ISSN: 0975-766X
CODEN: IJPTFI
Available Online through ***Review Article***
www.ijptonline.com

A SURVEY ON DETECTION OF SPOOFING ATTACK USING FINGERPRINT ANALYSIS METHOD IN MANET

[1*]Samik Roy Choudhuri, [2] P. Visalakshi
[1]PG student, CSE department, SRM University, Kattankulathur.
[2]Assistant Professor, CSE department, SRM University, Kattankulathur.
*Email:*samik.works @gmail.com*

Received on 11-01-2017 *Accepted on: 03-03-2017*

Abstract: As the technologies are increased, spoofing attacks in MANET are becoming a serious concern. The fingerprint reorganization is considered to be one of the most widely used biometric technologies. In this project, fingerprint authentication system for the privacy protection is introduced. By extracting minutiae points from one fingerprint and orientation of fingerprint, a new biometric authentication system is proposed for identifying an individual. The main objective of this project is security and privacy of mobile nodes. In order to attain high security and privacy liveness detection technique is applied to distinguish legitimate user and imposter user. The virtual identity is compressed and stored in the database.

Keywords-Spoofing attacks, Manet, Fingerprint recognition, Biometrics, Fake fingerprints, Database.

1. Introduction:

Biometrics technology is an example of the automated recognition system. Using biometric technology we can measure and analyze the human body characteristics such as fingerprint, face, iris, voice, and signature. Biometric methods are secure for identification and authentication. Now a day's biometric recognition system faces many challenges like unauthorized access to the individuals and effectiveness of the system is hampered. Spoofing attack it can be defined as a method of falsifying the biometric system. Fingerprint biometrics spoofing techniques involve placing genuine fingerprint or fake fingerprint in the fingerprint scanner. Liveness fingerprint detection can be either real or fake. This paper focuses on spoofing or its identification techniques using fingerprint analysis method.

2. Literature Survey: Most of the work on the fingerprint spoofing detection focuses on the pore extraction, multimodal biometrics, blood flow analysis, GADE & IDOL mechanism. It is hopeful that a detailed description of the features can be extracted to detect the spoofed sample and valid sample.

[1]Marcela Espinoza & et.al discussed about using the number of pores on fingerprint images to detect spoofing attacks. They are using two methods Direct & Indirect to detect a number of a fake fingerprint. In the direct method, two materials were used to reproduce the inverse of the friction ridge skin: a thermoplastic (Utile Plast, produced by Pascal Rosier) and a silicon molding paste (Siligum, produced by Gedeon).In the direct method simply fingerprint is taken in a glass. The image is then processed using Adobe Photoshop CS2 software and then printed on an acetate sheet using a printer. It is used as a blueprint. For each acquisition, two images were captured. The first image is captured in a normal condition means that the user or the fake user was allowed to press his finger on the scanner without any instruction. The second image is captured in an upward movement. Then a pore extraction algorithm is developed. It has less false acceptation rate and false rejection rate. But this method holds some disadvantages like it is not generalized.

[2] S.Raguvaran discussed about how Spoofing attack can be detected in the wireless network. He used Hash Generation algorithm and frames for authentication. In the hash generation it's a two-way communication, it should return the identical hash value. Here he used the basic principle of a hash function and its inputs are Computer name, CPU id. In frames for the authentication method, he implemented an effective algorithm for the authentication process. In his proposed system, he used two implementations for detecting spoofing. One part is to identify the uniqueness of the client address and other is to make the modification access point control list in each client. He used two algorithms (i) Authentication Process and (ii) Re-Authentication Process. The main advantage of this method is hash gathering because it cannot be fractured by the spoofed user. But the disadvantage is that spoofed user increases access none of the algorithms will work. [3] Prof. Santosh S. Sambre and et.al discussed how spoofing attack can be detected in the wireless network. They built an intermediate or dummy node which lies between the server and the users. The main advantages of this dummy node are it ignore the request by the imposter user and reduce the traffic. They are using two steps (i) GADE(Generalized Attack Detection) & (ii) IDOL(Integrated Detection and Localization Framework). In GADE it first determines the number of attackers present in the network. And in the IDOL it detects and locates the attacker. IDOL is an integrated system. They used RSS algorithm and K-mean algorithm. This method has an advantage using this method we can easily detect fake users and lock for the lifetime. But it has some disadvantage like it's not possible to locate fake users all time. [4] Voravud Santiraveewan proposed a system how Spoofing attack can be analyzed using Graph-based Methodology. He used two topologies (i) Abstract network topology and (ii) Abstract firewall topology. In Abstract

network topology he includes host, servers, firewall, networking devices and the internet. Second, the abstract firewall topology represents the topology of only firewalls which are present in the network. The main advantage of this method is it can be used not only to verify configurations vulnerable to the attacks but also to generate configurations free of the attacks. This method also has several disadvantages such as firewall not present in the network, it cannot detect the legitimate user.

