International Journal of Future Generation Communication and Networking
Vol. 11, No. 3 (2018), pp.33-48
http://dx.doi.org/10.14257/ijfgcn.2018.11.3.04

Device Fingerprint and Mobile Agent based Authentication Technique in Wireless Networks

Umesh Kumar[1] and Sapna Gambhir[1]

[1]*Department of Computer Engineering*
YMCA University of Science and Technology, Faridabad, India
umesh554@gmail.com, sapnagambhir@gmail.com

Abstract

Mobile agent technology is continuously evolving and generating lot of attention among researchers. This paper proposes a new authentication algorithm by using mobile agent technology. The proposed algorithm uses device signature based mechanism for authentication of the device on mobile agent based framework. Device features have been extracted for some specific values and from these features the device fingerprint is generated for the authentication. Research paper describes the device fingerprint extraction, registration and authentication algorithm. As the traffic on the internet is growing at a rapid rate, there is also the need of a technique to reduce the traffic on the internet. Comparison analysis of the proposed algorithm and comparison with the traditional client server based mechanism is done in terms of network traffic. The proposed algorithm reduces the traffic around the authenticator to a great extent as compared to the client server based mechanism. It can also be useful against various attacks in wireless networks, like man in the middle or fake access point etc.

Keywords: *Mobile Agent, Authentication, Device Signature, Device Fingerprint, Digital Signature, Mobile Agent based Framework for Wireless Authentication (MABFWA)*

1. Introduction

In the recent years, traffic on the internet has grown to a great extent. Number of users on the internet is growing continuously. In India only 323 million people who are 24 percent of country's population accessed the internet in 2016. By 2021 there will be more than 635.8 million internet users in India only [1]. According to the Cisco VNI, 2017 globally IP traffic growth is tremendous as and is increasing day by day. The report shows that growth of IP traffic from 2016 to 2021 is around 24%. As the traffic on the internet is growing at an unimaginable rate, there is a need for updating existing techniques which can reduce the traffic on the internet. Mobile agent technology can be one of the solutions to reduce the traffic on the internet [2]. Mobile agent is an autonomous code which can roam inside the network by following some of the nodes which is called itinerary of the mobile agent. This itinerary can be dynamic or static. Mobile agent technology has seen a good amount of growth over the period of time. In some scenarios, this technology can be used instead of client server architecture for reduction in the traffic around the network. In the adhoc wireless networks, authentication is always a big challenge.

Recently, Device fingerprinting has emerged as one of the solution for collecting information about the devices which are connected in a wireless network [3]. Device fingerprinting technique can be used in mobile agent based frameworks for authentication of mobile agent and the device which generated this. The main

Received (January 4, 2018), Review Result (March 26, 2018), Accepted (April 12, 2018)

ISSN: 2233-7857 IJFGCN

contribution of this paper is to develop a technique using Device Fingerprinting mechanism to authenticate the mobile agents in the **M**obile **A**gent **B**ased **F**ramework **F**or **W**ireless **A**uthentication (**MABFWA**) [4]. Proposed technique will also help in preventing the attacks like man in the middle, hijacking, replay, jamming and eavesdropping [5]. This paper concentrates on providing a solution for authentication of the devices meanwhile reducing the traffic on the internet. Over the period of time various algorithms and mechanisms have been proposed for authentication of mobile devices. This paper will try to summarize these models also.

The rest of the paper is organized as follows. Section 2 describes the motivation and related work for mobile agent authentication and device authentication. In Section 3 proposed algorithm for the mobile agent authentication is being discussed. Section 4 explains the numerical analysis of the protocol in contrast to the client server model. In Section 5 proposed mobile agent based approach is compared with client server approach through an example. Finally, the conclusion of the paper is done in Section 6.

2. Motivation and Related Work

Due to the broadcast nature of wireless networks, various types of attacks are possible in wireless networks. Node forgery is one of the attacks which can lead to other types of attacks depending upon the target of the attacker [6]. Node forgery can lead to forged mobile agents pretending to be a legitimate one and can lead to various types of attacks like agent to agent, agent to host and host to agent. Apart from this, below are some of the reasons for applying a fingerprint mechanism to mobile agent:

Authentication: Authentication of mobile device is one of the most important tasks in the wireless network. This paper focuses on this issue.

Integrity: It may be the case that during transmission of mobile agent the contents would have changed. So the mobile agent after change can also do the harmful task on the machine.

Non-repudiation: This is also one of the most important properties as neither of the party taking part in communication can deny about sending the mobile agent and receiving of agent as well as task performed by the agent.

So the above mentioned properties should be satisfied by the mobile agent based communication network to be successful. Recently many authentication mechanisms have been proposed each having its advantages and disadvantages but device fingerprinting approach has not been tested with mobile agents.

Related Work

Shimshon Berkovits *et al.*, [7] has proposed a model for mobile agent authentication using trust based mechanisms and proved the objectives of the research using the Lampson et al. [8] algorithm. The model also checks that the authenticity of the mobile agent during the transmission of the mobile agent over the mobile agent itinerary. Model uses the reference monitor that decides about grant of the request, operation of the request and the access rules also.

