International Journal of Scientific Research and Management (IJSRM)
||Volume||5||Issue||06||Pages||5490-5497||2017||
Website: www.ijsrm.in ISSN (e): 2321-3418
Index Copernicus value (2015): 57.47 DOI: 10.18535/ijsrm/v5i6.21

Design of Unique Auto Disconnect Password Generation for Public Wi-Fi Routers

Mr.T.M.Hayath[1], Ms.Akhila Kurni[2], Ms.Aishwarya Hiremath C[3], Ms.Sinduja J[4], Ms.Anita V Patil[5]
[1]hayathmail@gmail.com,[2]kurniakhila.ka@gmail.com,[3]ishwarya7979@gmail.com,[4]sinduja.u25@gmail.Com,[5]anitavpatil5464@gmail.com
[1]Assistant Professor,[2,3,4,5]UG Scholars, Department of Computer Science and Engineering,
Ballari Institute Of Technology And Management, Ballari, Karnataka, India.

ABSTRACT:

WI-FI has emerged as the single most popular wireless network protocol of the 21st century. While other wireless protocols work better in certain situations, WI-FI technology is used in many organizations and in other public places which often provide free access to wireless internet hotspots. Wi-Fi networks are prone to virus attacks. Wi-Fi Protected Setup (WPS) contains a design error that could allow a weaker-than-expected defense against brute-force attacks, which could allow an attacker to gain unauthorized access to the affected system. Do note that brute-force attack is a programme that hackers often use to crack and stealthily enter into an encrypted and password protected system. Usually, users in India opt the WPS method to set up a wireless router for home network. In this method, the standard requires a PIN to be used during the setup phase. By design this method is susceptible to brute force attacks against the PIN, said the agency in an advisory issued with high severity ratings.

An unauthenticated, remote attacker within range of the wireless point could use the PIN to gain unauthorized to the device to retrieve the password for the wireless network or change the configuration of the device. It also said that some WPS devices in the country do not implement any kind of lockout policy for brute-force attempts, which greatly reduces the time to perform a successful attack. Hence to avoid such circumstances, in this paper, we are implementing unique (one time password) key generation method. Each OTP assigned with fixed sessions. During those sessions it is allowed to access an internet until session ends. Once if session expires, it gets disconnect automatically. Hence enhancing security in Public Wi-Fi and provides an open option for researchers to implement various applications in such technologies.

Keywords: Wi-Fi, LAN, OTP, WEP.

I. Introduction

Wi-Fi stands for Wireless Fidelity. Wi-Fi it is based on the IEEE 802.11 family of standards and is primarily a local area networking (LAN) technology designed to provide in-building broadband coverage. Current Wi-Fi systems support a peak physical-layer data rate of 54 Mbps and typically provide indoor coverage over a distance of 100 feet. Wi-Fi has become the de facto standard for last mile broadband connectivity in homes, offices, and public hotspot locations. Systems can typically provide a coverage range of only about 1,000 feet from the access point. Wi-Fi offers remarkably higher peak data rates than do 3G systems, primarily since it operates over a larger 20 MHz bandwidth, but Wi-Fi systems are not designed to support high-speed mobility. One significant advantage of Wi-Fi over wimax and 3G is its wide availability of terminal devices. A vast majority of laptops shipped today have a built-in Wi-Fi interface. Wi-Fi interfaces are now also being built into a variety of devices, including personal data assistants (PDAs), cordless phones, cellular phones, cameras, and media players.

Radio Signals are the keys, which make Wi-Fi networking possible. These radio signals transmitted from Wi-Fi antennas are picked up by Wi-Fi receivers, such as computers and cell phones that are equipped with Wi-Fi cards. Whenever, a computer receives any of the signals within the range of a Wi-Fi network, which is usually 300

DOI: 10.18535/ijsrm/v5i6.21

— 500 feet for antennas, the Wi-Fi card reads the signals and thus creates an internet connection between the user and the network without the use of a cord.

Figure.1 Generalized Scenario of Wi-Fi usage.

