Open Challenges for Secure and Scalable Wi-Fi Connectivity in Rural Areas

Philip Virgil Berrer Astillo
University of San Carlos, Philippines
pvbastillo@usc.edu.ph

Jayasree Sengupta
IIIT Allahabad, India
jayasree@iiita.ac.in

Mathy Vanhoef
DistriNet, KU Leuven, Belgium
mathy.vanhoef@kuleuven.be

Abstract

Providing reliable, affordable, and secure Internet connectivity in rural areas remains a major challenge. Pay-for-use Wi-Fi hotspots are emerging as a scalable solution to provide affordable Internet access in underserved and rural regions. Despite their growing adoption, their security properties remain largely unexplored. In this paper, we present a security analysis of these hotspot ecosystems based on Wi-Fi surveys and practical attack validation. We first perform a Wi-Fi survey conducted in two countries, namely the Philippines and India, to understand the deployment and adoption of such systems in practice. Our results suggest that Piso-WiFi pay-to-use hotspots are particularly widespread in rural regions of the Philippines, and that India's PM-WANI initiative is slowly gaining traction. We then perform a security assessment of these deployments and demonstrate two practical attacks: (1) hijacking another user's paid connection; and (2) rogue hotspots. We analyze the root causes of these vulnerabilities, introduce threat models tailored to pay-for-use hotspot deployments, and outline practical security improvements, including a secure caching architecture. Our findings highlight security challenges in emerging rural connectivity infrastructure and provide directions toward more secure and scalable deployments.

Keywords

IEEE 802.11, Wi-Fi Hotspots, Piso-WiFi, PM-WANI, Security

ACM Reference Format:
Philip Virgil Berrer Astillo, Jayasree Sengupta, and Mathy Vanhoef. 2026. Open Challenges for Secure and Scalable Wi-Fi Connectivity in Rural Areas. In *Workshop on Security and Privacy for Asian Internet Communities (SPAIC '26), June 01–05, 2026, Bangalore, India.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3803632.3807891

1 Introduction

Reliable and affordable Internet connectivity remains a major challenge in many developing regions. While urban areas increasingly have widespread broadband coverage, rural communities often rely on limited and expensive data services. Furthermore, cellular networks often provide limited bandwidth and can incur substantial costs as data usage increases [16]. This limited Internet access causes a digital divide, restricting access to information, education, and economic opportunities. As a result, providing affordable, reliable, and secure Internet access in rural areas remains an important challenge.

One promising approach to increase Internet connectivity is the emergence of community-operated pay-for-use Wi-Fi hotspots. These act as a scalable solution to provide affordable Internet connectivity in underserved and rural regions. Such systems allow anyone with connectivity to act as a micro–service provider, thereby offering community-based Internet coverage without requiring large-scale infrastructure investments. These systems are typically deployed using low-cost routers, making them especially attractive in rural areas where broadband and cellular Internet are limited [11].

Despite their growing adoption, the security properties of these pay-for-use hotspot ecosystems remain largely unexplored. Unlike traditional enterprise or managed public Wi-Fi deployments, these systems operate in decentralized environments, often using commodity hardware and minimal configuration. This creates unique security challenges that differ from traditional Wi-Fi deployments. Understanding the security risks of these emerging connectivity models is useful in order to ensure safe and sustainable Internet access in developing regions.

To better understand the adoption of these systems, we conducted a Wi-Fi survey in two countries: the Philippines and India. Our observations suggest that Piso-WiFi coin-operated hotspots, named after the Philippines' peso currency, are widely deployed, particularly in rural and semi-urban regions, while India's PM-WANI (Prime Minister's Wi-Fi Access Network Interface) initiative is slowly gaining traction. Unlike Piso-WiFi, PM-WANI is not coin-operated, but relies on online subscriptions. These observations provide an initial view into how pay-for-use Wi-Fi can be a growing solution to provide affordable Internet connectivity, especially in rural regions.

Motivated by these observations, we perform a security review of Piso-WiFi. This showed that Piso-WiFi is vulnerable to known attack techniques that allow an adversary to (1) hijack another user's active session, and (2) set up a rogue Piso-WiFi hotspot to impersonate legitimate providers. Both attacks enable an adversary to obtain free Internet access. We implemented and validated both attacks in real-world settings, confirming that they can be exploited with commodity hardware and minimal technical expertise. Next, we analyze India's PM-WANI framework, which is another pay-for-use Wi-Fi hotspot model. It uses a different payment system with an online subscription. Based on its design and publicly available specifications, we identify potential security vulnerabilities that may arise in similar ways to those observed in Piso-WiFi. However, we emphasize that this analysis is preliminary and does not include a practical attack evaluation.

