# How To Address Unauthorized Broadband Sharing

A technical paper prepared for presentation at SCTE TechExpo24

**Serhad Doken**
Chief Technology Officer
Adeia
3025 Orchard Parkway San Jose CA 90325 USA
serhad.doken@adeia.com

**Dhananjay Lal**
Vice President, Advanced R&D
Adeia
3025 Orchard Parkway San Jose CA 90325 USA
dj.lal@adeia.com

Presented and first published at SCTE TechExpo24

# Table of Contents



## List of Figures

# 1. Introduction

Broadband service providers lose significant revenue each year when subscribers share wireless passwords. One user subscribes to the internet service, paying for a certain bandwidth tier, and provides their Wi-Fi password to neighbors. The subscriber and the neighbors develop an informal relationship to share the internet bill. This is more prevalent in dense urban areas – since Wi-Fi has limited range, several apartments in a multi-dwelling unit (MDU) or vacation properties can share Wi-Fi through informal arrangements between tenants. The use of previous generation Wi-Fi repeaters and improved Wi-Fi Mesh technology offered by Wi-Fi 6E and Wi-Fi 7 helps extend Wi-Fi range, increasing risk of revenue loss for internet service providers. There are plenty of online fora and articles that discuss this [4] [5]. Most, if not all, broadband providers' documented internet use policy prohibits the sharing of internet accounts and broadband bandwidth via Wi-Fi. ISPs and cable operators may consider enforcing prohibition of Wi-Fi password sharing in the future (similar to how stealing cable is illegal and has been strictly enforced). Moreover, detecting if someone is on your Wi-Fi network is important for consumers to not only know but act on for prevention since they will be exposed to numerous cybersecurity attacks. This paper will focus on multiple technical methods for Service Providers to detect if their customers are engaging in such broadband sharing by leveraging novel techniques involving RF, AI & ML and it will teach Service Providers how to mitigate, discourage and prevent such activity.

# 2. Context for Broadband Sharing

ISPs may consider taking action against unauthorized broadband sharing if they have robust detection mechanisms and they project such action will not create customer dissatisfaction. Similarly, Netflix as a SVOD Service have decided to act against account password sharing when revenue growth stalled. In the past, broadband accounts were a growing market which may explain the lack of action. However, growth has recently stalled due to declining household formation, and losing accounts may prompt the ISPs to crack down on Wi-Fi sharing. Moreover, with other upcoming FWA (Fixed Wireless Access) deployments, there will be more competition for broadband customers (versus cable companies historically enjoying a dominant position in a particular geographical region) due to 5G FWA (licensed millimeter Wave using 28 or 39 GHz) between telcos, cable companies and other newcomers (such as using LEO satellites or using unlicensed mmW at 60GHz). T-Mobile has already announced that they have surpassed 1M cellular backhauled broadband customers. AT&T and especially Verizon aims to deploy FWA within urban and large metropolitan areas where the population density is high. Verizon has publicly stated that they are treating 30M homes as potential new 5G FWA customers. These developments will make Wi-Fi sharing an even more important issue because sharing within metro areas may translate into significant revenue leaks for ISPs (cable and telco companies).

Below is Comcast's internet use policy that clearly is against sharing accounts and via Wi-Fi:

https://www.xfinity.com/corporate/customers/policies/highspeedinternetaup

*NETWORK AND USAGE RESTRICTIONS*

- *use the Service for any purpose other than personal and non-commercial residential use (except for your individual use for telecommuting);*

- *use the Service for operation as an Internet service provider or for any business, other legal entity, or organization purpose (whether or not for profit);*

- *restrict, inhibit, or otherwise interfere, regardless of intent, purpose or knowledge, with the ability of any other person to use or enjoy the Service (except for tools for safety and security functions such as*

 

*parental controls, for example), including, without limitation, posting or transmitting any information or software which contains a worm, virus, or other harmful feature, or*

- *impede others' ability to use, send, or retrieve information using the Service.*

- *restrict, inhibit, interfere with, or otherwise disrupt or cause a performance degradation, regardless of intent, purpose or knowledge, to the Service or any Comcast (or Comcast supplier) host, server, backbone network, node or service, or otherwise cause a performance degradation to any Comcast (or Comcast supplier) facilities used to deliver the Service.*

- *resell the Service or otherwise make available to anyone outside the Premises the ability to use the Service (for example, through Wi-Fi or other methods of networking), in whole or in part, directly or indirectly, with the sole exception of your use of Comcast-provided Wi-Fi service in accordance with its then-current terms and policies.*

- *connect the Comcast Equipment to any computer or device outside of your Premises.*

- *interfere with computer networking or telecommunications service to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abusing operator privileges, and attempts to "crash" a host; or*

- *access and use the Service with anything other than a dynamic Internet Protocol ("IP") address that adheres to the dynamic host configuration protocol ("DHCP"). You may not configure the Service or any related equipment to access or use a static IP address or use any protocol other than DHCP unless you are subject to a Service plan that expressly permits you to do so.*

