Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 3, March -2017

WIRELESS SECURE CONNECTION ESTABLISHMENT USING STEGANOGRAPHY

[1]Songhoti Adak, [2]Priya Patil, [3]Sanvedna Khaire, [4]Sunayna Patil
[1,2,3,4] Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Pimpri, Pune

Abstract - *According to IEEE 802.11 protocol, Access Point(AP) periodically transmit beacon frames which carry mostly network specific information. All the wireless stations , also known as wireless clients within the vicinity of transmission range of AP receive corresponding beacon and use the information embedded in it for various purposes. The larger channel width of IEEE 802.11 is supported by ns3. Various permutation algorithms are studied and implemented. One of the efficient algorithms of permutation will be used as a key, encoded at the access point*
The key will be decoded by the end user for providing security over the transmission. In this ,the Time stamp field of the beacon frames will be modified by adding the key and then that will be encoded with the help of protocol stenography. For generation of permutation, a pseudo random code generator will be used according to its efficiency. Ns3 is used for the simulation process. It is used because it studies the system behavior in highly controlled and reproducible manner.

Keywords: *Beacon Frame, Beacon Probe Request/Response, Wireless communication, Rouge Access Point, tenography.*

I. INTRODUCTION

If an authorized device receives the connection from the access point then the decoding algorithm will be applied and the secret key will be decoded, thus the connection is established. If spoofing occurs and a rogue access point behaves as the end point ,then the key will not be decoded it will be unaware of the exact decoding permutation algorithm .IEEE 802.11 wireless networks are extremely popular worldwide. There is a tendency to extend their range and throughput. There are a few reasons for such a situation. In the first place, the availability of devices using this standard they are more popular than other devices using this standards(e.g Bluetooth or WiMAX). Secondly they are easy to set up. IEEE 802.11 standard allows for creating a simple wireless network an deprovíding it with sufficient security without the need to have any speciality knowledge. Thirdly, the large number of devices practically each new portable PC,tablet or a cell phone is equipped with an IEEE 802.11 communications module. In this project we are using efficient permutation algorithms and the permutations will itself serve as a key used for encoding and decoding in steganography. We will be using some bits of beacon frames to embed the key in it and transmit. In our project we have collaborated two major domains of technology namely Wireless networks and network security to realize the notion of secured connection over the internet.The use of protocol steganograhy itself is indicative of the fact that we have endeavoured to impart maximum security over wireless channels. The concept of using efficient permutation algorithm enables the secret key not to be broken easily by any rogue access point or intruder or hacker .When the topic of communication over wireless medium comes up, security is the most challenging feature and we are trying to combat this problem. The visualization of the entire process will be shown in ns3.The main aim of this project is to provide a secure connection between access point and end point and to detect the rogue access points if any. Beacon frames are continuously transmitted from access point and carry mostly network specific information. All the wireless stations within the vicinity of transmission range of access point receive corresponding beacons and use information embedded in it for various purposes. Apart from providing the confidentiality of transferred information by encryption frame sent ,it is also ,it is also necessary to ensure the authentication of all stations and access points. The covert channel is performed using Beacon frames and Timestamp fields and takes advantages of the least significant bits of these fields[3].Using Steganography is one of the possible ways to solve the problem of Access Point Authentication .As it is associated with the modification of the information transferred to hide additional information, such method should be classified as active methods.

II LITERATURE SURVEY

1. This paper proposed that on the transmitted data of beacon frame some additional information can be embedded without breaking the standards and, in fact sometimes without increasing the size of beacon also. The implementation depends on the application and information to be embedded.Considering the IEEE 802.11-2007 protocol, in this paper it has been shown that without violating the standard ,in a beacon frame to carry additional non standard information there are few fields which can be utilized. Other than the fields proposed by R. Chandra et al ,it shows that the length field is also the potential candidate for the same. Using it, without consuming any extra channel/network resources about 10 octets of additional non standard information can be broadcasted . Of course, what information is to be embedded depends upon the application requiring it and how to use these fields [1].

2.Bypassing cellular base stations or access points in D2D communications, facilitate proximal devices to communicate with each other directly and bring many benefits. These benefits include improvement in spectral efficiency and energy efficiency., WiFi Direct is one promising protocol, among existing D2D enabling techniques , that offers high data rate D2D communications in local areas. However, WiFi Direct is susceptible to security threats due to the lack of security and infrastructures open access of wireless channels . Several attacks challenge WiFi-Direct-based D2D communications according to this article. Since pairwise key establishment lies in the area of securing D2D communications, this paper introduces a short authentication-string-based key agreement protocol and analyze its security performance. Implementing its usage in Android smartphones, this paper also integrates the SAS-based key agreement protocol into the existing WiFi Direct protocol.[2]