Lastly, we discuss these common challenges and outline open problems in designing secure, low-cost connectivity mechanisms for rural regions. Notably, we outline two threat models that can be used as a basis for better securing pay-to-use hotspots, and discuss secure local caching approaches that can help optimize limited backhaul

SPAIC '26, Bangalore, India

ACM ISBN 979-8-4007-2582-1/2026/06
https://doi.org/10.1145/3803632.3807891

bandwidth while preserving security. Overall, our exploratory study shows that more research is needed to provide secure but easy-to-use and scalable public Wi-Fi hotspots.

Summarized, our contributions are:

- We perform a systematic Wi-Fi survey in the Philippines and India, study security trends, and discuss the usage of pay-to-use Wi-Fi hotspots (§ 3).
- We conduct a security assessment of Piso-WiFi and demonstrate the feasibility of two attacks: hijacking connections and rogue hotspots (§ 4).
- We conduct a preliminary security assessment of the PM-WANI hotspots, and compare to Piso-WiFi (§ 5).
- We define new threat models for pay-to-use hotspots and propose ways to improve their security (§ 6).

Additionally, we cover related work in § 7, and conclude in § 8.

2 Background

In this section, we introduce the IEEE 802.11 standard that underpins Wi-Fi, explain how clients can discover nearby networks, and cover security and authentication aspects of 802.11.

2.1 Network discovery

When a Wi-Fi client wants to connect to a wireless network, it first discovers nearby Access Points (APs) through either passive or active scanning. In passive scanning, the station listens for beacon frames periodically broadcast by nearby APs. Each beacon advertises the network's name, also called the Service Set Identifier (SSID), as well as other network properties such as supported data rates, security capabilities, and other configuration parameters. In active scanning, the station transmits broadcast probe request frames. Nearby APs reply with probe responses containing similar information to that found in beacons. Both mechanisms allow clients to learn which networks are within their range and to decide which AP to associate with, typically based on received signal strength and preferred SSIDs.

Each individual AP has a unique Basic Service Set (BSS) Identifier, which typically equals the MAC address of the AP. Multiple APs can advertise the same network name, i.e., the same SSID.

2.2 Security of IEEE 802.11

Once an AP is selected, the client begins the authentication and association stages. During the authentication stage, the client performs open system authentication, which involves a simple exchange of request and response frames without actual credential validation. Only when using WPA3-Personal does actual authentication take place at this stage of the connection process [14]. When using WPA1/2 or WPA3-Enterprise, actual authentication takes place after association. Next, regardless of which WPA version or variant is used, the 4-way handshake is performed to negotiate session keys to protect and encrypt data frames.

Unicast Wi-Fi frames between the client and the AP are protected using pairwise session keys, and group-addressed frames, i.e., broadcast or multicast frames, are protected using a group key. This also implies that the cipher used to protect unicast and group-addressed frames can differ, i.e., networks can be configured using a different pairwise and group cipher, respectively.

Lastly, many commercial or community Wi-Fi systems, such as public hotspots, employ captive portals after association. These portals intercept HTTP traffic and redirect the user to a local payment or authentication webpage, or a page showing an end-user license agreement, before granting broader Internet access. While a common solution in practice, captive portals are not part of the IEEE 802.11 standard itself, and their security is therefore not always well-integrated and implementation-dependent, as we later discuss.

3 Wi-Fi Surveys

In this section, we present the methodology used for Wi-Fi surveys in rural areas of the Philippines and in India to study the prevalence of pay-to-use hotspots.

3.1 Methodology

To detect nearby Wi-Fi networks, we used the WiGLE Android app[1] while driving around various cities in the Philippines and India. This app uses Android's built-in functionality to detect nearby networks, meaning it will listen for beacon frames and will periodically trigger the transmission of broadcast probe requests.

During a Wi-Fi survey, WiGLE will log each detected AP, and store the MAC address (BSSID) of the AP, the SSID of the network, the geolocation, and other metadata. Importantly, WiGLE will also log the network security properties of the network as reported by Android's scan results.

More precisely, WiGLE takes the `ScanResult` object, which describes information about a detected access [5], and logs the capability string that is provided by the `capabilities` field of the scan result. Although there is no documentation on how this string is constructed, we can inspect the source code of Android's Wi-Fi Information Element parser, and specifically the function `generateCapabilitiesString`, to learn the information it provides.

First, the capabilities string contains information on whether the network is an infrastructure or ad-hoc network, whether Wi-Fi Protected Setup (WPS) is supported by the network, and whether Management Frame Protection (MFP) is either supported or required. Second, the network's supported authentication methods are listed, e.g., WPA1/2 password authentication, EAP-based Enterprise authentication, WPA3 password authentication with SAE, opportunistic wireless encryption, along with supported key sizes. Lastly, the capabilities also include the cipher suite used to protect and encrypt data once the station is authenticated with the network.