A Wi-Fi hotspot is created by installing an access point to an internet connection. The access point transmits a wireless signal over a short distance. It typically covers around 300 feet. When a Wi-Fi enabled device such as a Pocket PC encounters a hotspot, the device can then connect to that network wirelessly. Most hotspots are located in places that are readily accessible to the public such as airports, coffee shops, hotels, book stores, and campus environments. 802.11b is the most common specification for hotspots worldwide. The 802.11g standard is backwards compatible with .11b but .11a uses a different frequency range and requires separate hardware such as an a, a/g, or a/b/g adapter. The largest public Wi-Fi networks are provided by private internet service providers (ISPs); they charge a fee to the users who want to access the internet.

II. Literature survey

In paper [1], the author's expresses communication networks, which is used in internet to transfer data and to communicate in that Wi-Fi and Li-Fi are two major wireless networks. The Wi-Fi stands for Wireless Fidelity and this technology is completely established in 1999 and it is used to provide internet access to devices that are within the range of wireless network that is connected to the network Wi-Fi uses radio waves for data transfer. The Li-Fi stands for Light Fidelity is completely established in 2011 and still research is going on this technology and it is a visible light communication that uses LED's for data transfer.

In paper [2] the authors express their views that Bluetooth and IEEE 802.11 (Wi-Fi) are two communication protocol standards that define a physical layer and a MAC layer for wireless communications within a short range (from a few meters up to 100 m) with low power consumption (from less than 1 mw up to 100 mw). Bluetooth is oriented to connecting close devices, serving as a substitute for cables, while Wi-Fi is oriented toward computer-to-computer connections, as an extension of or substitution for cabled LANs. In addition to this, authors presented an overview of these popular wireless communication standards, comparing their main features and behaviors in terms of various metrics, including capacity, network topology, security, quality of service support, and power consumption.

In paper [3] states about Wi-Fi as a system of wirelessly connecting devices that use radio waves, allowing for connection

Between devices without the expense of cumbersome cables or without needing them to be facing one another and used to define the wireless technology in the IEEE 802.11b standard. It operates in the unlicensed 2.4 GHz radio spectrum, uses direct-sequence spread spectrum (DSSS) for modulation, supports variable data rates up to 11 Mbps, and has a range of about 50 meters. Wi-Fi allows users to gain convenient wireless internet access, though without the sufficient security precautions it can also let outsiders or intruders to do the same without anyone noticing. As "hot-spots" are becoming increasingly popular and cities working towards becoming entirely wireless, the authors express that, the users of Wi-Fi technology is becoming more vulnerable to cyber crime. Techno-criminal can attack a user's wireless network in order to gain free internet usage or obtain personal and valuable information. The threat of intrusion into the home wireless network has forced users to adopt a range of security. Security measures have improved since the release of the first system called Wired Equivalent Privacy (WEP). The majority of new Wi-Fi products use a system called Wi-Fi Protected Access, created by the Wi-Fi Alliance. It not only provides a 128-bit encryption of data that is being transmitted but locks on to individual computers and changes the access key every 10000 packets. It is more complicated than WEP, though it is more secure with improved authentication, authorization and encryption capabilities.

In paper [4] deals with security issues in wireless networks. As Security plays an important role in wireless networks. In the present scenario, 3G and 4G networks have separate security layers but still there is a possibility of certain prominent types of attacks. Authors have done a survey on all the possible attacks that may occur in present and future scenarios. Wireless network attacks are classified on the basis of access control, authentication, availability, confidentiality and integrity as attacks can appear in the form of Access, channel assignment and at the source end. It also reflects about the next generation attacks like Man in the Middle Attack, Denial of Service Attack and Eavesdropping. The security methods and tools which helps to find the protection against different types of attacks is also shown in this paper.

In paper [5] Authors stress on wireless networks, as wireless networks access gains popularity in corporate, private and personal networks, the nature of wireless networks opens up new possibilities for network attacks. It also includes negotiating Wi-Fi security against scanning of rogue Wi-Fi networks and other related activities and considers the monitoring of Wi-Fi traffic effects. The unauthorized access point (AP) problem has raised more attention and resulted in obtaining wireless access without subscriber permission. This work assumes WI-Fi AP under attack specially rogue AP and/or ad-hoc client. It provides a solution for detecting and preventing this attack. In addition, it provides the required user permissions to allow/block access of the files on the user of ad-hoc client. The experiments include the rogue AP attack are maintained and the effectiveness of the proposed solution are tested.

