Gesture based Finger Print Authentication System for Network Security and Mobile Devices in Heterogeneous Wireless Network

Purushothama K.P.1 and Dr. Shankaraiah2
1Research Scholar, JSS Research Foundation, SJCE, Mysore, India
Email: purushothamkp@yahoo.co.in
2Professor and Research Supervisor, Dept. of ECE, SJCE, Mysore, India
Email: {shankarsjce@gmail.com}

Abstract— Nowadays, there is a more significant demand for authentication in heterogeneous wireless networks. The heterogeneous networks are considered as combination of different wireless network technologies, different end user devices and various communication technologies. The present heterogeneous wireless network mainly suffers from providing authentication especially for mobile equipment. In this paper, a gesture based finger print authentication system has been proposed for securing both network and mobile devices.

The entire system depends on gesture based finger print authentication method which is totally isolated from the network, service provider and mobile devices. The user is allowed to enter secret code and gesture based finger print. The entered data will be verified in the pre-stored database. The user is allowed to access the network only after a complete finger print verification of user through mobile. The performance and efficiency of the system is evaluated based on simulation. The simulation result shows that gesture based finger print authentication inside heterogeneous wireless network is highly secured. If the connected device or other devices found to be malicious, the device will be immediately withdrawn from the network service.

Index Terms— Authentication, Heterogeneous Wireless Network, Gesture, Finger Print, Malicious.

I. INTRODUCTION

The heterogeneous wireless network is recognised as 4G mobile communication system. It consists of more than two wireless access technologies. Each and every technology has its own features and qualities in terms of area, coverage, bandwidth, QoS, cost and implementation etc. Nowadays, 4G is considered as the future generation for mobile network. As per paper [1], 4G heterogeneous network have good QoS, high capacity, low latency, low cost and good coverage, except security. The merits and demerits of 4G wireless networks are generally considered with respect to Heterogeneous Wireless Networks.

Authentication is considered as one of the major challenge in any heterogeneous wireless network. Many threats and thefts were happening mainly because of poor security for both mobile device and network. Therefore security plays important role in attracting the mobile user towards particular network. Therefore, there is a severe demand for developing authentication system for safeguarding 4G devices.

DOI: 03.AETS.2014.5.352
© Association of Computer Electronics and Electrical Engineers, 2014
Today, there are various authentication measures exist to safeguard both network and service provider. But only a few methods are existing to safeguard mobile device. The present technique doesn’t provide much security requirements like safe-guarding network as well as mobile equipment. The existing authentication techniques easily allows to access mobile content. Hence, mobile device will be targeted as an attacking tool. The present security system doesn’t obey any security policies under ITU-TM.3400 TMN management [6] functions or any other related standards.

The main contributions of this paper are
• Preventing any unauthorized mobile device to be used as attacking tool
• Detecting a mobile device which may damage other devices or network
• Avoiding any threats towards network

In this paper, an authentication system has been proposed which is responsible for implementing security policies and makes sure those security policies to be continued and followed. Mainly there are two ways to attack the network. First one is through mobile equipment and second one is with network service provider. The security requirement for mobile device [4] consists of confidentiality, privacy and integrity of device. The controlling of data access from the mobile, protecting the mobile device from any external attack, preserving mobile from theft, preserving data or being used as an attacking device are also some of the requirements. The present research mainly deals with security like providing authentication for an interface between the network and network operator.

The main objective is to prevent mobile devices to be used as an attacking tool. The mobile device will be authenticated by a gesture based finger print. The mobile device screen shall be provided with touch pad screen consisting of sensor elements. The elements are capable of recognising the movements made by a person on the screen of mobile device. The recognised data is considered as an input for authentication. Finally, System Architecture (SA) has been developed and proposed for authentication in heterogeneous wireless network. This mainly focuses on detecting and preventing any type of spurious attacks. The system architecture consists of Information Collection Centre (ICC), Security policy Administrator and Data base (policy).

For each and every connection towards a network, the user has to append their authentication through a new technology known as gesture based finger print verification method. The gesture is a movement of hand or finger. Since finger print of a human being is unique, finger gesture can be developed from the tip of any finger on a mobile screen which is unique in nature. The sensor elements inside a mobile device will acquire the movement made by user and treat it as an input data in addition to unique secret code. If the authentication doesn’t passes, the network immediately identifies that the mobile equipment is stolen equipment and the same will be recorded in a database by storing mobile details in the prestored database. In the data base, the International Mobile Equipment Identity (IMEI) of a stolen mobile will be highlighted and further measures can be taken.