We remark that captive-portal authentication cannot be detected using passive Wi-Fi surveys. This is because these deployments do not use authentication at the Wi-Fi layer, but instead intercept HTTP traffic, and perform authentication once the station is already connected to the Wi-Fi network. Additionally, the group cipher used to protect multicast and broadcast traffic is not included in the network's capabilities string, meaning it cannot be collected when using WiGLE.

3.2 Philippines

We performed a Wi-Fi survey in the Philippines in eastern Mindanao, while driving around the rural areas and cities near the coastline.

[1] Available at https://wigle.net/tools

Table 1: Summary of the Wi-Fi surveys that we performed in India and the Philippines. The column Hotspots refers to the number of detected Piso-WiFi and PM-WANI hotspots, respectively.

Country	#APs	Hotspots	WPA1-TKIP
Philippines	2 620	125 (4.8%)	513 (19.6%)
India	6 464	3 (0.05%)	851 (13.2%)

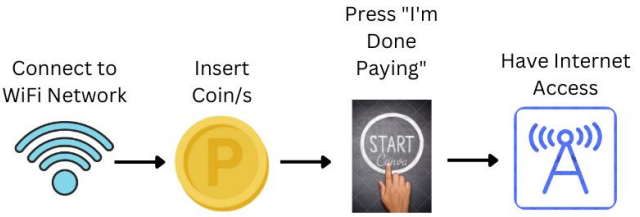

Figure 1: High-level overview of the steps that the user must perform to connect to a Piso-WiFi hotspot.

One challenge is that rural areas have few Wi-Fi networks, requiring us to perform surveys of several hours to detect a representative number of Wi-Fi networks. After driving around for three days in total, during which we drove for roughly 4 hours, we detected a total of 2 620 Wi-Fi networks.

A first surprising observation is that close to 20% of detected networks still support the old TKIP encryption cipher of WPA1 as the pairwise cipher (see Table 1). This cipher has been deprecated by the Wi-Fi Alliance and is known to be vulnerable to various side-channel attacks [22, 27]. A possible root cause of the continuing support for TKIP in practice is that people in rural areas may update their devices less frequently, causing many APs to still support this outdated cipher. For comparison, in India roughly 13% of networks still support TKIP as the pairwise cipher, and prior work reported TKIP support in 17.99% to 54.23% of networks across selected European countries in 2019 [23].

To detect how many Piso-WiFi hotspots there are, we can easily check if the string `piso` occurs in the SSID. This works because the main way for users to detect Piso-WiFi hotspots is based on the SSID, hence why these hotspots practically always include the string `piso`. This revealed that close to 5% of the networks in our dataset are identified as Piso-WiFi hotspots, showing that they are very popular in the region we surveyed.

3.3 India

In India, we performed a Wi-Fi survey using WiGLE in areas of Bangalore, Calcutta, and more rural areas near the outskirts of Allahabad. This was done by surveying each city for roughly an hour, spread out over two days, detecting 6 464 networks (see Table 1).

Unlike Piso-WiFi, the PM-WANI hotspots cannot be detected based on their SSID, i.e., their network name. Instead, there is an online list of the MAC addresses of PM-WANI access points. Users of PM-WANI use mobile apps that can download the list and notify the user when a PM-WANI network is nearby. To detect these hotspots ourselves, we scrape the list of MAC addresses of PM-WANI networks and intersect this with the set of detected networks in our Wi-Fi survey. This revealed that only 3 networks are PM-WANI hotspots in our dataset (see Table 1), which limits the conclusions that can be drawn about their broader deployment.

We believe the low number of PM-WANI hotspots compared to Piso-WiFi is due to the lengthier process of setting up a PM-WANI hotspot: users must first register their business, and can only then set up a hotspot. In contrast, a Piso-WiFi hotspot in the Philippines requires no registration, but only the provisioning of a router.

Finally, we observed that around 13% of networks still support the old and broken TKIP encryption cipher. Although lower than our survey in the Philippines, this is still a worrying number of networks that are potentially vulnerable to attacks.

3.4 Limitations of the Measurement Study

Our Wi-Fi survey provides an initial snapshot of pay-for-use hotspot deployments. However, it has a couple of limitations. Data collection was opportunistic and conducted while driving through selected regions, which may introduce sampling bias. The observation period was also relatively short. In addition, the number of detected PM-WANI hotspots in our dataset is small, so observations regarding PM-WANI should be interpreted as preliminary. Despite this, our dataset offers useful qualitative insights into the deployment and security characteristics of emerging pay-for-use hotspot systems.