III. Wireless Network Security

Hacking wireless hardware is an endeavor steeped in a rich history of experimentation. The wireless hardware hacker of today pursues his/her craft with a passion not seen since the amateur radio operators of the last generation. Many wireless enthusiasts are, in fact, connected with the ham community. Once solely the domain of a small group of Radio Frequency (RF) engineers becomes available, wireless gear has never been so inexpensive and accessible as it is today. By small investment, you can own wireless hardware due to rapidly declining hardware costs, then anybody can learn and experiment with 802.11 equipment. There are several wireless hacks, tricks, and hardware modifications, such as D-Link DWL650 card modification for adding an external antenna, openap (Instant802) reprogramming of AP to run an open-source version of Linux, and Dell 1184 AP exploring the embedded Linux operating system.

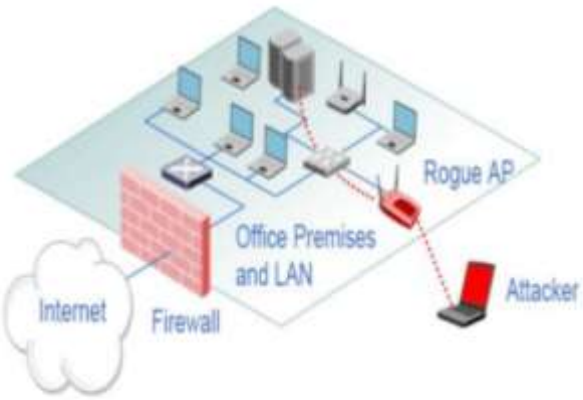
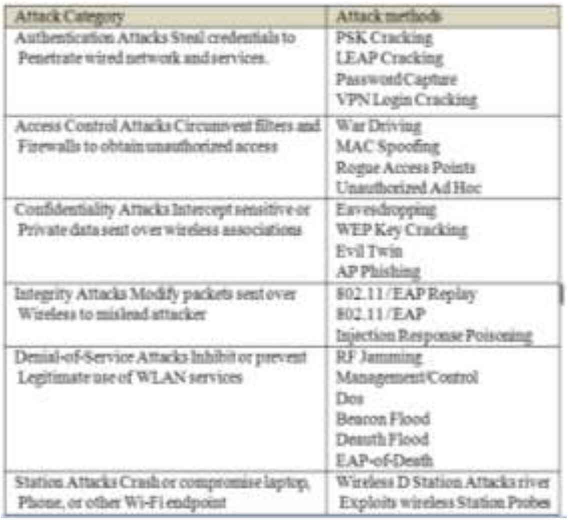


Figure.2 Firewall and Rogur AP.

WLANs attacker operated clients: using a wireless enabled laptop and couple of tools an attacker can successfully disrupt wireless service in networks few feet away. Most such Denial of Service (dos) attacks aim at exhausting AP resources such as the client-association table. Wi-Fi devices can monitor and record data in case of encryption-free. Such network devices may use a Virtual Private Network (VPN) or secure Hypertext Transfer Protocol (HTTPS) over

Transport Layer Security. Attackers are only out to log and gather information about the wireless network they find while scanning WLAN. Table 1 summarizes common 802.11 and 802.1X attack Categories, giving examples of available attack methods used by wireless intruders.

Table 1. Common 802.11 and 802.1X attack Categories



Attack Category	Attack methods
Authentication Attacks Steal credentials to Penetrate wired network and services.	PSK Cracking LEAP Cracking Password Capture VPN Login Cracking
Access Control Attacks Circumvent filters and Firewalls to obtain unauthorized access	War Driving MAC Spoofing Rogue Access Points Unauthorized Ad Hoc
Confidentiality Attacks Intercept sensitive or Private data sent over wireless associations	Eavesdropping WEP Key Cracking Evil Twin AP Phishing
Integrity Attacks Modify packets sent over Wireless to mislead attacker	802.11/EAP Replay 802.11/EAP Injection Response Poisoning
Denial-of-Service Attacks Inhibit or prevent Legitimate use of WLAN services	RF Jamming Management/Control Dos Beacon Flood Deauth Flood EAP-of-Death
Station Attacks Crash or compromise laptop, Phone, or other Wi-Fi endpoint	Wireless D Station Attacks river Exploits wireless Station Probes

.