Weidong Fang *et al.*, [9] worked on the model of reputation evaluation system for wireless sensor nodes. This model makes use of the trust calculation based on the previous communication of the node. Trust calculation can be either direct or indirect. Direct trust is calculated based on the trust distributed across the network.

After this the trust value from the adjacent nodes is calculated and used for the indirect trust calculation.

Govind P. Gupta *et al.*, [10] has proposed energy and trust aware mobile agent migration (ETMAM) protocol for trust and energy calculation. Proposed model adopted data aggregation model for computation of trust for mobile agent. In the proposed model comprehensive trust is calculated based on direct trust and aggregated trust value from the neighbouring nodes. Every node in this model is equipped with Trust Manager Component (TMC). TMC calculates the trust value of the neighbours based on some predefined values. After that comprehensive trust is calculated based on these values. This model leaves the nodes from the mobile agent itinerary if the node trust calculation is not up to the mark.

Napa Sae-Bae *et al.*, [11] has given the mechanism of online signature verification for the mobile devices. In this approach online signatures are represented using a histogram. Histograms are designed specially to capture the essential details of the signature as well as some of the relationships between multiple attributes of the signature. This approach can be used in mobile agent authentication process also.

Guenther Starnberger *et al.*, [12] have proposed a Quick Response Transaction Authentication Numbers (QR-TAN) for mobile transaction authentication. This technique uses the two dimensional QR barcodes. The advantage of this method is that the terminals do not require any up gradation from the current state. Colour barcodes can be used for further enhancement of the technique.

G. Geetha *et al.*, [13] proposed a new method for trust and reputation management in terms of mobile agent security. Trust value of each host is calculated and stored in the routing table along with other parameters. This trust value is updated over the period of time and the path for the mobile agent is selected based on the best value of the routing table.

Bhavin Shah *et al.*, [14] used the neural network based technique i.e. neural network based back propagation model for intrusion detection or malicious node detection in to the network. This paper also compared the various techniques of intrusion detection and worked on the objective of reducing the size of the agent to be transmitted over to the network. Paper suggested mobile agents for data communication in client server architecture for data transfer.

Dilli Prasad Sharma [15] proposed the concept of authentication mobile agent for the distributed environment. In this model whenever the system wants to authenticate a particular node then the system proxy calls the mobile agent and the agent is equipped with necessary authentication information. Model uses the signature concept to sign and verify the signature.

Mianxiong Dong *et al.*, [16] proposed the mobile agent based model for energy and time efficient data collection. Model also proposed the dynamic route selection of the mobile agent itinerary based on greedy approach. The dynamic route selection helps in planning the mobile agent itinerary in a much better way. Data can be collected in less time using this mechanism from the distributed nodes.

Michael Riecker *et al.*, [17] proposed the lightweight and energy efficient model for authentication of the node. The model makes use of the consumption of energy as the vital element in determining the node to be malicious. Node which is consuming abnormal energy is detected using the mobile agents carrying the necessary information across the network. Deviations from the normal consumption of the energy must be strong enough that it should be detectable.

Comparison of various above mentioned schemes is shown in Table 1 along with the advantages and disadvantages.

Table 1. Comparison of Various Schemes

Sr. No.	Model Name	Methodology	Advantages	Disadvantages
1.	Lampson [8]	Certificate	• A single certificate authority is used. • Certificates are refreshed after an interval of time. • Restrictions can be applied to both the parties about the power distribution. • Arguments can be passed remotely using RPC.	• Complexity is higher. • Requires new libraries and principals to be installed.
2.	BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks [9]	Prediction of Trust	• Prediction of node trust is calculated based on the communication between the nodes. • Trust value of the node is also calculated based on the neighbour's reply of the trust value of the node.	• Neighbour nodes can send the incorrect value if hijacked or may not reply at all. • One unintentional wrong transaction can lead to low trust value.
3.	Signature verification on mobile devices [11]	Histogram and signature mechanism	• Histogram from the signature sample is created. • Features are extracted from the histogram and these features are used by the matcher to verify the signature. • Lightweight protocol.	• Cloned signatures will be verified and cannot be prevented from the proposed scheme.
4.	QR-TAN: Secure Mobile Transaction Authentication [12]	QR Codes	• Transaction signing mechanism using QR codes is used.	• Additional requirement for QR code generation and reading • Higher resolution camera and

				computational power of the device.
5.	Trust and Reputation management for Mobile Agent [13]	Trust value	• Reputation value of a particular node is calculated from number of nodes connected in the network. • Lightweight protocol.	• Forged node can send wrong trust value.
6.	Improving Performance of Mobile Agent Based Intrusion Detection System [14]	Neural Network	• Backpropagation Neural Network Technique (BPNN) is used for intrusion detection. • Zero packet dropping rate to improve the efficiency.	• Training of Neural Network to take very long time. • Network parameters and node parameters can change after some time. So re-training may be required for BPNN.
7.	Mobile Agent-Based Authentication [15]	Digital Signature	• Key pair is generated. • Signature algorithm is used to sign and verify the message.	• Vulnerable to attacks if keys are compromised.