Beyond the revenue leak, there is also the threat of Wi-Fi password crack issue. There are a variety of available tools in the market that can enable a user to get a hold of someone else's Wi-Fi password. Consumers will be at risk if someone cracks their Wi-Fi password and shares the connection to:

- Steal their bank account credentials.
- Use their network to launch cyber-attacks.
- Watch porn!

and a long list of other malicious activities. It is not too surprising to expect that operators may offer services to detect Wi-Fi sharing and monetize this as a protective/preventative consumer service. It is likely that it makes sense to roll out such a feature/service for MDUs (Multi-Dwelling Units). **Figure 1** shows an example floor plan for such a building that hosts multiple units.

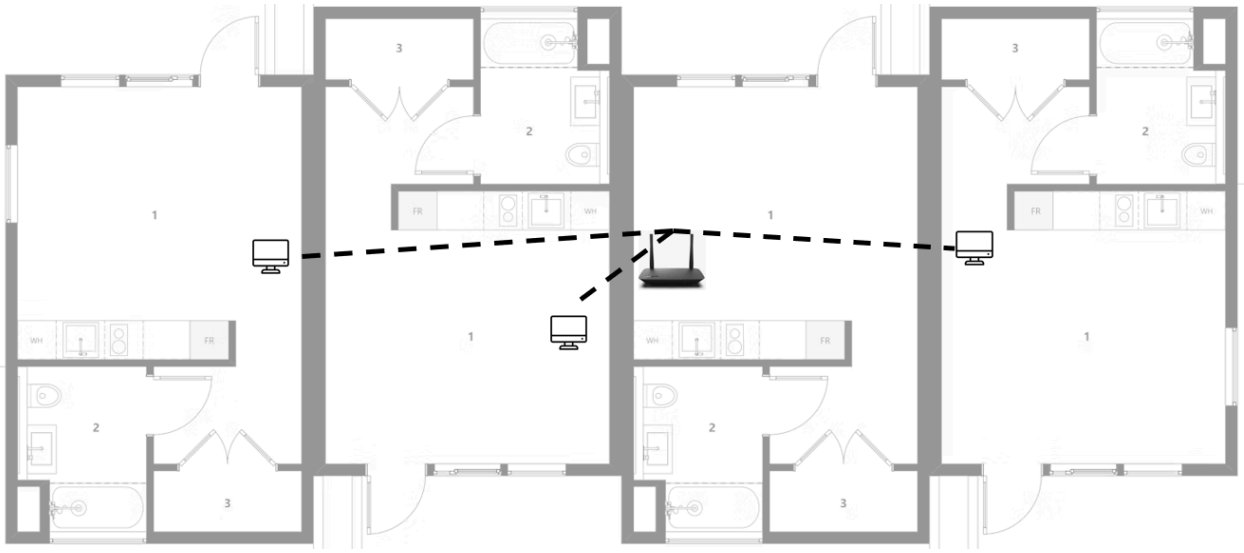

**Figure 1- Floor Plan for a MDU Building floor**

## 3. Multiple Solutions to the problem

We present the reader several different implementation choices for solving the problem. As a basic apriori setup for such implementations, the following parameters will need to be collected.

Broadband Service Provider maintains a table/record of usage data for all its subscriber accounts. Values are measured and updated at periodic intervals, typically at a wired or wireless internet gateway device or the router that is connected to the gateway device. A typical value of this time interval T may be 24 hours.

1. Total # of bits downloaded in time interval T (downstream tonnage)
2. Total # of bits uploaded in time interval T (upstream tonnage)
3. Peak (instantaneous) Downstream Bandwidth in time interval T
4. Peak (instantaneous) Upstream Bandwidth in time interval T
5. Downstream WAN link utilization (Proportion of time that the downstream WAN link is activated during time interval T)
6. Difference in number of browser-based ads served in 2 successive time intervals T

Service Provider also has each subscriber's address in its account data, and it uses an "out-of-band" means to derive the following information about each subscriber account:

1. Home Size
2. Proportion of neighboring Household Passings served = Number of neighboring Household Passings (HHPs)* served/Total number of neighboring HHPs
3. Whether any neighboring account was deactivated in last 30 days (Boolean field)

*A Household Passing is any household that can be served by the service provider, i.e., a household to which a WAN connection exists, and can be activated if requested by the household.

### 3.1. First Method of Implementation (Clustering and Machine Learning)

This method applies when a subscriber has taken broadband (internet) service from the ISP but may or may not have taken the ISP's managed Router (i.e., may have deployed their own router and/or Wi-Fi access points in the premise).