IV.Examples of Wireless Access Control Attacks

- ✓ War Chalking:-War chalking is a practice of marking a series of symbols on sidewalks and walls to indicate nearby wireless access. That way, other computer users can pop open their laptops and connect to the Internet wirelessly. It involves marking free websites for use by wireless hobos. Smart Phones, mobile devices and wireless vendors, have condemned as bandwidth theft the placing of chalk symbols on walls and pavements at places where free wireless network access is available . It becomes a security threat when attackers freely browse corporate networks and access private information or use a network to dispatch millions of spam.
- ✓ Wi-Fi Mooching:- You are become a mooch user if you are one of those people who think an unsecured Wi-Fi connection is an open invitation to come on in, you are not alone. If you are the sort that likes to mooch off of his neighbor's unsecured Wi-Fi connection, surfing the Internet or on their dime, you might want to think about ponying up for some access of your own". Wi-Fi theft, it turns out, can land you in the clink.
- ✓ Joyriders: - When Wi-Fi connections belonging to subscribers are opened without their prior consent, this action is called Joyriders. Roaming Wi-Fi users include " Joyriders" that use an open Wi-Fi connection to access the Internet. Joyriders find and use a Wi-Fi connection outside of their home or office for a variety of purposes, including checking e-mail, web surfing, or connecting to a corporate network. The motive is to connect to the Internet without having to pay for the service.
- ✓ War Driving: - War Driving is an extension of the concept of War Dialing that deserves some explanation. It is a method popularized by a character played by Matthew Broderick in the film wargames, and named after that film. The term originates from a phone hacking technique used in the 1980s - war dialing. War dialing consists of dialing every phone number in a specific sequence in search of modems. War Driving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, Smartphone or Personal Digital Assistant (PDA). The basic idea behind War Driving is to ―sniff‖ 802.11 traffics with a wireless card set in ―monitor‖ mode so that it accepts all traffic on frequency irrespective of intended target. The ―War Driving approach is considered as an example of attacks that exploit such Wi-Fi network vulnerabilities
- ✓ Piggybacking:- Piggybacking refers to access to a wireless Internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge. During the early popular adoption of 802.11, providing open access points for anyone within range to use was encouraged to cultivate wireless community networks, particularly since people on average use only a fraction of their downstream bandwidth at any given time. Recreational logging and mapping of other people's AP has become known as war driving. It is also common for people to use open (encryption-free) Wi-Fi networks as a free service, termed piggybacking.
- ✓ Hitchhiking:- Hitchhiker is a utility that checks all public Wi-Fi aps near to your current position, and

automatically configure your Pocket PC to allow you to connect quickly . This utility is perfect to Wi-Fi user when he or she out of his or her Wi-Fi AP coverage and about and discover that he or she needs some vital online information. Hitchhiker takes away the problems of manually searching for open aps then configuring Wi-Fi user Pocket PC to connect to nearest AP.

V.Proposed Methodology

Since the introduction of Wi-Fi on mobile devices, there has been interest in incorporating so called ‘public Wi-Fi’. The rise in smart phone usage at public hotspots has increased this interest. As the popularity of Wi-Fi enabled devices to provide access to the Internet and other data services rises, applications are increasingly being developed to be independent of access type.

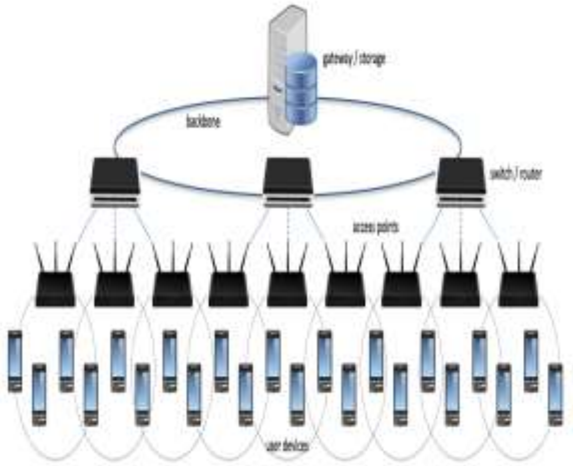


Figure 3:- Architecture of Public Wi-Fi

Architecture that utilizes IEEE 802.11i to encrypt subscriber data to the Access Point ensures privacy in the physical layer air space. Further, a new Access Point requirement, which tunnels subscriber traffic directly to and from the AP WAN interface, isolates subscriber traffic from each other at layer 2. This requirement prevents any possibility of packet eavesdropping between Wi-Fi devices.