3. **Robert Sedgewick's proposed idea** surveys the large number of methods that have been proposed for permutation detailing by computer. The various algorithms which have been developed are described in detail, and implemented in a modern ALGOL-like language. All of the algorithms are derived from one simple control structure. The problems involved with mplementing the best of the algorithms on real computers are treated in detail. Assembly-language programs are derived and analyzed fully. This paper intended not only as a survey of permutation generation methods, but also as a tutorial on how to compare a number of different algorithms for the same task.[3]

4.With the advance of network technology digital communication has become an essential part of infrastructure nowadays. The Internet is widely used as a medium for communicating and transferring information. The network security is becoming more important as the amount of data being exchanged on the Internet is increasing. Security requirements are necessary for the information transmitted which requires features of security like identification,confidentiality, non repudiation, integrity control and availability from the sender level up to the receiver level. This is resulting in a huge growth in the field of information hiding, by providing secured communication between two or more computers, for exchanging confidential data like passwords,credit card numbers, usernames, and tender amount etc. by preventing hackers from hacking the confidential data. This paper proposes a system that provides a novel method for secure data transmission using steganography by hiding data in TCP/IP header.[4]

III. ALGORITHM

Pseudo Random Number generation:-

Step 1:-The selected key characters are first replaced by their binary representations. Let the entered key consists of n-characters, then the length of this key will be 8*n (i.e. n-bytes).

Step 2:-A bitwise XOR operation are performed on the bit blocks of each two successive bytes, i.e. (1stXOR2nd) replaces the 1stbyte, (2nd XOR 3rd) replaces 2nd **character, etc., until the last byte where it is XOR'ed with** the first one, or (nthXOR1st) replaces the nth-byte.

Step 3:-Successive bytes are exchanged with each other in pairs. However, if n is odd number, then the last byte is left unaltered.

Step 4:-The resulting bit string of the previous step is divided into halve, left and right each of 4*n bits length. The resulting bit sequence of 8*n can be taken as the first pseudo random random key K1.

Step 5:-The generated key in step 4 can be fed back as an input to step 2 in order to generate next random key.

Step 6:-In order to generate more keys, steps 2-5 can be repeated as many as required.

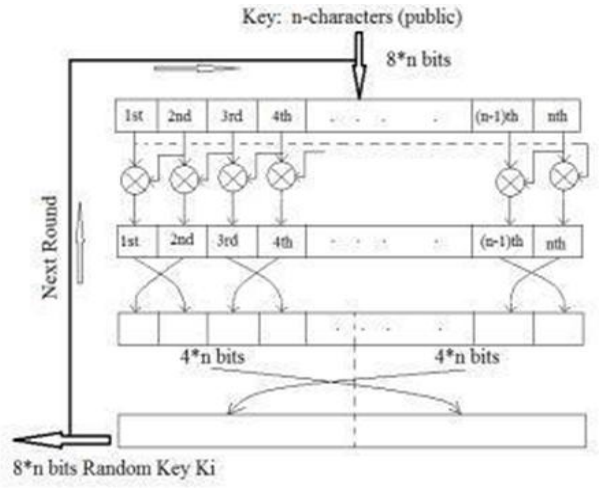

Fig.: Pseudo random Generator

IV. SYSTEM ARCHITECTURE

In our project we have collaborated two major domains of technology namely Wireless networks and network security to realize the notion of secured connection over the INTERNET. The use of protocol stenography itself is indicative of the fact that we have endeavored to impart maximum security over wireless channels. The concept of using efficient permutation algorithm enables the secret key not to be broken easily by any rogue access point or intruder or hacker. When the topic of communication over wireless medium comes up, security is the most challenging feature and we are trying to combat this problem. The visualization of the entire process will be shown in ns3.

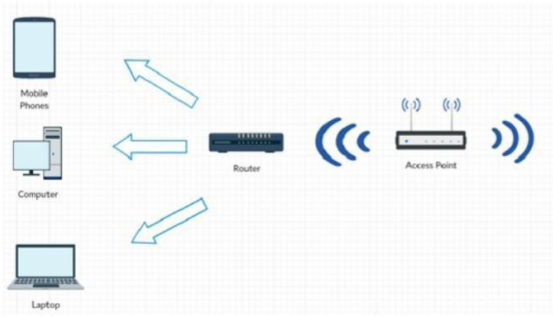

Fig.: System Architecture

Experimental setup:

Authentication: 802.11 authentication is the first step in network attachment. 802.11 authentication requires a mobile device (station) to establish its identity with an Access Point (AP) or broadband wireless router. No data encryption or security is available at this step. The Institute of Electrical and Electronics Engineers, Inc.(IEEE) 802.11 standard defines two link-level types of authentication:Open System and Shared Key.

Open system authentication: Open system authentication consists of two communications:

1. First, an authentication request is sent from the mobile device that contains the station ID (typically the MAC address).