For each element in the usage data record, service provider calculates the difference between the values for the 2 most recent time periods. It then augments the data set generated with the data set derived from the subscriber's home address. Thus, for each subscriber, the service provider has the following data, that is fed into a Machine Learning engine:

1. Difference in total # of bits downloaded in 2 successive time intervals T
2. Difference in total # of bits uploaded in 2 successive time intervals T
3. Difference in peak downstream bandwidth in 2 successive time intervals T
4. Difference in peak upstream bandwidth in 2 successive time intervals T
5. Difference in downstream WAN link utilization in 2 successive time intervals T
6. Difference in number of browser-based ads served in 2 successive time intervals T
7. Home size
8. Proportion of neighboring HHPs served.
9. (Boolean) Whether any neighboring account was deactivated in last 30 days

Machine Learning Technique Deployed

Initially, service provider has little/no labeled data, so it must use an unsupervised learning technique. The service provider builds its data set from neighborhoods/areas where it suspects that the greatest number of subscriber accounts are engaging in Wi-Fi password sharing, for instance, subscriber accounts in MDUs. This helps ensure the maximum likelihood of developing a "balanced dataset" [1]. The service provider shall prune the dataset to achieve balance [2]. The resulting data may have high dimensionality, so methods like Linear Discriminant Analysis (LDA), least absolute shrinkage and selection operator (LASSO), Locally Linear Embedding (LLE), Principal Component Analysis (PCA), Independent Principal Component Analysis (ICA), and Multidimensional Scale Transformation (MDS), are employed to process data to reduce dimensionality. Finally, to account for the difference in scales of the various features (inputs), the data is normalized to create the machine learning model.

Various unsupervised learning methods have been documented in the literature – for this application, a clustering or anomaly detection method will be employed. If clustering methods are employed, then outliers or outlier clusters will be identified. **Figure 2** explains how normalized, reduced dimensionality data may be abstracted in a clustering/anomaly detection machine learning method, where $O_1$, $O_2$ and $O_3$ are outliers, while $N_1$ and $N_2$ account for majority of the data and are regarded as normal.

 

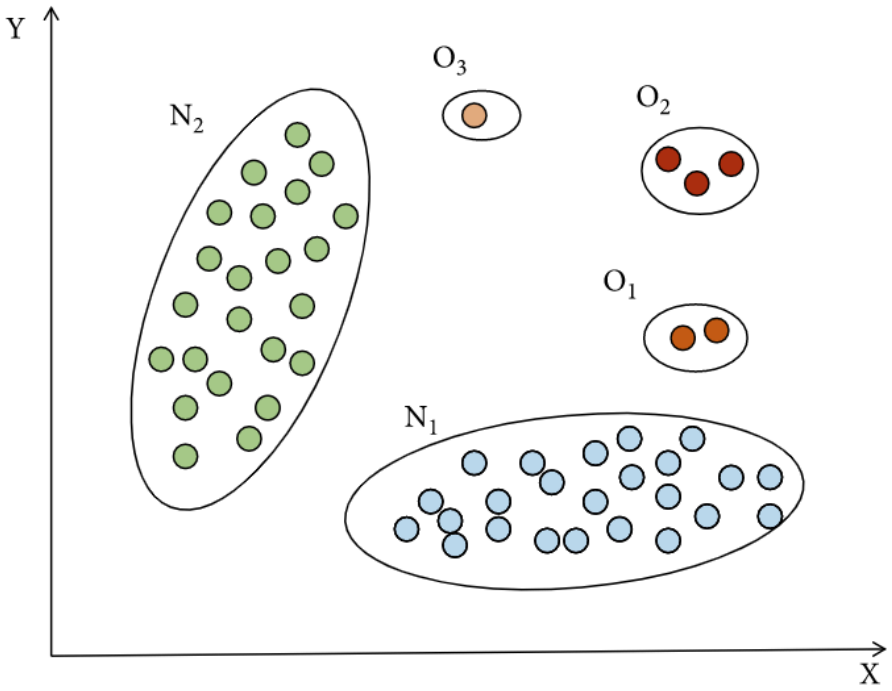


***Figure 2– Clustering of suspected accounts.***

The outlier accounts are marked as suspected accounts and tested using an "out-of-band" means (Ex., Customer outreach, or engaging a third party) as candidate accounts that have higher likelihood of password sharing. The ML engine, as shown on **Figure 3**, will recompute its output every time interval T. Once the predictive model has been created, any subscriber account can be tested for Wi-Fi password sharing.