Node forgery is one of the most severe problems in the wireless networks. In this the cryptographic valid credentials are captured by an attacker and later on impersonates to valid one. Existing techniques compared in Table 1 has some advantages and disadvantages in one form or another. So there is a need for lightweight authentication technique which can authenticate the devices as well as access point. Device fingerprinting with the help of mobile agent can be one of the techniques to authenticate the particular mobile device as well as access point over to the network.

3. Proposed Work

In the next section the mobile agent and device signature based authentication model is proposed. The model is then analysed in terms of traffic generated by the model and compared with client server model. This scheme will make use of the communication model proposed in our earlier paper [3]. Communication model will be having the three entities as shown in Figure 1.

Client/Supplicant: Client/Supplicant is the mobile device which will be authenticated after the particular authentication process. Client communicates with the authenticator.

Authenticator: Authenticator helps in validating the credentials supplied by the client. Authenticator passes the credentials to authentication server.

Authentication Server (AS): Authentication server verifies the credentials supplied by client through authenticator. It stores the credentials for validation as well as the signature of the device.

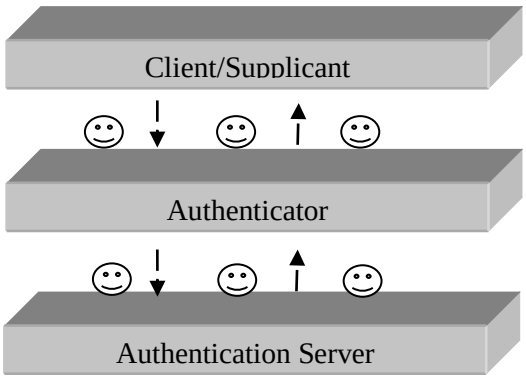

Figure 1. Communication Model

Layered authentication framework which is used in wireless authentication is shown in Figure 2.

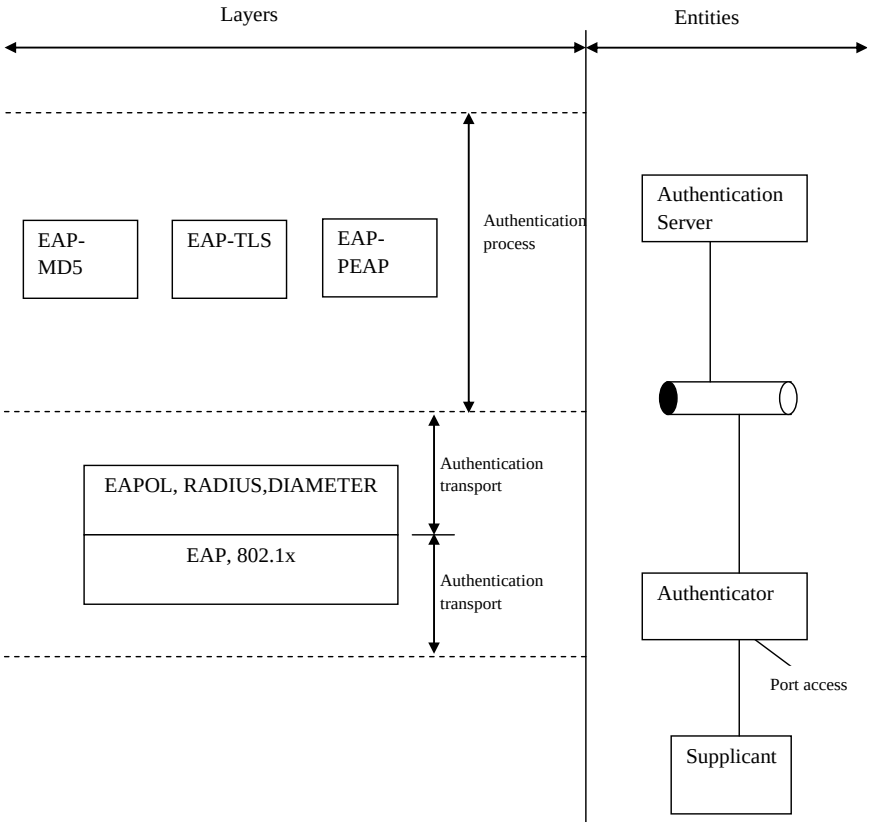

Figure 2. Layered Authentication Framework [18]

Supplicant communicates with the authenticator with the wireless method or wired method. Authenticator communicates with the authentication server and particular authentication process is used by the authentication server for the

authentication. Authentication process which is being used by the authentication server can be EAP- MD5, EAP- TLS, EAP-TTLS, EAP-PEAP and EAP-CHAP [18].

3.1. Device Fingerprint and Mobile Agent based Authentication

This section will describe the overview for device fingerprint based authentication model. Model describes the working of various components like Access Point (AP), Authenticator (A) and Authentication Server (AS). Various mobile nodes are connected to the access point with the help of 802.11 technologies. Architecture allows heterogeneous communication devices to contact each other in a secure manner. Here the authenticator acts as an interface between the AP and the AS. The authentication process goes through the access point to authenticator and then to the authentication server.