4 Security of PISO-WIFI

In this section, we analyse the security of Piso-WiFi, and empirically confirm that it does not defend, or otherwise mitigate, two attacks that can hijack a user's paid Internet connection. All attacks described in this section were experimentally validated in controlled and real-world settings using our own devices.

4.1 Background on Piso-WiFi

The idea behind Piso-WiFi hotspots is that ordinary users can share their Internet connection to earn extra income by providing Internet access to nearby users. To use the hotspot, nearby individuals can connect to the Wi-Fi network, and then insert a 1 peso coin to be given 5-10 minutes of unlimited internet access. Many individuals have embraced the idea of acquiring Piso-WiFi Machines to have an additional source of income. These machines are commonly installed near Sari-Sari Stores (small shops), along roadsides for use by passing travelers, and also near residential communities or near local cafe shops. The average cost of a new machine is approximately 9,000 pesos [25].

As also indicated by our Wi-Fi survey in the previous section, such networks are particularly common in more rural areas and barangays, where a significant portion of the population lacks the financial means to own their own Internet connection. In essence, these machines provide an affordable opportunity to connect to the Internet, especially in rural areas.

Figure 1 shows how users connect to Piso-WiFi hotspots. First, users initiate the process by connecting to the Wi-Fi hotspot to access the system's captive portal. Subsequently, the system guides users

through inserting coins into the physical Piso-WiFi machine. To make it easier to locate the machine, most will show blinking lights when coins need to be inserted. After inserting coins, the users can click a button to finish the payment, after which the corresponding usage time limit is calculated and Internet access is granted. This user-friendly design, with low overhead, is especially important since the target audience is non-technical people who may also not always own the most recent smartphones or IT equipment.

4.2 User Masquerading Attack

In our first experiment, we test whether Piso-WiFi tries to prevent or mitigate the known attack technique of spoofing the MAC address of an already-connected client. Note that modern APs have features that attempt to detect such attacks [9]. We test for these attacks in two phases: first in a controlled environment, and then under more real-world conditions. Note that for ethical reasons, we only test the attack against our own devices, and never against real users.

4.2.1 Controlled experiment. We first tested whether a user's connection can be hijacked in a controlled environment. In this environment, we assume the adversary knows in advance what the MAC address and IP address of the victim are, and we assume that the adversary knows exactly when the victim has paid for their Piso-WiFi Internet connection. Once the victim client has connected and paid, the adversary spoofs the MAC and IP address of the victim, and connects to the Piso-WiFi access point. In our experiments, this attack was always successful. We did observe that, when the victim tries to reconnect, the Internet connection of the adversary is disrupted. In other words, as long as the real user is present, their device might try to automatically reconnect, which can interfere with the adversary's hijacked Piso-WiFi connection. Nevertheless, once the victim goes out of range, or when they try to connect to a different Wi-Fi network, the hijacked connection becomes stable.

4.2.2 Real-world attack evaluation. As a second experiment, we more accurately simulate a real attack, where the adversary does not in advance know the MAC address of the victim, and does not know when the victim will connect to Piso-WiFi, i.e., we follow a *blind testing* approach. To handle this, the adversary will first use a Wi-Fi monitoring tool such as `airodump-ng` to determine which clients are currently connected to the Piso-WiFi network. Once all connected clients have been determined, the adversary can track how many data frames each client is exchanging with the hotspot. A high number of exchanged data frames indicates that the client has successfully connected with Piso-WiFi and is actively using the connection. In other words, seeing many data frames likely means the client has paid for Internet access. Since Piso-WiFi does not use encryption at the Wi-Fi layer, the adversary can trivially learn the MAC address and IP address that a victim client is using. The adversary can then spoof this MAC and IP address, similar to our controlled experiment, to hijack the victim's paid Internet connection. We successfully confirmed this attack strategy in practice.

4.3 Rogue Access Point

In case determining connected clients is challenging, e.g., due to the hidden station problem, or due to beamforming making it difficult to sniff the frames of clients [6], then an alternative attack strategy is creating a rogue clone of a Piso-WiFi hotspot (see Figure 2). The idea is that the adversary creates an almost identical clone of a real Piso-WiFi network, which is possible using commodity off-the-shelf tools such as `hostapd` on Linux. The adversary can then either wait until a victim connects to the adversary's rogue AP, or can abuse techniques such as the spoofing of Channel Switch Announcements to force the victim into connecting with the rogue AP [26]. The attacker can then conduct a Man-in-the-Middle (MitM) Attack, by positioning themselves between the client device and a real Piso-WiFi network, allowing them to intercept and manipulate communication between the two parties. Concretely, the victim is tricked into paying for the adversary's connection to the Piso-WiFi hotspot, after which the adversary can freely access the Internet.