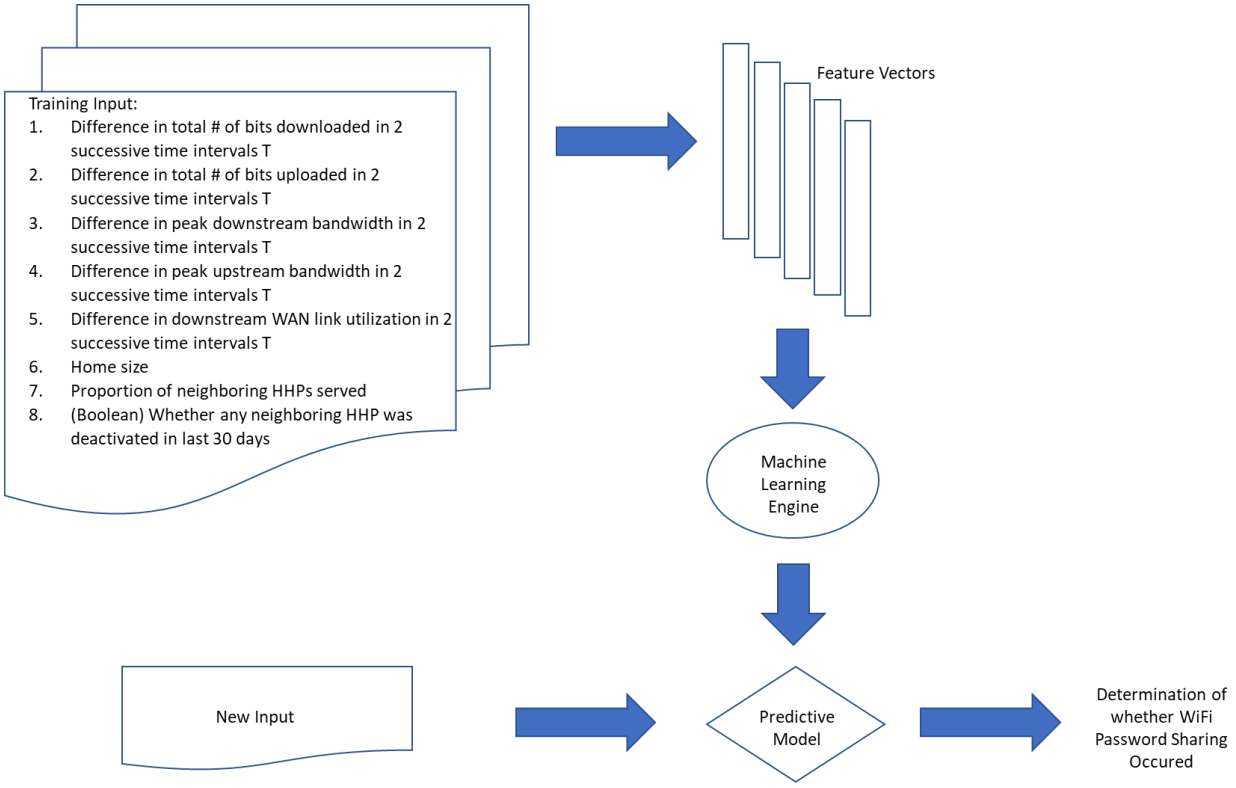


**Figure 3– Machine Learning Model Pipeline**

If the service provider has a means to determine with certainty through the "out-of-band" means that Wi-Fi sharing has occurred, then the service provider can begin to use hybrid unsupervised-supervised machine learning to determine candidate subscriber accounts most likely to have engaged in Wi-Fi sharing. The service provider attaches a "ground truth" True/False label to each data point that is verified against Wi-Fi sharing based on the final determination. In the hybrid technique, the unsupervised component of the ML method separates the data into clusters and outliers, while the supervised learning component helps assign labels to them, improving the identification accuracy of customer accounts that have engaged in Wi-Fi sharing. The True/False label of one or few "ground" truth data points can be assigned to an entire cluster in a hybrid unsupervised-supervised machine learning technique.

Finally, the service provider may, over a period of time, accumulate a large enough labeled data set, i.e., a data set in which it is known whether a customer engaged in Wi-Fi sharing or not through True/False label together with associated data record. At this stage, the service provider may migrate their machine learning technique to a supervised learning method, as shown on **Figure 4**.

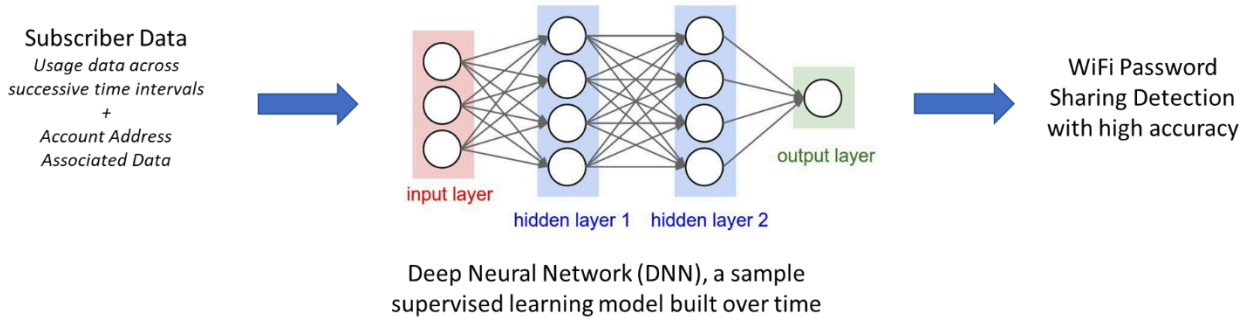


**Figure 4– Supervised DNN leveraging subscriber data (traffic + account)**

## 3.2 Second Method of Implementation (Wi-Fi Sensing)

Methods 2 and 3 would apply when a customer has subscribed to the ISP's managed Wi-Fi service (using the operator supplied router), i.e., the ISP has the ability to collect data about Wi-Fi signal strengths related to specific devices associated with the account.

