WWJMER 2023;1(02): 17-19
www.wwjmer.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal

Saka T.O
Department of Computer Science, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin.

Isiaka O.S
Department of Computer Science, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin.

Bolaji-Adetoro D.F
Department of Computer Science, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin.

Correspondence:
Saka T.O
Department of Computer Science, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin.

An Evaluation of a Handy Functional Universal Plug and Play-Compatible Hotspot Software

Saka T.O, Isiaka O.S, Bolaji-Adetoro D.F

Abstract
The increase in wireless users and network access methods necessitates the adoption of hotspot network software. Wireless local area networks (WLANs), often known as hotspots, provide a viable networking platform for extending network connectivity to a variety of locations, including homes and public venues. The aim of this research is to create a low-cost, functional, and Universal Plug and Play (UPnP)-compatible wireless hotspot software. The technology enables consumers to use hotspots in accordance with provider specifications, reducing deployment and maintenance expenses. It also supports hotspot software network connections for devices that do not have built-in hotspots, providing for a broader range of internet access. The project intends to offer a framework that enables for the establishment of as many hotspots as possible, hence improving wireless network access efficiency.

Keywords: Hotspot software, provider specification, UPnP compatible, Wireless Local Area Network (WLAN), network connectivity, internet access.

1. Introduction

The growth of wireless users, apps, and network access methods has been astonishing in recent years. Today's laptop users connect to the Internet in a number of places and settings, including their homes, businesses, and even public facilities like convention centers, airports, shopping centers, libraries, and other places where they spend a lot of time away from their home networks. As a possible networking platform for extending network access to these public areas, often known as hotspots, wireless local area networks (WLANs) have come to light. Now, IEEE 802.11b-based "Wi-Fi" wireless LANs offer reasonably strong data connection at 11Mb/s, and in the years to come, this data rate is anticipated to rise dramatically (Nwabueze & Akaneme, 2009). Wireless Internet service providers (WISPs) have recently increased the number of Wi-Fi hotspots in public areas, giving tourists local coverage and allowing them to access email, the Web, and other Internet applications while on the move (Maleh & Ezzati, 2013).

In a wireless network, a method of computer communication, data is sent wirelessly between network nodes. Network nodes are the networking hardware and endpoints that are located inside the network's coverage area. These networking components switch and transport data between end devices. These networking devices are set in an infrastructure mode, which specifies the network architecture, to link all end devices within a region or domain. Any town that does not have enough contemporary comforts is considered to be rural. There are several issues there, including a lack of security, social amenities, and a severe lack of access to healthcare and education. Due to their high price, mobile phones have lately become more popular than other computer devices in these areas. Amongst mobile devices employing GSM technology, voice communication is the exchange of voice packets (Anand, 2005).

Hotspots face authentication, security, coverage, network management, billing, and interoperability challenges. The growing demand for high-speed connectivity in public places is driving the deployment of hotspots (Moses, Wario & Onyeke, 2018). A successful and viable hotspot business model must provide value to all stakeholders - the end user, the network

service provider, and the building and premise owners. To benefit the end user, the system must offer an easy-to-use, cost-effective mechanism that provides fast access in a transparent, device-independent, and access-technology-independent manner. Hotspot network providers need a trustworthy and capable third-party authenticating entity, peering relationships with other providers, and the ability to meet users' diverse resource and performance requirements (Chukwuemeka & Ifeanyi, 2014). Premise and building owners must sign into commercial contracts with providers for installation, maintenance, monitoring, and support, as well as make network access a standard utility for end users. The Universal Plug and Play (UPnP) networking protocol enables devices to locate and connect to each other without human configuration or user intervention. It automates all procedures needed for device identification and communication on the same network, providing a fully automated technique for adding and connecting new hardware to a local network.

The protocol allows a device to connect to the network by:

1. Configuring the IP address of the device
2. Communicating the device's name and capabilities to the rest of the network.
3. Informing the new piece of hardware about the capabilities of other connected devices.
4. Permitting network devices to communicate and work together

UPnP is also used to connect printers, gaming consoles, and smart TVs. It can also be used to connect wireless speaker sets to mobile phones, home surveillance systems, and Internet of Things (IoT) systems such as lighting, thermostats, and locks. It can also be used to remotely control IoT systems such as lighting, thermostats, and locks.