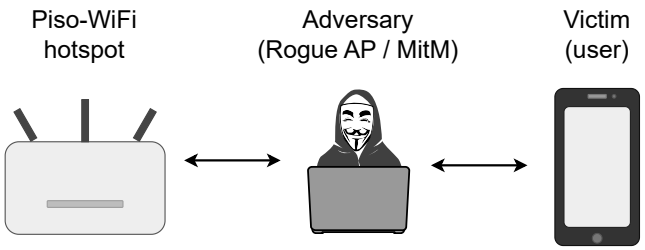

Figure 2: Using a rogue AP to perform a MitM attack against Piso-WiFi.

5 India's PM-WANI

In this section, we give a description of how the PM-WANI hotspots in India work, and compare it with the Piso-WiFi hotspots of the Philippines (see Table 2).

5.1 Overview of PM-WANI

India's growing digital economy has made reliable broadband Internet access ever more important. However, although access to mobile Internet in India has increased significantly in recent years, rural and remote regions often still lack affordable and high-quality Internet access. To address these challenges, and provide affordable Internet access to all citizens, India's Department of Telecommunications approved the Prime Minister's Wi-Fi Access Network Interface (PM-WANI) framework in 2020 [10].

Compared to Piso-WiFi, the PM-WANI system is a more centrally managed but still *federated* architecture, with a similar goal of providing Internet access to all regions in the country.

In this federated model, responsibilities or various tasks are split between the following stakeholders:

- **Public Data Office (PDO):** Will establish and operate compliant Wi-Fi hotspots that provide Internet access.
- **Public Data Office Aggregator (PDOA):** They will aggregate PDOs, including the PDOs' Wi-Fi APs, network names, and locations. The PDOA also has the responsibility of performing authentication and accounting of users wanting to use a hotspot, handling payment transactions, and keeping track of each user's usage. PDOAs must register with the government.

Table 2: Comparison between PM-WANI and Piso-WiFi

Aspect	PM-WANI	Piso-WiFi
Nature	Federated registry	Local pay-to-use
Regulation	Government-backed with registration	Informal, unregulated
Architecture	Multi-entity design	Standalone kiosk
Payment	With digital wallet or voucher-based	Physical coin payment
Authentication	App-generated token	Open access with captive pay-to-use portal
Roaming	Possible using central registry	None; sessions limited to individual kiosks

- **App Providers:** Will create mobile apps that allow users to discover nearby PM-WANI Wi-Fi hotspots. This implies that users must have such an app installed in order to use PM-WANI. App providers must register with the government.
- **Central Registry:** Maintains an overview of all App Providers, PDOAs, and PDOs.

As a user, you first register *once* in a PM-WANI compatible App from an App Provider. This identity is then used by any PDOA when you connect to their hotspot. An Internet package is bought from a specific PDOA, and that Internet package can only be used with hotspots aggregated by that specific PDOA. More precisely, when you first connect to a hotspot behind a given PDOA, that PDOA sees you (via the app) and, if you are a new customer for them, shows you its data packs and registers you as its subscriber once you pay. To use hotspots of another PDOA, you can still log in using the same app account, but that second PDOA will typically treat you as a new subscriber and ask you to buy one of *its* data packs. The only exception is when there are roaming agreements between PDOAs, so that each other's subscribers can use any Wi-Fi hotspot associated with either PDOA.

5.2 Technical details of PM-WANI

A typical operational flow involves the following three key stages:

5.2.1 Hotspot advertisement. To advertise a new PM-WANI hotspot, and thereby become a PDO, the new hotspot first has to be registered by a PDOA. This registration includes the hotspot's SSID, MAC address, and location. The PDOA then registers this metadata of the hotspot with the Central Registry, ensuring that the hotspot becomes discoverable by App Providers.[2]

5.2.2 Hotspot discovery and connection. To detect nearby PM-WANI hotspots, users must first install a mobile app created by an App Provider. Such an app, created by an App Provider, scans for nearby APs and queries the central Provider Registry XML to detect if a nearby AP is a PM-WANI hotspot.

Simplified, when a user selects a hotspot, the app generates a `waniapptoken` containing the username, password, timestamp, and the MAC address of the chosen AP [8]. This token is encrypted with the App Provider's public key and passed through the Wi-Fi Captive Portal, which re-encrypts it with the PDOA's private key and forwards it to the App Provider. The App Provider verifies the identities of both the app and PDOA against the central WANI registry. After verification, the captive portal shows the available data packages and payment methods.