[5] Asier Martinez proposed a system using the Beacon Frame. Using this Beacon Frame he detects spoofing attack in IEEE 802.11 Networks. He modifies the firmware of the access points and 802.11 cards in order to log the transmitted data. Beacon Frames must be transmitted in a regular interval. This interval was specified by the access point and it’s circulated in the network. If a frame does not maintain the interval then it's denoted as a malicious. The main aim is monitoring the time intervals between Beacon Frame. The main advantage of this system is it can be implemented in Ad-Hoc network. But it has the drawback that if the network is congested it cannot detect the imposter user.

[6] Ajay Kumar proposed a method using blood flow analysis. In this method, he estimates the percentage of oxygen-saturated blood by using LEDs. It operates on a selected wavelength. In this method, he collects an individual’s identity, oxygenated blood measurement (the saturation of oxygen in hemoglobin), and pulse (taken from the fingertip).It checks the proportion of oxygenated blood (SpO2%) in the biometric sample. The main disadvantage of this method is it operates on a selected wavelength.

[7] Jeong Heon Lee and R. Michael Buehrer developed a method to detect spoofing attack in Wireless Networks. They proposed a statistical and pattern matching techniques known as relative error detection (RED) and topological residual fingerprint matching (TRFM).Using these two techniques they detect both signal strength and beam forming attacks. They also used the geometric technique to improving reliability. They develop an idea termed Geometric Filtering for reliable attack detection and localization. The main advantage of this method is fast detection. The major drawback of this system is they did not use database concept to store data. [8] Qi Zeng, Husheng Li, and Lijun Qin established a method for GPS Spoofing Attack on Time Synchronization in Wireless Networks and Detection Scheme Design. Global position system (GPS) has been used in a variety of wireless applications, like mobile ad hoc network, cellular phone network, smart grid and etc. The CUSUM algorithm was developed for detection of GPS spoofing attack as quickly as possible. It works in this way, detection of a packet is failed if the frequency hit occurs during the packet interval;

otherwise, the detection is successful. This CUSUM algorithm is available in other wireless communication devices which are harmful to the GPS spoofing attack.

[9] Ying HAO, Tieniu TAN, Yunhong WANG proposed an algorithm for fingerprint matching. Fingerprint matching its similar to pattern matching. This fingerprint matching algorithm is based on error propagation. They are trying to match minutia points. This team used common region estimation technique. The first fingerprint is divided into N sectors, then find the farthest minutia in both referenced and input object. After this, they estimate common region boundary and lastly minutia points are counted. The main drawback of this system is if ridge segments are extracted then the result will be different. [10] Mouhannad Alattar, Franc¸ oiseSailhan and Julien Bourgeois proposed a method using Log-based Link to detect spoofing attack in MANET. They proposed IDAR, log and signature-based intrusion detection system that periodically collects logs(packet reception).It has some steps (i) Suspicious-Evidence (ii) Initial-Evidence (iii) Confirming Evidence (iv) Cancelling Evidence.

They proposed an advanced investigation algorithm.

```
STEP 1: Suspicious MPRs= new (MPR)
STEP 2: Old MPRs = Get Replaced-MPR ();
STEP 3: for (suspicious 2 Suspicious MPRs) do
STEP 4: Common2HopsNeighbors = GetCommon2HopsNeighors (suspicious, Old MPRs)
STEP 5: for (2HopsNeighbor 2 Common2hopsNeighbors) do
STEP 6: if (Verify Link (2HopsNeighbor; suspicious) == false) then
STEP 7: Generate Alarm (Suspicious);
STEP 8: Terminate (Suspicious);
STEP 9: end if
STEP 10: end for
STEP 11: Cancel the suspicious;
STEP 12: Suspicious MPRs=Suspicious MPRs - suspicious;
STEP 13: end for
```

Where MPR= Multipoint Relay

This method shows a high rate of intrusion detection and low false positive rate even under increased mobility and density. [11] Wesam S. Bhaya and Suad A. Alasadi proposed a system how to detect spoofing attack in Mobile Ad Hoc Networks. In MANET devices can communicate each other without any network infrastructure or any centralized administration. In Manet devices used open medium and dynamic topology. IEEE 802.11 MAC frames used to hide the identification data in order to distinguish between the true frame and the false frame. The proposed system has several steps. These steps are run by the sender and receiver nodes.