II. Literature Review

According to Balachandran, Voelker, and Bahl (2005), a growing number of Wi-Fi hotspots have been set up at public locations by wireless Internet service providers (WISPs) in recent years. However, a number of technological and deployment difficulties still exist today that did not exist before hotspots were a commonplace technology. Okoro & Emmanuel (2017) discuss wireless network implementation as a viable option for building network infrastructure in rural communities. The aim of their research was to create a wireless network infrastructure architecture for providing network services to rural residents. A user-centered approach was used, and a wireless network infrastructure was designed and deployed to cover five rural locations. Data was collected and analyzed to evaluate the performance of network facilities.

According to Maleh & Ezzati (2013), before the invention of computers, connecting to a public computing network like the Internet was not a common occurrence. The ArpaNet network, created by US military and academic organizations, marked the beginning of this. According to Hare, Hartung, and Banerjee (2012), the previous ArpaNet was transformed in the 1990s into the Internet, a vast computer network that linked computers all over the world. WiRover is a bus system that has been in operation for years and provides a WiFi hotspot to which bus passengers can connect. As of December 1, 2011, the WiRover system has 17,567 distinct client devices connected, and these devices had downloaded more than 337.53 GB and uploaded 48.19 GB of data since its initial deployment.

III. UPNP Methodology

With the help of an automated port opening and closing system, the UPnP protocol enables devices and applications to connect to LAN networks. Its foundation is comprised on the Internet Protocol Suite (TCP/IP), the Hypertext Transfer Protocol (HTTP), the Extensible Markup Language (XML), and the Simple Object Access Protocol (SOAP). As UPnP is based on widely used networking protocols, it may run without the need for any special drivers or technology (Andreas, Frank & Andreas, 2006). Most devices may participate in UPnP, regardless of their operating system, programming language, or manufacturer.

Through the UPnP protocol, newly connected network devices will interact with one another. The device is set up in six steps, which are described in more detail below (Sales et al., 2010).

i. Addressing: The new device's unique IP address will be requested from a DHCP server or AutoIP, and the domain name obtained during a DHCP transaction will be used in network operations.
ii. Discovery: Network control points, which may either actively search for devices or passively listen for Simple Service Discovery Protocol (SSDP) messages, can access the device's information through the SSDP.
iii. Description: The network must learn about a new device before interacting with it, and the device sends an XML format to create a device description document with URLs for control, eventing, and presentation.
iv. Control: The network sends messages invoking actions on services, written in XML and using SOAP, before interacting with the discovered device.
v. Eventing: In order to receive alerts for changes in device status, a control point can register as a service using the UPnP protocol. The service notifies all registered control points of an event when a state variable changes using an XML format.
vi. Presentation: The control point will load a web page from a browser using the URL set during the description phase. The web page's and device's capabilities determine how much a user can interact with the device via the presentation URL.

IV. Security Risks of UPnP Protocol

UPnP should be activated on networks within a small region, such as home networks, rather than business networks, due to the security risk of a skilled hacker entering through a device with a major vulnerability or malware joining the protocol (Palacios et al. 2011). Despite its advantages, UPnP poses two significant security risks:

i. UPnP does not authenticate devices by default, assuming that all devices are trustworthy.
ii. UPnP enables an entity outside the home network to breach the router and gain access to local devices without going through a firewall.

UPnP allows traffic to bypass security barriers, but connecting a malware-infected device to the network can lead to security issues. Additionally, different routers support different applications, and many deployments have specific UPnP-related bugs that hackers can exploit. Additionally, many router manufacturers enable UPnP by default, leaving LAN-based devices vulnerable to WAN

discovery (Sales et al., 2010). The following prominent UPnP-based attacks happened as a result of router-related port forwarding issues:

i. A Flash UPnP attack occurs when a victim accesses a website that sends requests for port forwarding to a malfunctioning router.
ii. The Mirai attackers targeted vulnerable routers with open telnet ports, using credential stuffing to gain network access and install the Mirai malware on all local devices.
iii. A router-based UPnP flaw can lead to data loss due to the CallStranger vulnerability.