Lastly, the specification of PM-WANI also requires that users must be able to log in without an app by manually entering their credentials on the captive portal of the hotspot [8].

5.2.3 Payment and monetization. Before payment, the hotspot grants temporary Internet access for completing any needed payment transactions.

Once payment is confirmed, all devices that authenticate with the same username–password pair share the same session and data pack. Some PDOAs also employ alternative monetization schemes, e.g., where users can gain Internet access by watching ads [24].

5.3 Security Risks of PM-WANI

To the best of our knowledge, the security of the PM-WANI architecture has not yet been studied. However, unlike Piso-WiFi, we do not perform a practical attack evaluation against PM-WANI deployments; rather, we conduct a risk assessment based on the architectural design and publicly available specifications of PM-WANI. Nevertheless, based on our analysis, one major risk is that hotspots are not required to use encryption at the Wi-Fi layer, such as WPA2 or WPA3. This means that PM-WANI hotspots may potentially be vulnerable to the same attacks as covered in Section 4.2 and 4.3 against Piso-WiFi, i.e., they may be vulnerable to user masquerading attacks and rogue-AP-based MitM attacks.

The federated trust model, involving multiple independent PDOs, App Providers, and PDOAs, also introduces additional risks if one of these becomes malicious or compromised. For instance, if the central registry is compromised, an adversary can potentially add their own hotspot as a trusted PM-WANI hotspot. Similarly, if a PDOA is compromised, then an adversary can potentially also add their own hotspot as part of those managed by the PDOA aggregator.

6 Threat Models and Research Directions

In this section, we define threat models and propose directions for more secure and cache-enabled Wi-Fi hotspots.

6.1 Threat models

To design more secure pay-to-use Wi-Fi hotspots that can be set up without requiring registration, we first need concrete threat models. We propose the following two threat models:

Multi-use model. In this threat model, we assume the client uses a particular hotspot multiple times. As a result, we can assume that in the first connection the adversary is not present, but aim to prevent attacks in subsequent connections.

Single-use model. In this threat model, we assume the client only uses the hotspot once, e.g., when they are traveling. To provide security, we assume the user is within physical proximity of the hotspot and can for instance see its display. We assume an adversary will not compromise the physical display or equipment of the hotspot.

[2] At the time of writing, the central registry XML can be found at https://pmwani.gov.in/wani/registry/wani_providers.xml

6.2 Securing the Wi-Fi connection process

Multi-use case. For the multi-use threat model, one solution is a trust-on-first-use protocol, where during the first connection a shared secret is negotiated between the client and hotspot. In later connections, this shared secret, which can also be a public key, is then used to verify the hotspot's authenticity. The main challenge is ensuring backward compatibility and user-friendliness. One solution is to instruct the user to reconnect using an SAE-PK passphrase. This passphrase acts as a digital signature of the hotspot and prevents rogue APs. Unfortunately, older clients rarely support SAE-PK. A second option is to force users to reconnect using Enterprise WPA2/3 with a given username and password. The client can then pin the certificate of the hotspot's RADIUS server to prevent rogue APs, which must be done with care to avoid rogue APs [7]. However, it is unclear whether this is user-friendly, i.e., user studies are needed to study feasibility, or research is needed to see whether this process can be (partly) automated, e.g., using the provisioning features provided by the Passpoint feature on current devices [4].

In the single-use model, we can rely on the physical proximity to the hotspot. One option is displaying a QR code with the hotspot's Enterprise certificate [13], though current devices do not yet support scanning such QR codes.

An alternative is to use the LED lights already present on most Piso-WiFi hotspots as an out-of-band channel. A client app can record the hotspot's blink pattern to authenticate session key material exchanged over Wi-Fi. This can be based on the protocol of Saxena et al., who also use blinking LEDs for communication [21].

6.3 Secure local caching solutions

In addition to providing a secure connection, optimizing the backhaul bandwidth is also essential, especially when there is limited connectivity. Unfortunately, neither Piso-WiFi nor PM-WANI provide features to locally cache data, e.g., they do not provide an HTTP proxy cache. Doing so would also be non-trivial because most websites use HTTPS, and a local proxy solution would require breaking the end-to-end security properties of HTTPS [2].

One solution to balance end-to-end security with caching, without needing to trust the local cache provider, is to separate authentication and encryption of data. This is feasible since most website content is public and identical for all users [2], meaning this shared data can be locally cached in plaintext while being authenticated (i.e., signed) by the data's origin. Initial experiments indicate that a concrete approach to achieve this can be based on Signed Exchanges (SXGs) [1]. This enables the authentication of web data, independent from where the data is loaded. The local cache provider can still download data using encryption, but store a plaintext signed SXG object in the cache. Clients can query this cache, while still being able to verify that the cached data has not been modified. Interesting future work would be to create a proof-of-concept and to conduct studies to measure the performance advantage of this approach.