Figure 3 shows the architecture and working of device signature based authentication model. Here multiple **A**ccess **P**oints (**AP**'s) are connected to the **A**uthenticator (**A**). Authenticator in turn is connected to the **A**uthentication **S**erver (**AS**).

1. **Access Point (AP)**: Access point provides the access to various devices within the wireless range. Multiple access points can be within the range of a single device. Device is connected to the access point with the strongest signal after registration process (if not registered) and authentication. An access point supports multiple devices.
2. **Authenticator (A):** All access points are connected to the authenticator for authentication purposes. Authenticator contains three modules:
    - **Device Fingerprint Scanner:** It extracts the device fingerprint parameters from the mobile agent and creates fingerprint from the device fingerprint parameters. It stores it in cache memory and forwards it to the authentication server for registration purposes. If the device requires authentication then device fingerprint is forwarded to the cache memory.
    - **Cache Memory:** Cache memory stores the fingerprint of most recent devices which are connected to the AP or the devices which are recently registered on the network. Cache memory forwards the device fingerprint to the threshold comparator.
    - **Threshold Comparator:** It compares the two fingerprints and gives true or false depending upon the value of the threshold matched.
3. **Authentication Server (AS):** Authenticator has access to the AS. It registers all the device signatures in the database and further provides the signature value when required by the authenticator.

Proposed Model Works in following modes:

- **Single Device Authentication:** Single device authentication is required when a new device comes into the range of the access point and wants to connect to the network. This single device can be a user mobile device or a fixed access point.
- **Multi Device Authentication**: Proposed model also supports the authentication of multiple devices in one go. Mobile agent from authenticator follows the itinerary for multiple devices and carries the device signatures of these devices. If the signature matches to the calculated one

then it gives success otherwise failure. This loaded mobile agent then comes to the authenticator with necessary information.

Device Fingerprint Calculation

Device fingerprint is a unique signature of the device. This device fingerprint is generated depending upon the various parameters. These parameters will be extracted from the device using mobile agent which is being sent by the authenticator and executed on the target machine.

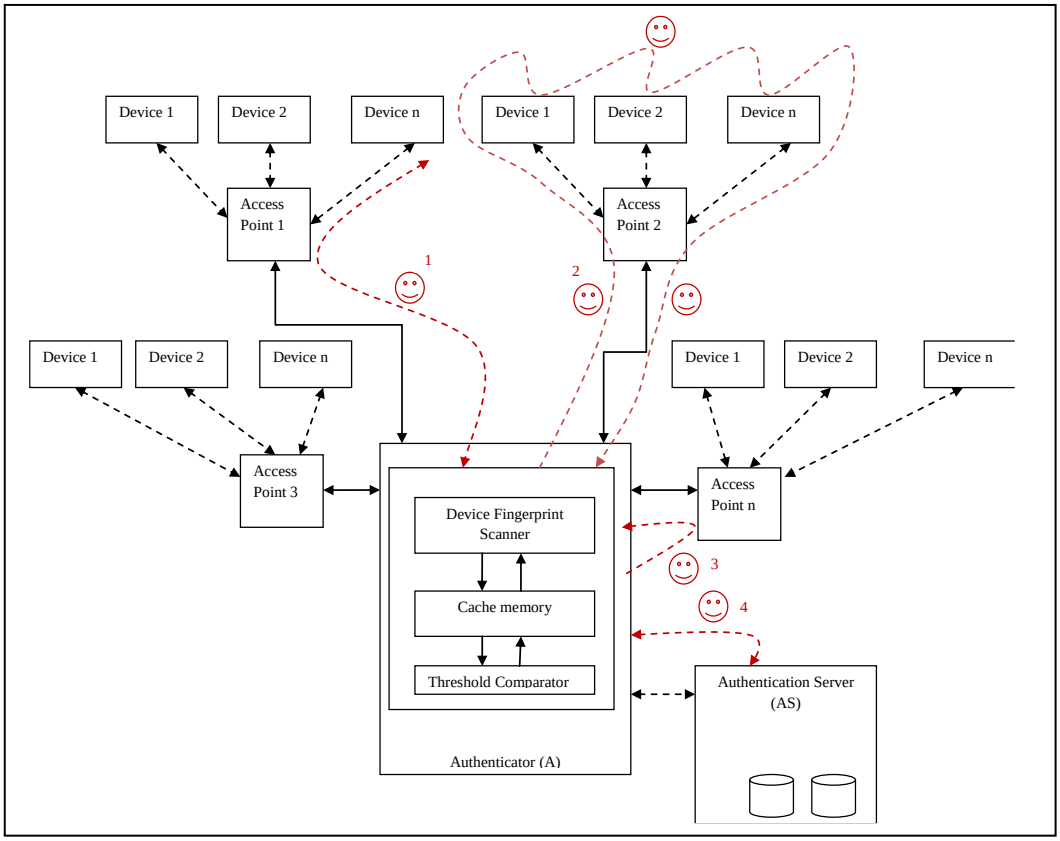

Figure 3. Architecture and Working of the Proposed Model

Various parameters that are used to calculate the device signature value are listed below. It may be the case that device have only some parameters value.