The structure of the paper is as outlined. section II presents literature survey and issues based upon 4G mobile networks. Section III describes proposed approach and architecture of authentication system. The section IV illustrates an example of authentication system during any attack to the network and mobile equipment. The section V explains the simulation and simulation result. Finally, section VI gives conclusion for the paper followed by future work.

II. LITERATURE SURVEY

The open architecture and IP based environment [1] identified that, 4G heterogeneous wireless networks are suffering from new security threats and inherent threats from the internet. These threats were not seen in 3G network infrastructure and is owned by service provider and access was denied for network equipment. In this open architecture, diversity in mobile devices and various security levels results in greater security threats.

Y. Park and T. Park have proposed the open natured architecture [2] of 4G network. The open natured infrastructure is accessible from various external connection points through each operator. These elements are at risk from providing holes in security vulnerabilities. Also, the core network infrastructure is shared by different service provider. The single provider compromised the effects of whole network infrastructure. In this open natured architecture, there is no protection for both entities and infrastructure.

In one more research study from the same authors, they have shown that, in a network security procedure, network is secured by avoiding threats while accessing network. This network security procedure is inefficient for open architecture network like 4G. The attackers try to find security weakness in network
protocols and security threats. From these types of security weakness, system performance will be decreased and the network will be abused.

M. Aiash, G. Mapp, A. et al., have presented [3] various security challenges by the application of current security techniques related to 4G network. They have proved that present and new security threats were inherent to 4G technology. The various standards related to X.805 of 3G authentication and key agreement to 4G communication framework were applied. After applying X.805, they have observed many threats to the networks security.

Zheng, Dake He, et al., presented [4] the trusted computing based computer architecture for mobile network. They have not addressed the issue of end user devices.

In paper [5], G. Mapp, et al., have proposed that Y-Comm and Hocky consists of security architectures like Hocky and Y-Comm for 4G networks. Y-Comm architecture consists of multi-layer security model to offer security solution. The model is applied together with peripheral and core frameworks. The four security levels work together through both peripheral and core frameworks. They have not addressed the authentication of devices and focussed mainly on network architecture.

According to ITU-T, M.3400 [6] comes under Telecommunications Management Network (TMN). The security management is an important part of TMN management. The security cannot be isolated from any telecommunication network.

G. Lapiotis, et al., in paper [7] presented that scalability is also an important challenge to be addressed in any security system. These scalability issues are presented in conjunction with local policy autonomy. They have developed auto system administrator with respect to network changes. The system is higher in speed and difficult to manage by human beings.

J. Burns et al., have focused on automatic management on network [8] security policy. In automatic management, the end user has not been considered for any authentication during sudden attack from outsider. The importance of safeguarding [9] and [13], the end user device due to increasing danger of root kits has been presented. These malware will modify the operating system of mobile devices and information in devices. Most of the malware used to target Android Operating systems. The new end user mobile devices are the main sources of denial of service attacks, and so on. In recent days, smart phones are targeted as attractive elements for attacker. This makes the attacks more dangerous.

WLAN security system needs, [10] and [11], high expensive management and equipment with respect to a local server for each wireless security policy zone. The security framework designed for wired network is not suitable for wireless network. The reason is mobility and changes in network topology parameters. A common framework can be designed which is more expensive and complex in nature. In WLAN network security, the network is divided into several wireless policy zones.

The problem arises [12] due to disconnection of mobile for battery exhaust is identified. The time at which connection establishes from disconnection point gives an opportunity for an attacker to overcome security threats.

In our paper, an authentication system has been proposed, where both network and mobile devices will be protected from any external attack. The gesture based fingerprint authentication and secret code; both are used as a tool for verification of authentication before connection will be established.

III. PROPOSED GESTURE BASED FINGERPRINT AUTHENTICATION SYSTEM

We have proposed a Gesture Based Finger Print authentication system which detects an attack on network and mobile device. The network should be preserved and mobile should not be used as an attacking tool which harms the network. The attacker is considered as malicious user. They used to access system configuration like password, data stored in the device, and also they may affect some or all network functions [14]. Fig 1 shows the four main parts of the authentication system architecture. The system consists of Mobile device connected to 4G network, Information Collection Center (ICC), Data Base, Security Policy with Administrator.