From this point forward, we'll refer to different sets, in terms of Wi-Fi sharing, as:

- Suspected account list (as maintained by the operator's subscriber management module in their network)
- Suspicious device list (per account). This list may be maintained by a subscriber management module and occasionally pushed to the local Wi-Fi Access Point (AP)/Router
- (Per account) Allowed device list = Total device list - Suspicious device list
- Ensuing methods will be triggered when the ratio of:
    - Suspected devices list / Total device list > Trigger

Trigger is a percentage number that operator determines based on the account nature. Operator will only run further analysis to progress to next steps to detect Wi-Fi sharing if it thinks that this particular account has a high percentage of suspicious devices, not belonging to the account owner. If the suspicious device list contains only one or two devices (could be a desktop in the basement), operator will skip the rest of the steps of the algorithm disclosed below. However, if the suspicious list of devices is 20-30% of the total devices, algorithm will proceed. This trigger percentage number can be determined differently by the operator if the account owner resides at an MDU/Apartment complex or condo or single-family house or simply based on the square footage of the home. Reason for this trigger is not to employ all methods (such as Method 4 and 5, as will be explained below) at once that may be received as annoying or considered overzealous by the account owner. It enables to eliminate most of the false positive cases.

Note that while these methods are separately explained, they may be implemented in a cascaded fashion, especially when the Service Providers limits the set of outliers that are suspected of Wi-Fi sharing. For the outlier accounts (01-03), customer premise deployed router will employ a Wi-Fi sensing method to build a dynamic map of the residence with respect to routers/APs, repeaters, and client devices, as shown on **Figure 5**. This map will be used by the router collecting a time series RSSI and CSI measurements on its own, via its Rx/Tx antennas as well measurements reported by the client devices. Router will be determining home/wall boundaries based on signal reflecting, bouncing and fading characteristics. CSI data will be processing using techniques such as down sampling, frequency domain analysis, logical regression etc.). This method leverages the same 3D CSI matrix of values representing the amplitude

 

attenuation and phase shift of multi-path Wi-Fi channels. Using this data and residence map, router will start marking suspected clients that do not seem to be within the boundaries of this residence. Over time, using the ML techniques utilized on method 1, router SW will strengthen its judgement about certain client devices whether they belong to this residence or not. Such outliers (i.e., candidate devices suspected of sharing the Wi-Fi) that are downloading/uploading traffic may have their access cut off (after a sufficient probation method) by adding them to a blacklist on the router (optionally recording their MAC address) either via their device name or IP address. Other than completely blocking WAN access, other alternate methods may be employed for suspicious devices such as:

- Reducing the uplink/downlink speed
- Increasing latency
- Preventing access to frequently accessed destinations (based on historical patterns)
- Alternating access/block during short time intervals
- Shutting down Rx or Tx channels (alternating during random time intervals)

Service Provider at this point may choose to issue a warning to the account owner via their subscription app or web site that these devices have been suspended due to suspected Wi-Fi sharing.