At the sender side:

(i) Capture IEEE 802.11 MAC Frame: connection is established between sender and receiver then capture MAC frame.
(ii) Steganography: hiding hostname of the sender and sequence number of the sequence control field.
(iii) Encryption: Information is encrypted using encryption algorithm.
(iv) Send IEEE 802.11 Modified Frame

At the receiver side:

(i) Analyze the Received Frame: extract the frame field and get the Third MAC address field.
(ii) Decryption: decrypt the hostname of the sender and sequence number of the sequence control field.
(iii) Matching: receiver node search in the list
(iv) Determine the Frame Type: receiver determines the frame type whether it is spoofed frame or a real frame. If it is spoofed frame then it will discard the frame.

The main advantage of this system is it doesn’t require any additional overhead and bandwidth.

3. Procedure:

Step 1: Fingerprint is taken.
Step 2: Fingerprint is converted into the Binarized image.
Step 3: Segmentation is done on Binarized image.
Step 4: Then Thinning is done on the segmented image.
Step 5: Minutiae points are extracted from the thinned image.
Step 6: Live fingerprint is checked with stored fingerprint if both the fingerprints are matched then the user is authorized else it shows imposter user.

4. Conclusion:

In this paper various spoofing detection methods were analyzed and among them Marcela Espinoza’s [1] system which combines two methods direct and indirect performs well for identifying the spoofed fingerprint and valid fingerprint. It has the capability to extract the liveness characteristics. Using the pore extraction algorithm it can easily distinguish between the valid fingerprint and spoofed fingerprint. It has an advantage of providing better security, efficiency, performance and accuracy. As a future work, minutia extraction can also be taken into consideration for providing a better security and authentication.

References:

1. Marcela Espinoza, C.Champod, “Using the Number of Pores on Fingerprint Images to Detect Spoofing Attacks”, IEEE 2011.
2. S.Raguvaran, Member IEEE, “Spoofing Attack: Preventing in Wireless Networks”, International Conference on Communication and Signal Processing, April 3-5, 2014, India.
3. Arjunsingh Sushil Yadav ,Pooja Milind Natu, Deshana Manoj Sethia, Amruta Balaji Mundkar, Santosh S. Sambare, “Prevention of Spoofing Attacks in Wireless Networks”, ICCUBEA '15 Proceedings of the 2015 International Conference on Computing Communication Control and Automation Pages 164-171 IEEE Computer Society Washington, DC, USA ©2015.
4. Voravud Santiraveewan and Yongyuth Permpoontanalarp, “A Graph-based Methodology for Analyzing IP Spoofing Attack”, IEEE 2014.
5. AsierMart´ınez, UrkoZurutuzayz, Roberto Uribeetxeberriay, Miguel Fern´andezy,Jesuslizarragay, AinhoaSernay and I˜nakiV´elezy, “Beacon Frame Spoofing Attack Detection in IEEE 802.11 Networks”, 2008 IEEE.
6. Ajay Kumar, “Fingerprint spoof detection using blood-flow analysis”.
7. JeongHeon Lee and R. Michael Buehrer, “Location Spoofing Attack Detection in Wireless Networks”, 2010 IEEE.
8. Qi Zeng, Husheng Li and Lijun Qian,“ GPS Spoofing Attack on Time Synchronization in Wireless Networks and Detection Scheme Design”,2013 IEEE.
9. Ying HAO, Tieniu TAN, Yunhong WANG, “AN EFFECITVE ALGORITHM FOR FINGERPRINT MATCHING”.
10. MouhannadAlattar, Franc¸oiseSailhan and Julien Bourgeois, “Log-based Link Spoofing Detection in MANET”.
11. Wesam S. Bhaya and Suad A. Alasadi, “ Security against Spoofing Attack in Mobile Ad Hoc Networks” , European Journal of Scientific Research ISSN 1450-216X Vol.64 No.4 (2011), pp. 634-643.