6.4 Other improvements and challenges

It may also be beneficial to combine the above proposal with letting clients cache data to create a distributed cache, e.g., extensions of [17]. Other open challenges are ensuring that bandwidth is shared fairly between users, and that users cannot attack each other, i.e., ensuring secure client isolation [29].

7 Related Work

Several works study deployment strategies for extending Internet connectivity to rural regions. Gupta provides a description of India's PM-WANI framework [11], including more technical aspects of its design [12], though without focusing on security. Kumar et al. survey rural Internet connectivity in India and examine technological and economic approaches, including fiber backbones, TV white-space, cellular, and Wi-Fi-based access, highlighting that connectivity remains sparse and often unaffordable in many villages [19]. Additionally, projects such as TUCAN3G explore small-cell and heterogeneous wireless backhaul architectures tailored to isolated rural communities in developing countries [20]. These works primarily focus on coverage, cost, and deployment models, while we focus on the security aspects of low-cost pay-to-use Wi-Fi hotspots.

Other works study the security and privacy of public Wi-Fi networks and their access mechanisms, for instance, Ali et al. conduct a large-scale measurement study of captive portals in public hotspots and show that many track users and leak personal data to third parties [3]. Wang et al. analyse the dedicated mini-browsers used by captive portals and found that missing TLS validation, lack of isolation, and other weaknesses enable credential theft and session hijacking [28]. James provides an overview of practical attacks against open and poorly configured Wi-Fi networks, including MAC-spoofing-based time theft, rogue access points, and man-in-the-middle attacks [18]. Finally, Ishtiaq et al. perform a security analysis of in-flight Wi-Fi paywall systems and uncover design flaws that allow free access and privacy violations [15].

8 Conclusion and Future Work

Providing easy-to-use pay-as-you-go access to Wi-Fi hotspots in a secure and reliable manner remains a challenge, especially in rural areas. Due to limitations of the IEEE 802.11 protocol and its implementations, it is currently challenging to design a solution that is both easy to use, secure, and backwards-compatible. This is evidenced by the practical attacks we confirmed against Piso-WiFi and the PM-WANI system having similar design limitations.

Future Work. An open challenge is performing a practical security evaluation of the PM-WANI framework, e.g., determining its practical susceptibility to user masquerading and rogue AP attacks. Additionally, we believe it is interesting and important future work to design and evaluate improved methods to provide Wi-Fi Internet access in rural regions. A core challenge is doing this in a manner such that the resulting hotspots are compatible with older laptops and smartphones that may not yet support the latest Wi-Fi features. A closely related challenge is also ensuring that, once multiple users are connected, bandwidth is shared fairly between them, and that users cannot attack each other at the network layers above Wi-Fi.

Acknowledgments

This research is partially funded by the Research Fund KU Leuven and the Cybersecurity Research Programme Flanders.

References

[1] 2020. Signed exchanges (SXGs). https://web.dev/articles/signed-exchanges?hl=en. Accessed: 2025-11-12.

[2] Abdulrahman Al-Dailami, Chang Ruan, Zhihong Bao, and Tao Zhang. 2019. QoS3: Secure Caching in HTTPS Based on Fine-Grained Trust Delegation. *SCN* (2019).

[3] Suzan Ali, Tousif Osman, Mohammad Mannan, and Amr Youssef. 2019. On privacy risks of public wifi captive portals. In *International Workshop on Data Privacy Management*. Springer, 80–98.

[4] Wi-Fi Alliance. 2024. *Passpoint Specification Ver. 3.4*.

[5] Android. 2025. API Reference: ScanResult. Retrieved 10 November 2025 from https://developer.android.com/reference/android/net/wifi/ScanResult.

[6] Daniele Antonioli, Sandra Siby, and Nils Ole Tippenhauer. 2017. Practical Evaluation of Passive COTS Eavesdropping in 802.11 b/n/ac WLAN. In *International Conference on Cryptology and Network Security*. Springer, 415–435.

[7] Rathan Appana and Mathy Vanhoef. 2025. Measuring and Preventing Certificate Misconfigurations in Enterprise WPA2/3 Networks. In *9th Cyber Security in Networking Conference (CSNet)*. IEEE, 1–5.

[8] Mahanagar Door Sanchar Bhawan and Jawahar Lal NehruMarg. 2021. PM-WANI framework: Architecture & Specification (Version 2.0). https://www.scribd.com/document/589077192/Annexure-II-PM-WANI-Framework-Architecture-and-Specifications-V2-0. Accessed: 2026-02-25.