Parameters to calculate device fingerprint:

- **Geo location lat/long:** This is the geographic location of the device. The location can be calculated by the network or GPS (if supported).
- **IP addresses:** This is the unique 32/128 bit address which is allocated to the device. The version of the IP address can be IPv4 or IPv6.
- **MAC addresses:** This is the media access control address which is assigned to the network interface card of the device.
- **Network ID:** Every network created has the unique id value associated with it. This is the id of the network to which the device is connected.

- **Browser name and version:** This is the name of the browser currently installed and the version of the browser. Device may have more than one browser then the details of both are included in fingerprint.
- **OS name and version:** This is the name and current version of the operating system of the device.
- **ESN:** stands for electronic serial number. This number is generated by the manufacturer on the microchip on mobile devices.
- **IMEI or MIN:** stands for international mobile equipment identity or mobile identification number. It is the unique identification number that all mobile phones have.
- **RSSI:** stands for received signal strength indicator. With this parameter the received signal power can be measured.
- **BSSID:** stands for basic service set identifier**.** This is the mac address of the access point which is the combination of the organization unique identifier and identifier for the radio chipset.
- **SSID:** stands for service set identifier. This is the name which is assigned to the wireless local area network. Mobile devices use SSID to identify the network and to join the network also.
- **CenterFreq:** Center Frequency is the measure of the frequency between upper and lower frequency cutoffs. Arithmetic mean or geometric mean of the lower and upper cutoff frequency is used to define this.
- **Frequency:** This is the frequency value in MHz. This is the value over which the communication will take place.
- **Level:** This is the strength of the signal received. This is measured in dBm.
- **Timestamp:** This will contain the time of a particular communication. This value is generally mentioned in microseconds.
- **VenueName:** This is the name of the location that is distributed by the access point.
- **Device to AP RTT Supported:** This is the value of the inbuilt function supported by the device. Using this function device can calculate the distance between the access point and device.
- **isTdlsSupported:** This is the value of the tunneled direct link setup. IEEE 802.11z supports this. Its value will be true if supported.
- **WifiConfiguration.GroupCipher:** This is the cipher mechanism supported by device value can be CCMP, TKIP.
- **LinkSpeed:** This is the current speed in Mbps of the channel.
- **Capabilities:** describes the authentication, key management, and encryption schemes supported by the access point.
- **Camera characteristics:** If the device has the camera features than camera characteristics can also be included in the signature.
- **Gateway address:** This is the address of the router which is maintained by ISP.

These parameters are entered in to the device fingerprint generator which generates the device fingerprint. Most of the parameters mentioned above will give the real time dynamic values and some values will remain unchanged like IMEI number, MAC address and camera characteristics etc. Every time the mobile agent fetches the device fingerprint parameters, it is compared with the earlier stored one. If the percentage of signature matching is more than threshold, then access can be granted. This threshold value can be decided depending upon the criticality of the application.

In the proposed model, first of all the device needs to be registered in the authentication server for gaining the access of the network resources. The step by step registration algorithm is shown in Algorithm 1.

Algorithm 1: Registration

Input:
1. Number of Nodes
2. Client addresses i.e. client(i)
3. Authenticator address i.e. authenticator_address
4. Authentication Server address
5. itinerary[ ]

Output: Success or failure of registration.

1. create itinerary[ ] of i number of nodes for MA
2. create MA sign_Collector( )
3. while itinerary[ ] is not empty
    3.1 if node itinerary[i] is active then
        3.1.1 dispatch sign_Collector( ) to the itinerary[i] node.
        3.1.2 compute device signature and append it to the results
    3.2 else
        3.2.1 continue
    3.3 end if
4. end while
5. authenticator stores the signatures in cache memory and forwards it to the authentication server.

After every device is registered into the network and device comes later on for the use of network services then the device needs to be authenticated. The itinerary created in this approach can use the location fingerprinting technique to create the three dimensional graph of various mobile stations. Later on **L**ocal **C**losest **F**irst (**LCF**) or **G**lobal **C**losest **F**irst (**GCF**) technique is applied to create the itinerary for the mobile agent.

Algorithm 2: Authenticator

Input:
1. Necessary information for authentication process e.g. username, password or device fingerprint
2. Client addresses i.e. client(i)
3. Authenticator address i.e. authenticator_address
4. Authentication server address
5. itinerary[ ]

Output:
Success or failure of authentication.

