesday 19 August 2015. [Online]. Available: http://wirelotech.com/articlesmenu/miscellaneous/whatis/internetofthingsiot.html.

[5] C. BEKARA, Security Issues and Challenges for the IoT-based Smart Grid, ALGERIA: Conference Program Chairs, 2014.

[6] Q. He and K. Sycara, "Towards a secure agent society," in ACM AA'98, U.S.A, 1998.

[7] A. Tripathi, T. Ahmed, S. Pathak, M. Carney and P. Dokas, "Paradigms for Mobile Agent-Based Active," in Network Operations and Management Symposium, 2002, Minnesota, 2002.

[8] F. Kamangar, D. Levine, G. V. Záruba and N. Chitturi, "Distributed Network Monitoring using Mobile Agents Paradigm," in Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications, Las Vegas, NV, 2003.

[9] A. Cecil, "A Summary of Network Traffic Monitoring and Analysis," http://www.cse.wustl.edu/~jain/cse567-06/net_monitoring.htm, 2006.

[10] M. J. Dubal, M. T R and P. A. Ghosh, "DESIGN OF NEW SECURITY ALGORITHM," in Electronics Computer Technology (ICECT), 2011 3rd International Conference on , Kanyakumari, 2011.

[11] p. a. lopez and G. j. perez, "collaborative agents framework for the IOT," in Workshop Proceedings of the 8th International Conference on Intelligent Environments, Mexico, 2012.

[12] H. Yu, Z. Shen and L. C., "From Internet of Things to Internet of Agents," in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, Beijing, 2013.

[13] Y. Wang, C. Lin, Q. -L. Li and Y. Fang, "A queueing analysis for the denial of service (DoS) attacks in computer networks," Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 51, no. 12, pp. 3564-3573 , 2007.

[14] S. Kumarasamy and D. R. Asokan, "An Efficient Detection Mechanism for Distributed Denial of service (DDoS) Attack," IJECCE, vol. 3, no. 6, pp. 1492-1496, 2012.

[15] Shikha, V. Kaushik and S. Gautam, "Wireless LAN (WLAN) Spoofing Detection Analysis and the victim Silent case," in *Signal Processing and Communication (ICSC), 2013 International Conference*, Noida, 2013.

[16] D. T. Palanivelu and A. Vijayalakshmi, "Detection of Malicious Nodes in Densely Populated Wireless Sensor Network Using Mobile Agents," International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 10, pp. 2278-0181, 2013.

[17] T. Sathyamoorthi, D. Vijayachakaravarthy, R. Divya and M. Nandhini, "A Simple And Effective Scheme To Find Malicious Node In Wireless Sensor Network," *International Journal of Research in Engineering and Technology*, vol. 3, no. 2, pp. 2321-7308, 2014.

[18] C. BEKARA, "Security Issues and Challenges for the IoT-based Smart Grid," in *International Workshop on Communicating Objects and Machine to Machine for Mission-Critical Applications (COMMCA-2104)*, ALGERIA, 2014.

[19] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things:Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security .*, vol. 4, p. 65–88, 2015.

DOI 10.17148/IJARCCE.2016.5688