As soon as link is established between mobile device and network, proper authentication is performed inside the data base. The mobile equipment will be verified for fingerprint authentication from a user mobile. The data base analyses the details of mobile devices through ICC. After analysing the data, the information will be send to administrator. If authentication is confirmed, the connection is established. The data flow is shown in Fig 2. Initially, for the first time, the user has to get register themselves.
As user get registered, the network provider will allot a secret code for each mobile device or user. The mobile device’s IMEI number will be automatically saved against secret code and gesture. The user has to enter their gesture based finger print on the mobile device in addition to secret code provided by network provider through mobile device. If the authentication is passed, a complete connection is established. If the authentication is failed, two more chances are provided to a user. If authentication fails still further, mobile device is treated as a stolen device and the entire device is get blocked by the network. The IMEI number is transferred to administrator for further action. The user may also be treated as unknown user. The device is treated as a dummy device. The device will not be allowed to use in future. The device details will be stored in a database for future reference. The entire operation is shown in Algorithm 1.

A. Information Collection Center (ICC)

The ICC collects all the details of the mobile devices like hardware, IMEI number, operating system etc. A complete database will be maintained for each and every mobile device, as and when they get connected provisionally for network. The flow of complete data from Information Collection Centre to Administrator is shown in Fig 2.

B. Data-Base

The Database will receive and saves the data from the Information Collection Centre. The Database will checks the data from the mobile device for secret code and gesture based finger print for authentication purpose. If the authentication doesn’t passes even though after two more chances, the database will immediately send a message to administrator or network service provider for non-authentication. The stolen device with IMEI number details can be transferred to nearby police station for immediate action. The network connection cannot be established henceforth. The details of the devices will be stored in a database for future reference.

C. Security Policy and Administrator

The Security Policy is a set of rules which defines the functions for maintaining very good security in any authentication system. Whenever any security system is developed, it is mandatory to develop another system which identifies the policies and responsible for ensuring these policies to be followed carefully and ever. The Administrator keeps on updates new policies as and when it is framed and new settings when the policies are out-dated. The important functions of administrator are (i) to overcome any mismatch between policies and status of the network (ii) to check whether domain of the network and entities are together working in a better way. If the administrator receives any data from database regarding mismatch with entered data in mobile device and database, the device will not be allowed to access the network.

The security policy levels are classified into two levels:

- Normal Level
- Danger Level

When authentication passes, the authentication system will work normally, by simply monitoring all functions.
• When authentication fails, level is called as dangerous level. During this level, Administrator retrieves the data from database. As soon as the authentication system overcomes dangerous level, system moves to normal level. The data will be stored in the security database for future reference.

<table>
<thead>
<tr>
<th>Algorithm 1 Proposed Algorithm for Authentication System Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Begin</td>
</tr>
<tr>
<td>2: Obtain the identity of a mobile user (gesture based finger print)</td>
</tr>
<tr>
<td>3: Store the data in a database</td>
</tr>
<tr>
<td>4: Assign a secret code (unique) to a mobile user</td>
</tr>
<tr>
<td>5: Call get disconnected</td>
</tr>
<tr>
<td>6: User makes a call</td>
</tr>
<tr>
<td>7: Verify the data (entered gesture and secret code) for authentication</td>
</tr>
<tr>
<td>8: if authentication passes then</td>
</tr>
<tr>
<td>9: connect a mobile device to a network</td>
</tr>
<tr>
<td>10: end if</td>
</tr>
<tr>
<td>11: if authentication fails, give two more chance for entering the identity</td>
</tr>
<tr>
<td>12: Even though authentication fails, make a note of that device</td>
</tr>
<tr>
<td>13: end if</td>
</tr>
<tr>
<td>14: Device should be listed in separate data base</td>
</tr>
<tr>
<td>15: Device is considered as an attacking tool</td>
</tr>
<tr>
<td>16: if the same device tries to make a call in future, should not be allowed</td>
</tr>
<tr>
<td>17: end if</td>
</tr>
<tr>
<td>18: if authentication passes, a careful track is required</td>
</tr>
<tr>
<td>19: The device may get connection through blue tooth with other devices</td>
</tr>
<tr>
<td>20: The device suffers from a attack through some other device</td>
</tr>
<tr>
<td>21: Other devices may try to grab the details of the new device</td>
</tr>
<tr>
<td>22: The attacked device should be blocked from the connection</td>
</tr>
<tr>
<td>23: end if</td>
</tr>
<tr>
<td>24: The message should be sent to administrator through application layer, the connection is not established for particular device</td>
</tr>
<tr>
<td>25: The second/other device(s) are also considered as attacking tool even though they are authorized user</td>
</tr>
<tr>
<td>26: Network is protected from any damage</td>
</tr>
<tr>
<td>27: Device is also protected from retrieving any data or files</td>
</tr>
<tr>
<td>28: Both network and device are protected from malicious attacks</td>
</tr>
</tbody>
</table>