Mainly IEEE 802.11x divides network environment in 3 parts:

1) Server, which has to perform authentication decisions.

2) An Authenticator, which has to controls access.

3) Supplicate, who wants to be connected to network.

The working of IEEE 802.11x is based on simple concept, it implement access control at connection point between user and network. It provides port security to protect network security. To achieve its goal IEEE 802.11x utilizes well known protocol such as Extensible Authentication Protocol and RADIUS.”

To design session based password protocols we are going to use unique RANDOM NUMBER GENERATOR algorithms, which generates unique numbers. These unique numbers are used as OTP, which is assigned with fixed sessions. The user has to enter OTP to access internet. Once the predefined session for a particular OTP is ends, then the user is disconnected automatically, hence providing enhanced security for public Wi-Fi.

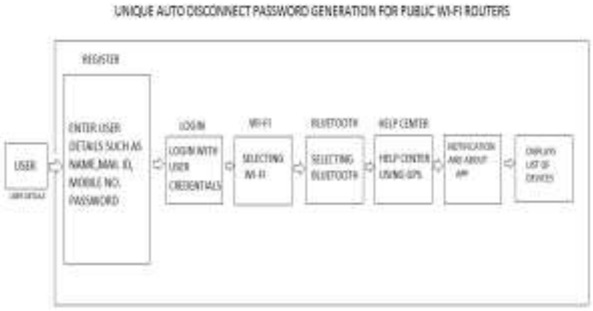
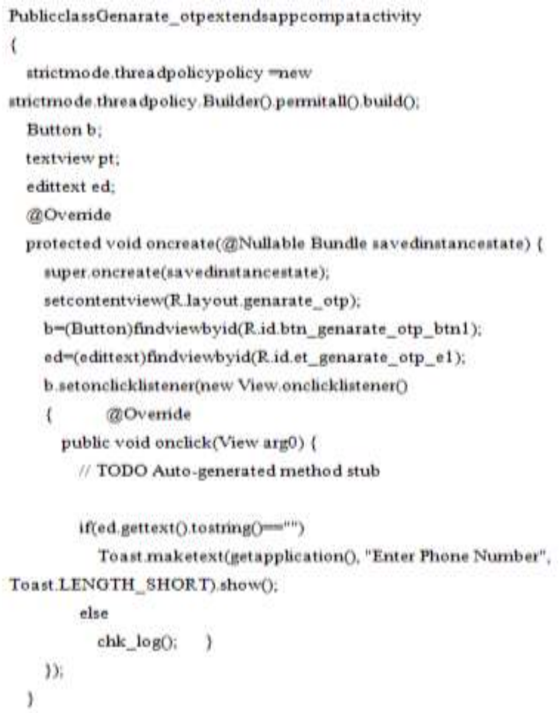

UNIQUE AUTO DISCONNECT PASSWORD GENERATION FOR PUBLIC WI-FI ROUTERS
USER
USER DETAILS
REGISTER
ENTER USER DETAILS SUCH AS NAME, MAIL ID, MOBILE NO, PASSWORD
LOGIN
LOGIN WITH USER CREDENTIALS
WI-FI
SELECTING WI-FI
BLUETOOTH
SELECTING BLUETOOTH
HELP CENTER
HELP CENTER USING GPS
NOTIFICATION AND ABOUT APP
DISPLAYS LIST OF DEVICES

Figure 4. Proposed Architectural Diagram

The OTP generator code is lisetd below:-



```
PublicclassGenarate_otpextendsappcompatactivity
{
   strictmode.threadpolicypolicy =new
strictmode.threadpolicy.Builder().permitall().build();
   Button b;
   textview pt;
   edittext ed;
   @Override
   protected void oncreate(@Nullable Bundle savedinstancestate) {
      super.oncreate(savedinstancestate);
      setcontentview(R.layout.genarate_otp);
      b=(Button)findviewbyid(R.id.btn_genarate_otp_btn1);
      ed=(edittext)findviewbyid(R.id.et_genarate_otp_e1);
      b.setonclicklistener(new View.onclicklistener()
      {          @Override
         public void onclick(View arg0) {
            // TODO Auto-generated method stub

            if(ed.gettext().tostring()=="")
               Toast.maketext(getapplication(), "Enter Phone Number",
Toast.LENGTH_SHORT).show();
            else
               chk_log();     }
      });
   }
```

VI. Description of Modules

Flash Page module: - The Flash Activity gets activated when the app gets started and after two seconds flash activity get close.