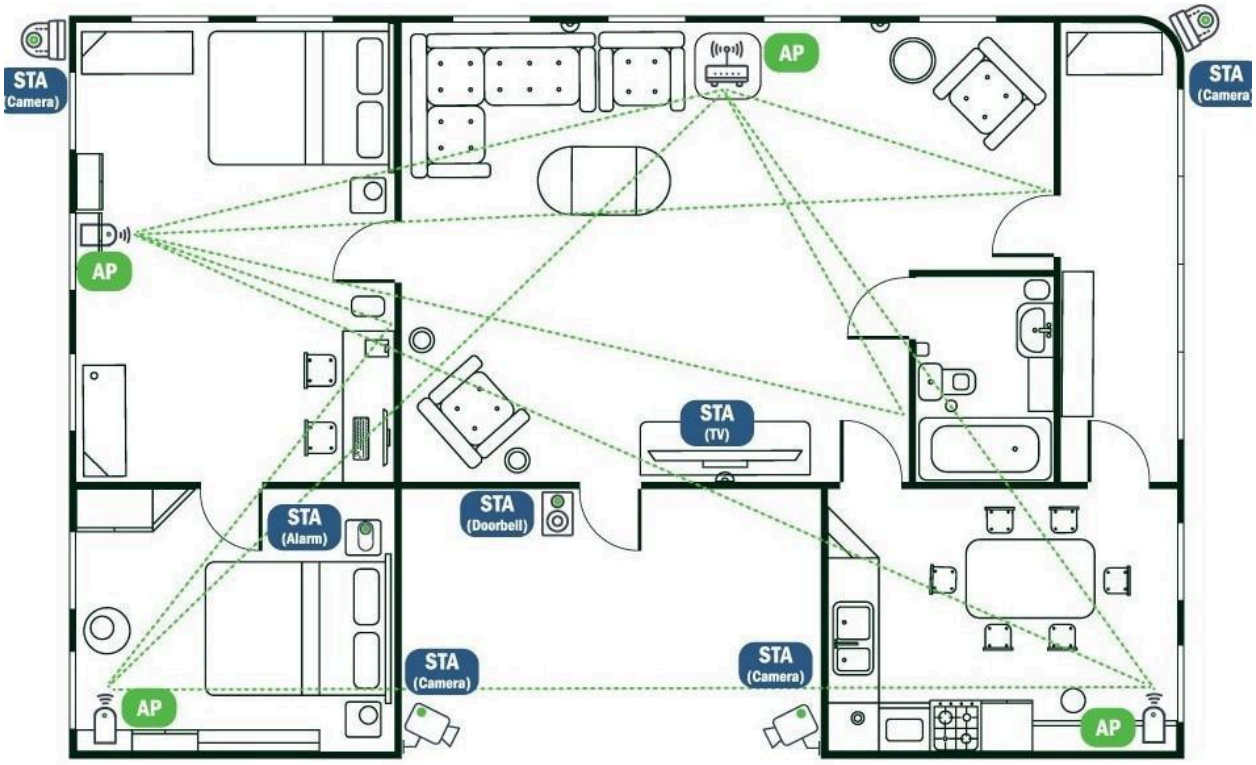


**Figure 5– Dynamic Map of the Household based on Wi-Fi sensing**

 

### 3.3 Third Method of Implementation (Device Ranging)

This third implementation method is a variation of the previously explained second method of implementation. Rather than building a full map of the house, this method aims to employ a lightweight method:

- Collect RSSI / dBm measurements from the client devices connected to the AP/Router. (RSSI is an unscaled value read from a register and can be converted to dBm – they can be used interchangeably)
- Run a histogram to identify devices that have consistently low signal strength / low dBm values (-90 to -60dBm range, for example).
- Determine if these devices move at all. If they are moved, then dBm sometimes strengthens (say occasionally to -30dBm), this means they are more likely to be within this residence so exclude them from the list. If they do move but if RSSI & dBm even goes down furthermore, it's more likely and a stronger indication that these are devices from the neighbor or adjacent apartment unit and add such devices to the suspect list.
- For the remaining devices, determine if they are a static device or more likely installed just outside of the home (desktop in the basement, wireless home surveillance camera etc.) by inspecting the traffic it generates. Employ the techniques described in Method 1 for the suspected devices using only the usage parameters 1-4. For instance, a wireless camera will not be browsing YouTube videos (as opposed to a laptop that may) and therefore exclude them from the list. Or a laptop taken to the backyard temporarily will likely not be there for long periods of time and hence remove them from suspect list.
- This method alone will not be the single one employed since it may generate false positives. Therefore, Service Providers may choose to employ a combination of all methods disclosed.

Furthermore, Inventors acknowledge that range extenders and 802.11ax deployment will make it harder to identify suspicious device list. 802.11ax is just getting rolled out and despite its small footprint today, within the next 5-7 years it is expected that it will be the dominant Wi-Fi standard that will be used by operators. In fact, several operators have already started upgrading their CPE with 802.11ax support. Thanks to that, most devices will enjoy increased signal strength. Since 802.11ax offers extended range and mesh capabilities, we offer slight variations to the disclosed method to identify suspicious devices that are sharing the Wi-Fi network. This algorithm can be implemented as follows:

1. For a short amount of time (split sec), turn off the extension functionality.
    a. Alternatively for a split second, turn off the 6GHz channel.

2. Determine the distance from main router/AP of the suspected device using the dB data reported using the following Free Space Path Loss (FSPL) formula:

    $$FSPL\ (dB) = 20log10(d) + 20log10(f) + K$$

    d = distance

    f = frequency

    K= constant that depends on the units used for d and f

 

If d is measured in kilometers, f in MHz, the formula is:

$$FSPL\ (dB) = 20log10(d) + 20log10(f) + 32.44$$

3. Given home size is known by the operator, check if the computed distance is larger than both width, length, hypotenuse of the residence and issue judgement if this suspected device is within the boundaries of the residence or not. Algorithm will use heuristics, using the historical dBm data from the suspicious devices, since the computed distance may not be totally accurate due to fading signal due to passing human or furniture in the home.