343
IV. EXAMPLE OF AN AUTHENTICATION SYSTEM DURING AN ATTACK

The example on which the authentication system architecture works is as explained below. The user identity is obtained with the help of gesture based fingerprint data. The same data will be stored in the database and a secret code is assigned to the user by the network provider. The user has to enter their unique code and gesture based fingerprint through their mobile. The device is loaded with Android Operating system. This Android Operating System is compatible with identifying the gesture entered by mobile user. This device consists of system image and image consists of Android configuration files. The configuration files can be accessed with READ and WRITE functions. As soon as the user makes a call, the person has to enter unique secret code followed by pre-defined gesture on the touchpad screen of their mobile device. The Information Collection Centre retrieves the user mobile device data. The data will be sent to database for verification. The entered data (both unique code and fingerprint) will be verified for authentication with pre-stored data. If the authorization fails, two more chances are provided for the user. Even though authentication fails, the user mobile device details will be stored in the database immediately. Information will be sent to Administrator for further action. The connection will not be established. The device will be treated as an attacking tool. The stored IMEI number will be retrieved from the database and other details of the mobile will be transferred to Police Station for further action. If the call is made from the same mobile in future, the device will not be allowed to access the network. The network is protected from such malicious attack from unknown user. If the authentication passes, the call will be connected successfully. The Administrator used to have continuous track on the connected mobile. The device may be connected to some other mobile devices inside heterogeneous wireless network. There may be chances of attacking of any mobile device which may grab the data from neighbouring devices. The Administrator may keep track...
of all devices connected to a network. After authentication passes, if any device is considered as malicious, the administrator have complete authority to save the details of such devices and the call may be disconnected immediately or blocked in future.

The Authentication System Architecture should follow the guidelines provided by TMN M.3400 Exception Report and Theft of Service actions related function sets. In the report, they have mentioned that, mobile device should be totally isolated and should not be allowed to use the network. The device is treated as an attacking tool. They may grab the detail of the network, network provider. They may perform any type of harm to the network and may affect other devices connected to the same device inside heterogeneous wireless network.

The Administrator will prevent the user’s access and keep away the malicious device from the network by having a contact with service and application in Y-Comm [5] architecture security model. The model is mainly responsible for authenticating the user. The database will keep a track of data of mobile device where authentication fails. The stored data helps in future for fast detection of the same device, if the user calls with same device. The Fig 4 shows the order at which the functions inside the architecture took place.

V. SIMULATION RESULT

A. Simulation Setup

The simulation environment is shown in Fig.3. A heterogeneous wireless network has been considered for the purpose of testing the complete algorithm. Assuming two types of network, GSM and WiFi, a new mobile equipment is made to connect for existing network. In addition to call establishment, the new device will be get connected to other existing devices inside heterogeneous wireless network. The entire network is connected to database through security administrator.

The complete sequence of operation is clearly shown in Fig 4. The entire connection will be established only when 100% authentication is performed. For trial purpose, the three secret code and three different gestures have been considered. They have been allotted with secret code on first come first entry into the network.

When the corresponding secret code and gestures are plotted, the entire system shows linearity characteristics. If the authentication is not confirmed, connection will be failed. This results in non-linearity in nature. Fig. 5 shows the Linearity characteristics exhibited by heterogeneous wireless network. The Fig 6 and Fig 7 show non-secured nonauthentication and secured authentication system respectively. The Fig 8 shows the result comparison of existing method with proposed method. The proposed method shows higher degree of performance in terms of efficiency.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we have proposed the Gesture Based Security Architecture of an authentication system in a heterogeneous wireless network. The authentication system is totally gesture based finger print authentication system. The system is aimed to safeguard both network and mobile device. The device is completely blocked for using as attacking tool. The mobile device should be loaded with android operating system and should be dealt with touch screen facility. This helps in getting the gesture of a user for authentication system. The administrator is provided with automatically updating the policies to database. Because the policies are keep on changing.

The system can be still improved for fast changing network. Since finger print is a unique identification for any human being, gesture based finger print authentication system provides high significance in avoiding any malicious attacks. The mobile is prevented at earlier stage, detected in a second stage and avoided in a third stage. The complexity of mobile security due to handoff can also be minimised for a greater extent in an extended work and higher degree of security can be achieved.
Fig 4. Sequence of Operation inside Security System

Fig 5. Linearity Characteristics of a Network

Fig 6. Non-secured non-authentication System

Fig 7. Secured Authentication System

Fig 8. Simulation Result Comparison
REFERENCES