[9] Cisco. 2025. Configure Anomalous Endpoint Detection and Enforcement on ISE 2.2. Retrieved 12 November 2025 from https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-22/200973-configure-anomalous-endpoint-detection-a.html.

[10] DoT, GoI. 2020. PM WANI – Wi-Fi Access Network Interface. https://dot.gov.in/pm-wani Accessed: 2025-11-12.

[11] Satya N Gupta. 2023. PM-WANI: A Disaggregated Wi-Fi Roaming Architecture to Connect the Unconnected. *Journal of Mobile Multimedia* 19, 1 (2023), 103–116.

[12] Satya N Gupta. 2024. PM-Wifi Access Network Interface (WANI) and "HotSpot as Managed Service"-Use Case for Connecting the Unconnected.

[13] S Mahmudul Hasan, Che Wei Tu, Endadul Hoque, Omar Chowdhury, and Sze Yiu Chau. 2025. SeQR: A User-Friendly and Secure-by-Design Configurator for Enterprise Wi-Fi. In *CHI*.

[14] IEEE Std 802.11. 2024. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec*.

[15] Abdullah Al Ishtiaq, Raja Hasnain Anwar, Yasra Chandio, Fatima Muhammad Anwar, Syed Rafiul Hussain, and Muhammad Taqi Raza. 2025. Cloud Nine Connectivity: Security Analysis of In-Flight Wi-Fi Paywall Systems. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 76–87.

[16] ITU. 2023. *Measuring digital development: Facts & Figures 2023*. International Telecommunication Union, Telecommunication Development Sector, Geneva. https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/

[17] Sitaram Iyer, Antony Rowstron, and Peter Druschel. 2002. Squirrel: A decentralized peer-to-peer web cache. In *PODC*.

[18] Jason E James et al. 2021. Analysis of Security Features and Vulnerabilities in Public/Open Wi-Fi. *JISAR* 14, 3 (2021), 4.

[19] Shruthi Koratagere Anantha Kumar, Gangavarapu Vigneswara Ihita, Sachin Chaudhari, and Paventhan Arumugam. 2022. A survey on rural internet connectivity in India. In *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*. IEEE, 911–916.

[20] Andres Martinez-Fernandez, Josep Vidal, Javier Simó-Reigadas, Ignacio Prieto-Egido, Adrian Agustin, Juan Paco, and Álvaro Rendón. 2016. The TUCAN3G project: wireless technologies for isolated rural communities in developing countries based on 3G small cell deployments. *IEEE communications magazine* 54, 7 (2016), 36–43.

[21] Nitesh Saxena, J-E Ekberg, Kari Kostiainen, and N Asokan. 2006. Secure device pairing based on a visual channel. In *IEEE S&P*.

[22] Domien Schepers, Aanjhan Ranganathan, and Mathy Vanhoef. 2019. Practical side-channel attacks against wpa-tkip. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*. 415–426.

[23] Domien Schepers, Aanjhan Ranganathan, and Mathy Vanhoef. 2021. Let numbers tell the tale: measuring security trends in Wi-Fi networks and best practices. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 100–105.

[24] Abhishek Sonawane. 2024. Introduction to PM WANI and Gavedu. https://gavedu.com/blog/monetization-passive-income-from-hotspots/introduction-to-pm-wani-gavedu. Accessed: 2025-11-12.

[25] The Filipino Times. 2018. Piso Wi-Fi vending machine can earn you as much as P6,000/month. Retrieved 12 November 2025 from https://filipinotimes.net/feature/2018/10/24/piso-wi-fi-vending-machine-can-earn-much-p6000month/.

[26] Mathy Vanhoef, Prasant Adhikari, and Christina Pöpper. 2020. Protecting wi-fi beacons from outsider forgeries. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 155–160.

[27] Mathy Vanhoef and Frank Piessens. 2013. Practical verification of WPA-TKIP vulnerabilities. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*. 427–436.

[28] Ping-Lun Wang, Kai-Hsiang Chou, Shou-Ching Hsiao, Ann Tene Low, Tiffany Hyun-Jin Kim, and Hsu-Chun Hsiao. 2023. Capturing Antique Browsers in Modern Devices: A Security Analysis of Captive Portal Mini-Browsers. In *International Conference on Applied Cryptography and Network Security*. Springer, 260–283.

[29] Xin'an Zhou, Juefei Pu, Zhutian Liu, Zhiyun Qian, Zhaowei Tan, Srikanth V. Krishnamurthy, and Mathy Vanhoef. 2026. AirSnitch: Demystifying and Breaking Client Isolation in Wi-Fi Networks. In *NDSS*.