1. create and load agent **signature_Verifier( )** with the device signatures of all the devices.
- **1.1** For all the devices whose signatures are not present at the authenticator cache memory
  - **1.1.1** creates a mobile agent signature_Collector(devices [ ]), loads it with the device id's of the devices**.**
  - **1.1.2** Server loads the signatures from the database.
  - **1.1.3** dispatch signature_Collector( ) to the authentication server.
  - **1.1.4** append the signatures to signature_Verifier ( ) agent.
- **1.2** end for

2. create itinerary[ ] of MA using itinerary algorithm
3. while itinerary[ ] is not empty
- **3.1** dispatch agent **signature_Verifier( )** from authenticator to node itinerary [i].
- **3.2** agent collects and checks the device fingerprint against the stored signature.
- **3.3** agent gives the success/ failure message depending upon the threshold value of the signature verification result.

4. end while.
5. Last client dispatches the **signature_Verifier( )** to authenticator.
6. Authenticator collects the success or failure message from agent signature_Verifier( ) based on the device signature verification and provides the access.

Authentication server stores the information of all devices that are registered and authorized to use network resources. Algorithm for the same is presented in Algorithm3:

Algorithm 3: Authentication Server

Input:
1. Mobile agent

Output:
Successful retrieval or storage of signature.

Repeat for every request from Authenticator
1. if signature_Collector( ) arrives for registration
   - 1.1 retrieve the signatures from mobile agent
   - 1.2 store it into the database.
2. if signature_Collector arrives for device signature
   - 2.1 retrieve the signatures from database
   - 2.2 load and dispatch the mobile agent signature_Collector( ) to authenticator.

Bulk data transmission facility which is not provided in traditional EAP based approach has been incorporated into the proposed mobile agent based approach. Agents can be loaded with bulk data and can be dispatched to the destination. Algorithm for the same is been presented below:

Algorithm 4: Data_Transmission

Input:
1. Data to be transmitted
2. Destination address (server or client)

Output: Success or failure of data transmission

1. Repeat while client or server has data to send
1.1 create agent **Load_Data( ).**
1.2 load agent with the requisite data and session_key.
2. dispatch agent to the destination

4. Numerical Analysis of Client Server and Proposed Mobile Agent Technique

Proposed technique is compared with the existing client server technique against parameters like management cost and remote interaction time. Numerical analysis of both the approaches has been done.

- **Client Server Approach**

In Client-Server approach the Authenticator receives the traffic from multiple clients seeking authentication within the network. Following equation is used to calculate the complete traffic around authenticator within the network:

$$TrC_{cs}^{m} = \sum_{i=1}^{n} \begin{Bmatrix} (Sreq + Sres) * x * \\ Avg.number\ of\ sessions + (Sreq + Sres) * y \end{Bmatrix} \quad ...(1)$$

where, TrC_{cs}^{m} is the management cost in terms of network traffic.

$Sreq$ is the size of request from client to the server and $Sres$ is the size of response from the server to client

Avg. = Average number of sessions per client

x= Number of message exchanges between client and authenticator depending upon protocol

n= Number of clients

y= Number of calls to authentication server depending upon protocol

Remote interaction time required by the authenticator to validate the clients over the network will depend upon the bandwidth available and will be calculated as:

$$Remote\ interaction\ time = \frac{Traffic}{Bandwidth} \quad ...(2)$$

$$TmC_{cs}^{r} = \sum_{i=1}^{n} \frac{(Sreq + Sres)}{Bw_i} + 2Lt_i \quad ...(3)$$

where, TmC_{cs}^{r} is the remote interaction time for one message exchange with n number of clients in client server architecture.

Lt_i is the latency time between authenticator and i[th] client.

- **Proposed MA based Approach**

In case of mobile agent based approach the management cost in terms of network traffic generated at the authenticator will be calculated as follows:

$$TrC_{ma}^{m} = \{Sma + \sum_{i=1}^{n} Spr\} \quad \ldots(4)$$

where, TrC_{ma}^{m} is the management cost in terms of network traffic for mobile agent architecture.

Sma is the size of mobile agent carrying the authentication algorithm code to be executed.

Spr is the partial result generated at each client.

Here we can have single user authentication and multiuser authentication also. For single user authentication the traffic will be

$$TrC_{ma}^{m} = \{Sma + Spr\} \quad \ldots(5)$$

So according to the above equation the amount of traffic generated at the authenticator just depends upon the size of the mobile agent.

Remote interaction time required by the authenticator to validate the clients over the network will depend upon the bandwidth available and will be calculated as follows for MA:

$$TmC_{ma}^{r} = \sum_{i=1}^{n} \frac{(Sma + Spr)}{Bw(i-1,i)} + Lt(i-1,i) \quad \ldots(6)$$

where, $Lt(i-1,i)$ is the latency time between the i-1 and i[th] node.

Table 2. Comparison of Cost and Time

Parameters	CS	MA (Single user)	MA (Multi user)
Management cost	$\sum_{i=1}^{n} \begin{Bmatrix} (Sreq + Sres) * x * \\ Avg.number\ of\ sessions + \\ (Sreq + Sres) * y \end{Bmatrix}$	$Sma + Spr$	$Sma + \sum_{i=1}^{n} Spr$
Remote Interaction Time	$\sum_{i=1}^{n} \frac{(Sreq + Sres)}{Bw_i} + 2Lt_i$	$\frac{(Sma + Spr)}{Bw(i-1,i)} + Lt(i-1,i)$	$\sum_{i=1}^{n} \frac{(Sma + Spr)}{Bw(i-1,i)} + Lt(i-1,i)$

5. Example

Authentication requires multiple message exchange in client server based approach. As the number of message exchange increases, the traffic around the authenticator increases to a great fold.