4. Turn on the extension function (or 6GHz channel) when computation is complete

Given that most cable operators also offer cellular services as MVNOs, in case the account owner is also a MVNO customer, yet another method to detect Wi-Fi sharing is whether "suspected mobile devices" are falling back to the MVNO cellular service if the Wi-Fi access are interrupted momentarily. This switch over can be monitored at the ISP vs MVNO Service subscriber management module and mobile devices that are not switched over can be marked as suspicious. Once a suspicious mobile device is detected, this enables the operator to apply more scrutiny to the account and analyze other suspicious devices activity in detail (using methods described above)

## 3.4 Fourth Method of Implementation (Attestation)

This method focuses on using continuous authentication techniques as attestation of whether Wi-Fi sharing is occurring. Despite account owner sharing the simple Wi-Fi password, other account specific info that only the account/residence owner have access to will be queried on suspected list of devices to ensure that particular device on the network is actually a device that belongs to the account owner. There won't be only one question but a series of questions that will be randomly changed and asked to suspected devices. One basic example of that is asking for the router password on the suspected device as shown on **Figure 6**:

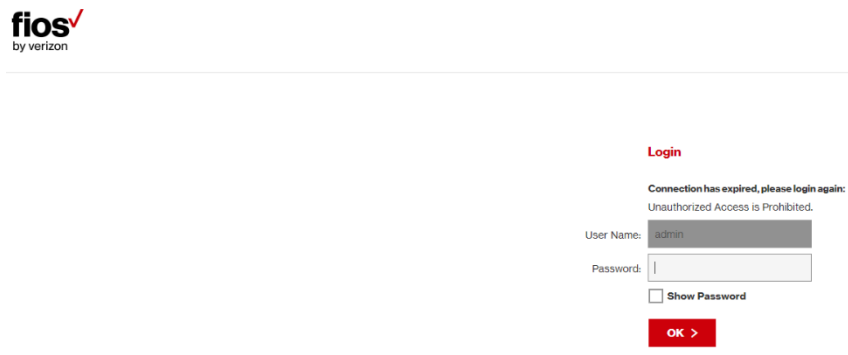


**Figure 6– Attestation via Router password**

It is much less likely that account owner will share their router admin password (not the passkey associated with the SSID) in addition to the Wi-Fi password with a neighbor/freeloader due to security concerns. Note that these questions can be pushed through the router at the residence via the ML algorithms running at the subscriber management module that is on the ISP backend (for instance cable headend) side. It's expected that when attestation questions continuously (but at random times during the day) are pushed to the account owner about the suspected devices (or on the suspected devices), it will create annoyance on the account owner side that will act as a deterrence and possibly terminate Wi-Fi sharing practice. On the other side, freeloader will get tired of trying to guess the answers to the attestation questions and access to his/her device being suspended upon failure to answer correctly.

Another example of attestation is to present the following question to the suspected client device that only the account owner will know. On **Figure 7**, device names within this network are shown:

 