Register Module:- The Create new account page is use to create the new register where the new user has to create the account by filling the user information like Name, Email-ID and Address then those all data will store into the database.

Login Module: - The Login Page Activity is use for an existing user has to login by using the valid username and password and access the application.

Wi-Fi Module: - The Wi-Fi activity page is main sub module in this application. This application will access to connect the available Wi-Fi list and generates the OTP password by using the OTP connect to the Wi-Fi.

Bluetooth Module: - The Bluetooth activity page use to connect the all available Bluetooth device and get paired with the particular Bluetooth then the user can create the file and store the some string and send to the paired device.

Help Center using GPS:- The Help center module is use to find the nearest Hospital ,atms, Schools, Hotels based on user current location and the user gets all the places in Google maps and the user can view the particular places by using this module.

Notification: - The Notification module is use to get latest notification from particular organization admin and admin will send the notification to registered user.

Feedback Module: - The feedback application is use to send the user feedback to admin.

VII.RESULTS

Proposed method is implemented as an experimental usage in form of an android app.Varuious operations snaps are listed below:

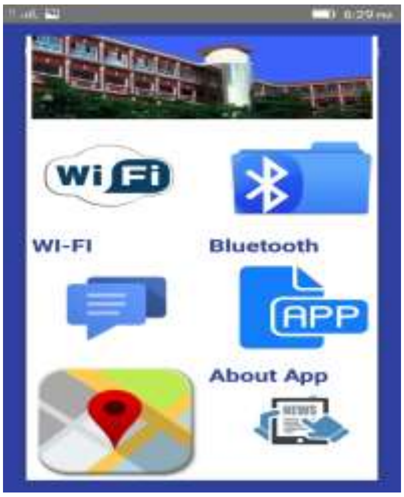
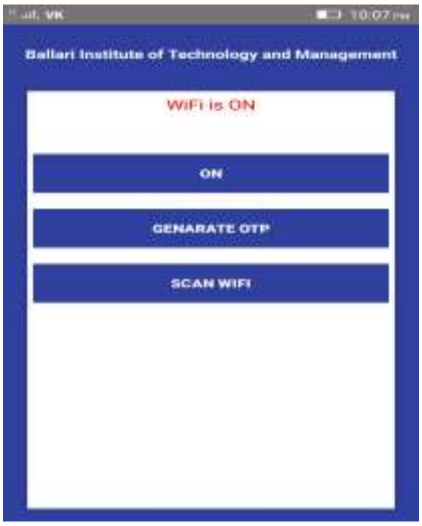


Figure 5. Dash board.

This dashboard screen shows homepage for overall operations. By selecting each icon we czn further process its detailed operation.



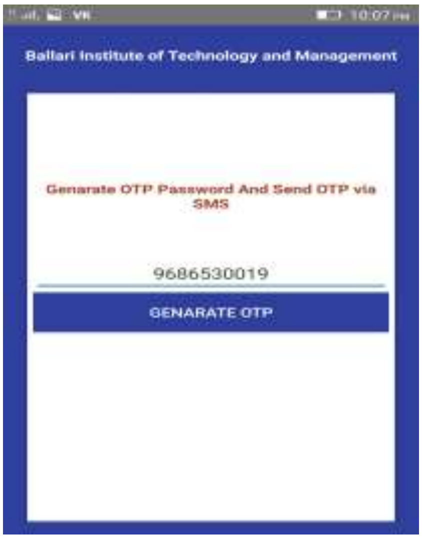
Ballari Institute of Technology and Management

WiFi is ON

Figure 6.OTP Generation

DOI: 10.18535/ijsrm/v5i6.21

If user Selects "Genarate OTP",it Calls Gererate OTP Module which has Unique Ramdom Number Generator Algorithm and Session Paring, which Pairs OTP with Fixed Sessions.