V. Components of UPNP Protocol

The major components of the UPnP Protocol are as follows.

i. UPnP Media Server Control Point is a UPnP-client that can stream media/data files from UPnP-servers on the network.
ii. UPnP Media Renderer DCP is a 'slave' device capable of rendering (playing) content.
iii. UPnP Rendering Control DCP manages Media Renderer settings such as volume, brightness, RGB, sharpness, and others.
iv. UPnP Remote User Interface (RUI) client/server transmits and receives control commands, such as record, play, pause, stop, etc., over a network.
v. Quality of Service (QoS) is a critical service function for UPnP AV (Audio and Video). It assigns different levels of priority to different users or data flows, or guarantees a certain level of performance. QoS guarantees are especially important when network capacity is limited, such as in public networks like the internet.
vi. Remote Access specifies how to connect UPnP device sets that are not in the same multicast domain.

VI. Conclusion

The findings indicated a number of technological and deployment-related difficulties that must be resolved before high-speed internet can be widely provided through hotspots. Interoperability, billing, coverage, security, authentication, and network administration are among the challenges. Hotspot implementation is being accelerated by the rise in demand for high-speed internet in public spaces. The ability of a hotspot business model to benefit all parties—the end user, the network service provider, and the building and premises owners—will be what makes it effective and profitable. The system must offer a simple, affordable mechanism that offers quick access in a transparent, device- and access-technology-independent way for the advantage of the end user. In order to benefit, building and premises owners must enter into business agreements with hotspot network providers for installation, upkeep, monitoring, and support as well as for making network access a regular amenity for end users.

References

1. Andreas H., Frank R. & Andreas F. (2006). UPnP Control Point for Mobile Phones in Residential Networks. Agder University Research Archive.
2. Balachandran A, Voelker G.M & Bahl P. (2005). Wireless hotspots: current challenges and future directions. Mobile Networks and Applications, 10, 265–274.
3. Chukwuemeka, O. A. & Ifeanyi, I. A. (2014). A Review of Setting up a Secured Web Based Wireless Hotspot. International Journal of Engineering Trends and Technology (IJETT), 16(5), 208-215.
4. Hare, J.& Hartung, L. & Banerjee, S. (2012). Beyond deployments and testbeds: experiences with public usage on vehicular WiFi hotspots. 10th international conference on Mobile systems, applications, and services, 393–406, https://doi.org/10.1145/2307636.2307673
5. Maleh Y. & Ezzati A. (2013). A review of security attacks and intrusion detection schemes in wireless sensor networks. International Journal of Wireless & Mobile Networks (IJWMN), 5 (6), 1-12, https://doi.org/10.48550/arXiv.1401.1982
6. Moses, A., Wario, R. & Onyeke, I. (2018). Shared Wireless Access Point Security in a Hybrid Star Topology using Primary Host Authentication: A Case Study of NAITES Wi-Fi. International Information Management Corporation, 1-8.
7. Okoro O. & Emmanuel E.A (2017). A wireless network infrastructure architecture for rural communities. International Journal of Computer Science and Information Technology.https://doi.org/10.5121/IJCSIT.2017.9304
8. Nwabueze C.A. & Akaneme S.A. (2009). Wireless Fidelity (Wi-Fi) broadband network technology: an overview with other broadband wireless networks. Nigerian Journal of Technology, 28 (1).
9. Palacios J.M., Fernández M., Corcho O., Méndez V. and Gómez-Pérez J. M. (2011). Semantically enabling UPnP networks of multimedia home content. Facultad de Informática (UPM).
10. Sales, T., De Sales, L., Almeida, H. & Perkusich, A. (2010). A UPnP extension for enabling user authentication and authorization in pervasive systems. Journal of the Brazilian Computer Society16(4):261-277, 261-277, https://doi.org/10.1007/s13173-010-0022-2