Typical Sreq size for client server architecture is around 50 Bytes.

Sreq = 50 Bytes
Sma (MA size) is 3 KB= 1024*3 = 3072 Bytes

Traffic generated in CS mode = α times of Sma, as data generated in the CS approach is much higher than MA approach.

$$(Sreq + Sres) = 50 + \alpha * Sma$$

Putting these parameters in equation 1

Case A: Taking α = 7,

50+7*3072 =21554 Bytes

Case B: Taking α = 30,

50+30*3072 = 92210 Bytes

Table 3.Traffic Around Authenticator in MA and CS based Model (bytes)

No. of Nodes	MA	CS α =7	CS α =30	CS α =50
1	3272	21554	92210	153650
5	4272	107770	461050	768250
10	5272	215540	922100	1536500
15	6272	323310	1383150	2304750
20	7272	431080	1844200	3073000
25	8272	538850	2305250	3841250
30	9272	646620	2766300	4609500
35	10272	754390	3227350	5377750
40	11272	862160	3688400	6146000
45	12272	969930	4149450	6914250
50	13272	1077700	4610500	7682500
55	14272	1185470	5071550	8450750
60	15272	1293240	5532600	9219000
65	16272	1401010	5993650	9987250
70	17272	1508780	6454700	10755500

Case B: Taking α = 50,

50+50*3072 = 153650 Bytes

Putting these parameters in equation 3, the management cost at authenticator in MA approach can be calculated as

$$C_{ma}^{r} = (Sma + Spr)$$

= (3072+200)
=3272 Bytes

It can be analyzed from Table 3 that as the number of nodes increases, traffic increases many fold around authenticator as compared to MA based approach.

The results can also be analyzed as shown in Figure 3.

So the device fingerprint calculation is done using the mobile agent approach. This device fingerprint will be very useful in determining the authenticity of the mobile device. By analyzing the results above, it can be seen by taking into account the traffic around the authenticator that traffic has been decreased to a great extent in the client server approach. Although some parameters of device fingerprinting can change over the period of time but most of the values will remain same which will be very useful in determining the authenticity. This approach using mobile agent also has the additional benefit of reducing the traffic around the network to a great extent.

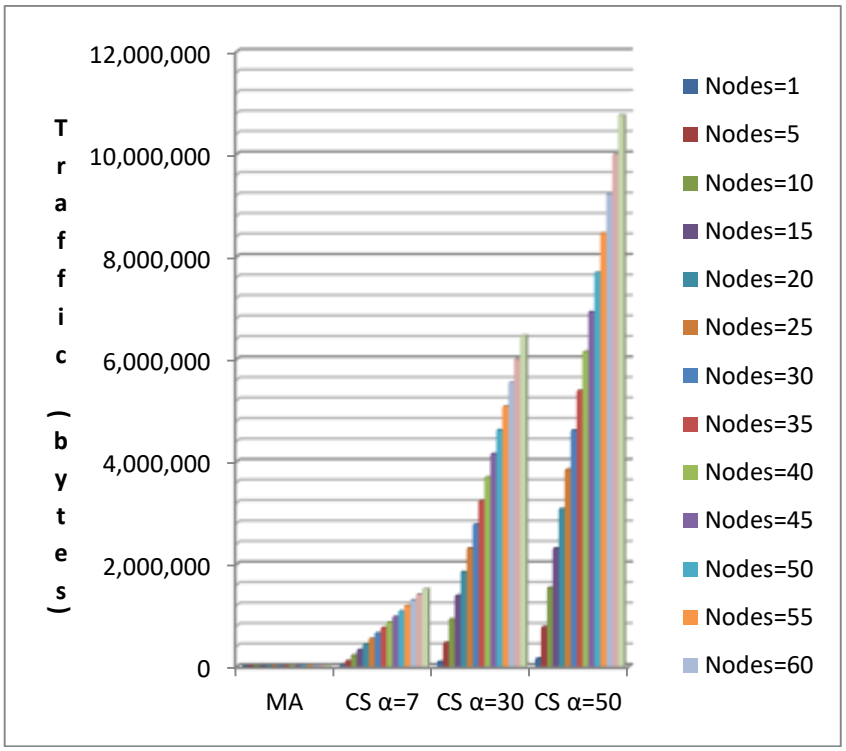

Figure 3. Traffic Analysis for CS vs MA Approach

6. Conclusion

In this paper device fingerprint and agent based device authentication mechanism has been proposed. Mechanism uses various parameters for device signature calculation. Proposed model includes device fingerprint generation and comparison with the stored one against a threshold value. Percentage of signature matching gives the robust decision making capability that whether the access should be granted or not. Apart from authentication, the proposed approach which makes use of the MABFWA also reduces the traffic around the authenticator to a great extent, which is one of the main problems in client server architecture that already suffers from the problem of scalability. In the client server approach traffic increases exponentially but in proposed mobile agent based approach traffic increases linearly.