Ballari Institute of Technology and Management

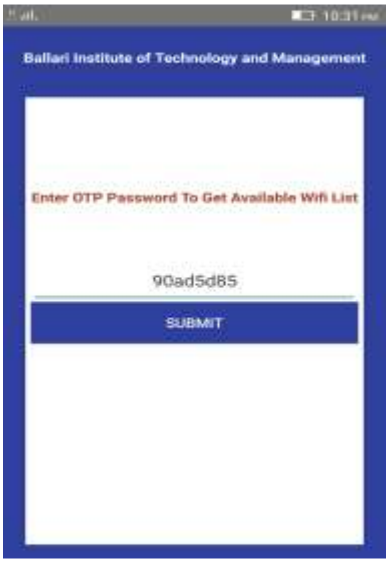
Genarate OTP Password And Send OTP via SMS

9686530019

GENARATE OTP

Figure 7.Destination Node to generate OTP.

User has to Enter Destination Node(Mobile) Number, to which OTP with fixed session is sent.


Ballari Institute of Technology and Management

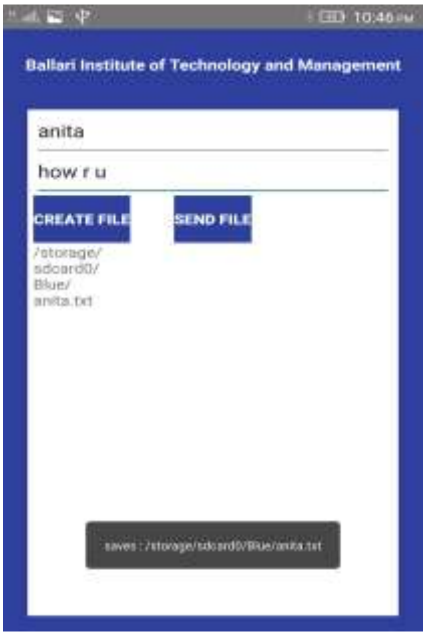
Enter OTP Password To Get Available Wifi List

90ad5d85

SUBMIT

Figure 8.OTP to Access Intenet.

Once Destionation Node number is entered, an unique OTP sent to that number and now user has to enter OTP, which is received as SMS, to get connected to Wi-Fi with pre fixed session.


Ballari Institute of Technology and Management

anita

how r u

CREATE FILE

SEND FILE

/storage/sdcard0/Blue/anita.txt

saves : /storage/sdcard0/Blue/anita.txt

Figure 9.Transfer of Folder between Nodes.

This function suppports transfer of files between two nodes.

VIII.Conclusion

The Proposed method "Unique Auto Disconnect Password Generation For Public Wi-Fi Routers" is used to connect to the nearby Wi-Fi devices and automatically disconnect after a certain time. Bluetooth is used to create a folder dynamically and send to the nearby devices along with path name, In this method, we have proposed an android application which contains six modules i.e.., Wi-Fi, Bluetooth, Help Center, Feedback, About App, Notification.

IX.References

[1] A Survey On Wi-Fi And Lifi Technologies Anil B C1 D Janardhana2 Chayadevi M L3, Int.J.Computer Technology & Applications,Vol 6 (6),1047-1051

[2] Bluetooth And Wi-Fi Wireless Protocols:
A Survey And A Comparison-Erina Ferro And Francesco Potorti`,Institute Of The National Research Council (Isti—Cnr) Ieee Wireless Communications • February 2005

[3] Wi-Fi Technology: Security Issues Vandana Wekhande* Graduate Student, M.S. In Computer Science Program, Rivier College , Rivier Academic Journal, Volume 2, Number 2, Fall 2006

[4] International Conference On Computing, Communication And Automation (Iccca2015) Isbn:978-1-4799-8890-7/15/$31.00 ©2015 Ieee 389 Security Threats Of Wireless Networks: A Survey.

[5] I. J. Computer Network And Information Security, 2013, 7, 9-20 Published Online June 2013 In Mecs (Http://Www.Mecs-Press.Org/) Doi:10.5815/Ijcnis.2013.07.02 Copyright © 2013 Mecs I.J. Computer Network And Information Security, 2013, 7, 9-20 Wi-Fi Networks Security And Accessing Control Tarek S. Sobh Information Systems Department, Egyptian Armed Forces, Cairo, Egypt

*****