2. At next step, an authentication response from the AP/router with a success or failure message. Shared key authentication With shared key authentication, a shared key, or passphrase, is manually set on both the (/content/www/us/en/homepag e.html) mobile device and the AP/router. Several types of shared key authentication are available today for home or small office WLAN environments. Here , we are using permutations generated from the most sought out and efficient permutation algorithms Association

Once authentication is complete, mobile devices can associate (register) with an AP/router to gain full access to the network. Association allows the AP/\ or the router to record each mobile device so that frames are properly delivered. Association only occurs on wireless infrastructure networks, not in peer-peer mode. A station can only have association with one AP/router at a time.

Association process:

1. Mobile device authenticates to an AP/router and then sends an Association Request.

2. AP/router processes the Association Request. AP/router vendors may have different implementations for deciding if a client request should be allowed or not. When an AP/router grants association, it responds with a status code of 0 (successful) and the Association ID (AID). The AID is used for identification the station for delivery of buffered frames when power-saving is enabled. Failed Association Requests include only a status code and the procedure ends.

3.AP/router forwards frames to or from the mobile device. The three 802.11 connection states are: Not authenticated or associated. Authenticated but not yet associated. Authenticated and associated.

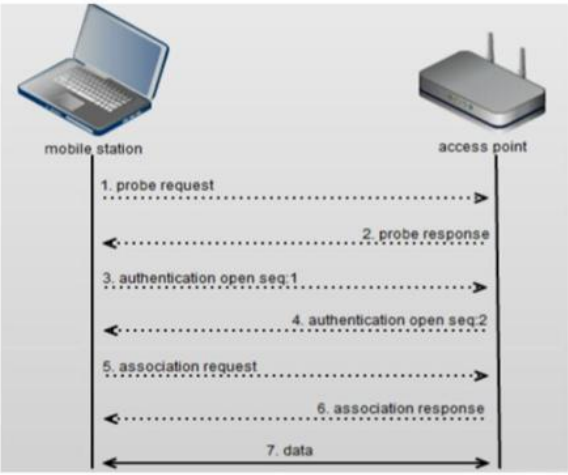

Fig.: Communication between two points

When a mobile station starts, it is not authenticated and associated.

1. probe requests are sent by a mobile station to discover 802.11 networks within its proximity. Advertisements are done by probe requests which the mobile stations supports data rates of 802.11 capabilities such as 802.11n. Since the probe request is sent from the mobile station to the destination layer **address and BSS ID of type ff:ff:ff:ff:ff:ff, all AP's** that receive it will respond.

2. Access Points that are receiving the probe request check to see if the mobile station has at

least one common supported data rate. If there is compatible data rates, a probe response is sent advertising the SSID (wireless network name), supported data rates, encryption types and other 802.11 capabilities. A compatible network is chosen from the probe responses by mobile station and receives it. Compatibility could be based on encryption type. Once a mobile station determines which AP it like to associate to, it will send an association request to that AP. The association request contains required encryption types if necessary and other compatible 802.11 capabilities. Now the mobile station is successfully associated to the AP and data transfer can begin**.**

V. CONCLUSION

There is an immense need to provide security to the connection between access point and end point. Permutation is generated and used as a pass key. Steganography is used for encoding and decoding data. With help of decoding mechanism the identification of rouge access point can be done. Spoofing is avoided and secure connection is establish.

VI. REFERENCES

1] Vishal Gupta, Mukesh Kumar Rohil , Information Embedding in IEEE802.11 Beacon Frame, Published in IJCA ,2012.

2] Secure Device-to-Device Communications over WiFi Direct

3] Robert Sedgewick Permutation Generation Methods , Computer Survey , Vol. 9 , No 2 June 1977,138.

4] N.F.Johnson and S.Jajodia,Exploring steganography : Seeing the unseen,Computer ,Vol.31, No.2,pp.26-34-1998.

5] Krzysztof Sawicki, Zbigniew Piotrowski, The Proposal of IEEE 802.11 network access point authentication mechanism using covert channel ,Published in MKON 2012,19th International Conference on Microwaves, RADAR and Wireless Communication ,May 21-23,Warsaw,Poland.

6] Institute of Electrical and Electronics Engineer ,Wireless LAN medium Access Cotrol and Physical Layer Specification, IEEE Standard 802.11,2007.

7] Y.Song ,C.Yang,G.gu, Who is Peeping at your Password at Satrbucks? To catch an Evil Twin Access Point ,International Conference on Depemdable Systems and Network,Chicago,US,2010.

8] grnenberger Y.,Rousseau F. Virtual Access Points for transparent Mobility in wireless LANs.In proceedings of IEEE Wireless Communications and Networking Conference(WCNC)(Sydney,Austrlia,April 18 - 21,2010)

9] Nicolson A.J Wolchok S. ,Nobel B.D. Juggler :Virtual Network for Fun and Profit. IEEE Transaction on Mobile Computing ,Vol.9,no-1,pp.31-43,Jan-2010