References

[1] https://www.statista.com/topics/2157/internet-usage-in-india/.
[2] U. Kumar and S. Gambhir, "Mobile Agent Based MapReduce Framework for Big Data Processing", In: Aggarwal V., Bhatnagar V., Mishra D. (eds) Big Data Analytics. Advances in Intelligent Systems and Computing, Springer, vol. 654, **(2017)**.
[3] Q. Xu, R. Zheng, W. Saad and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities", IEEE Commun. Surveys Tuts., vol. 18, no. 1, **(2016)**, pp. 94-104.

[4] U. Kumar and S. Gambhir, "Mobile agent based framework for wireless authentication", 8th IEEE International Conference on Cloud Computing, Data Science & Engineering (Confluence), **(2018)**, pp. 219-224.
[5] U. Kumar and S. Gambhir, "A literature review of security threats to wireless networks", International Journal of Future Generation Communication and Networking, vol. 7, no. 4, **(2014)**, pp. 25-34.
[6] C. Liu and T. Y. James, "An analysis of DoS attacks on wireless LAN", Proc. IASTED Int. Conf. WNET, Banff, AB, Canada, vol. 34, no. 1, **(2006)**, pp. 346-351.
[7] S. Berkovits, J. D. Guttman and V. Swarup, "Authentication for Mobile Agents", In: Vigna G. (eds) Mobile Agents and Security. Lecture Notes in Computer Science, vol. 1419, **(1998)**, pp. 114-136.
[8] B. Lampson, M. Abadi, M. Burrows and E. Wobber, "Authentication in distributed systems: Theory and practice", ACM Transactions on Computer Systems, vol. 10, **(1992)**, pp. 265-310.
[9] W. Fang, C. Zhang, Z. Shi, Q. Zhao and L. Shan, "BTRES: beta-based trust and reputation evaluation system for wireless sensor networks", J. Netw. Comput. Application, vol. 59, ver. 1, **(2016)**, pp. 88-94.
[10] G. P. Gupta, M. Manoj and K. Garg, "Energy and trust aware mobile agent migration protocol for data aggregation in wireless sensor networks", Journal of Network Comput. Application, vol. 41, **(2014)**, pp. 300-311.
[11] N. Sae-Bae and N. Memon, Fellow, IEEE, Online Signature Verification on Mobile Devices, IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, **(2014)**.
[12] G. Starnberger, L. Froihofer and K. M. Goeschka, "QR-TAN: Secure mobile transaction authentication", IEEE Computer Society, ARES '09 The Fourth International Conference on Availability, Reliability and Security, **(2009)**, pp. 578-583.
[13] G. Geetha and C. Jayakumar, "Implementation of Trust and Reputation Management for Free-Roaming Mobile Agent Security", IEEE Systems Journal, vol. 9, no. 2, **(2015)**, pp. 556-56.
[14] B. Shah and B. H. Trivedi, "Improving Performance of Mobile Agent Based Intrusion Detection System", Fifth International Conference on Advanced Computing & Communication Technologies, **(2015)**, pp. 425-430.
[15] D. Prasad Sharma, "Mobile Agent-Based Authentication: A Model for User Authentication in a Distributed System", International Journal of Computer Applications, vol. 112, no. 13, **(2015)**.
[16] M. Dong, K. Ota, L. T. Yang, S. Chang, H. Zhu and Z. Zhou, "Mobile agent-based energy-aware and user-centric data collection in wireless sensor networks", Computer Networks, vol. 74, no. PB, **(2014)**, pp. 58-70.
[17] M. Riecker, S. Biedermann and M. Hollick El Bansarkhani, "Lightweight energy consumption-based intrusion detection system for wireless sensor networks", International Journal of Information Security, vol. 14, **(2015)**, pp. 155-167.
[18] U. Kumar and S. Gambhir Praveen, "Analysis and literature review of IEEE 802.1x (Authentication) protocols", International journal of Engineering and advanced Technology, vol. 3, no. 5, **(2014)**, pp. 163-168.
[19] http://www.ciscopress.com/articles/article.asp?p=369223.

Authors

Umesh Kumar, received his M.Tech. degree in Computer Engineering from YMCA University of Science and Technology, Faridabad, India. Presently he is working as an Assistant Professor in the Computer Engineering department of same University. His research interests include Wireless Security, Mobile Agent, Distributed Computing.

Dr. Sapna Gambhir, is working as an Assistant Professor in Computer Engineering department of YMCA University of Science and Technology, Faridabad, India. She has completed her doctorate in Computer Engineering in 2010 from Jamia Milia Islamia, Delhi, India. She has teaching experience of 15 years during which published many papers in various national/ international conferences and journals. Her current areas of interest are Network Security, Mobile Adhoc Networks, Wireless Sensor Networks and Online Social Networks.