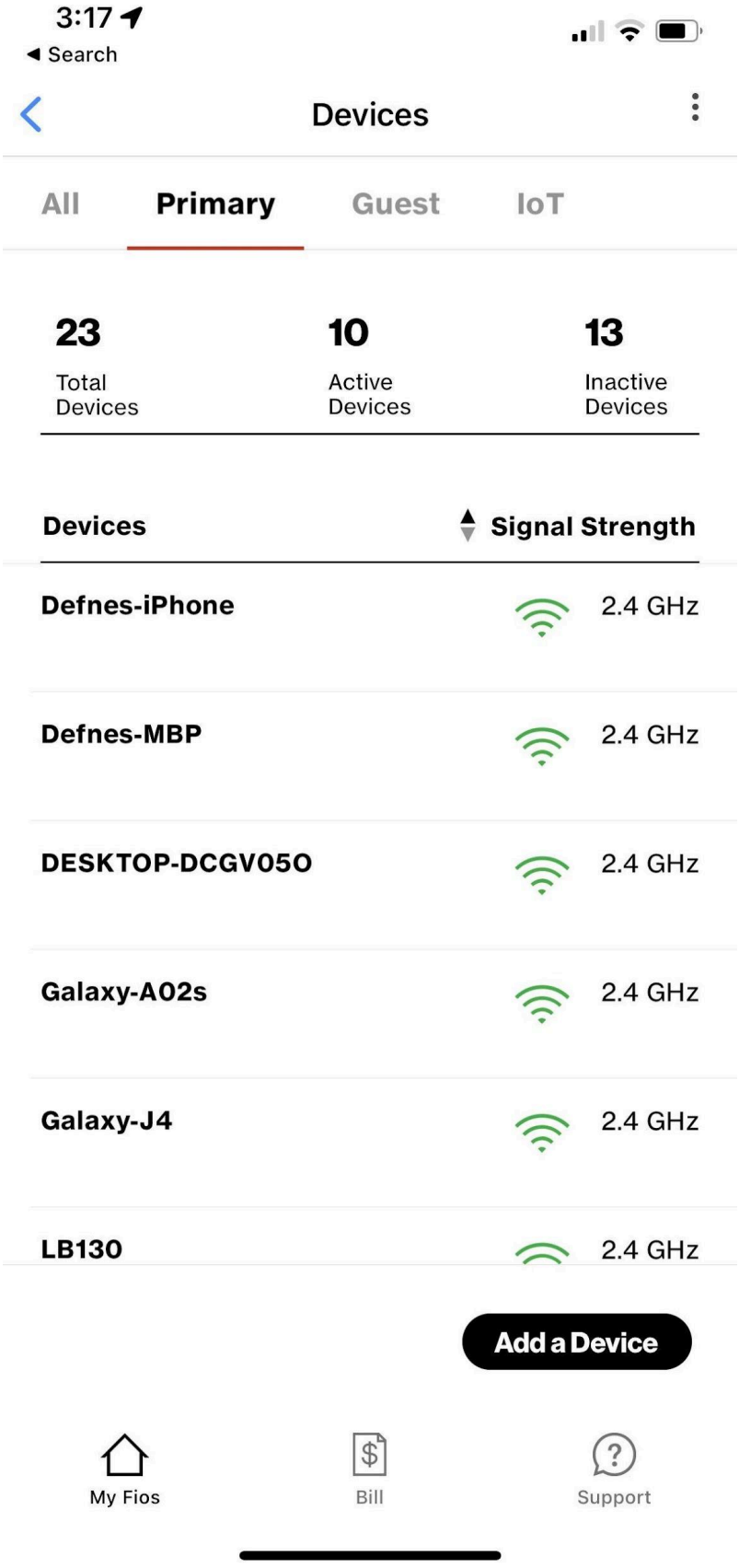

**Figure 7– *Attestation via devices on the network***

Suspected devices will be presented a challenge question to enter the name of a device on the network (or their MAC address or what channel they are using such as 2.4, 5 or 6 GHz) and if they cannot answer it or answer incorrectly, their access will be suspended.

Variety of other multiple-choice challenge questions could be constructed such as:

- Last bill amount
- Last bill payment date
- Specific service details related to account bundle.
- Whether a specific video channel or service is subscribed to by the account owner (if applicable)
- Last truck roll service details like problem and resolution (if applicable)
- Last customer service call details like problem and resolution (if applicable)
- Parental Profile name (if applicable)
- Device Model name

While we also pay attention to not get into PII (Personally Identifiable Info) matters during these challenge questions. Moreover, main account owner devices that are not on the suspected devices list may occasionally be presented questions about the devices from the suspect list whether they want to allow access to this device that the Operator is suspecting that is sharing the Wi-Fi password. This would serve as a deterrent.

### 3.5 Fifth Method of Implementation (RF Signal Control)

Most routers are theoretically capable of supporting 4000 sq ft of coverage area. As a lightweight solution, if the operator strongly suspects that Wi-Fi sharing is enabled by the account owner, despite warnings, it can take control of the main router and adjust its transmit power and antenna gain to surgically fit the coverage area with respect to main account owner residence size. In order to ensure that these parameters are not tinkered with, operator may limit the usage of these parameters to only itself and not the account owner. In the same fashion, alternatively, using beam steering, MIMO RX/TX antennas can be trained to provide the most coverage to devices that are on the clean list and electronically steer the signal away from devices that are on the suspicious list.

## 4. Conclusion

In this paper, we proposed multiple solution implementation choices for an ISP to deal with unauthorized broadband sharing. While the methods have been described at a high level so far, algorithm level details are available for interested readers. Methods explained above leverage sophisticated RF Engineering as well as Machine Learning algorithms. These solutions will help ISPs to prevent revenue leak that may happen due to sharing as well as offer a value-added service for consumers or even apartment operators to protect users against cyber-attacks.

# Abbreviations

| | |
|---|---|
| AI | Artificial Intelligence |
| AP | Access Point |
| DB | Decibel |
| DBM | Decibel milliwatts |
| DNN | Deep Neural Network |
| CSI | Channel Strength Indicator |
| ISP | Internet Service Provider |
| MAC | Medium Access Control |
| MIMO | Multiple Input Multiple Output |
| MVNO | Mobile Virtual Network Operator |
| RSSI | Radio Signal Strength Indicator |
| RX | Receive |
| SSID | Service Set Identifier |
| TX | Transmit |
| WAN | Wide Area Network |

# Bibliography & References

[1] What Is Balanced And Imbalanced Dataset?

https://medium.com/analytics-vidhya/what-is-balance-and-imbalance-dataset-89e8d7f46bc5

[2] Adapted pruning scheme for the framework of imbalanced data-sets

https://www.sciencedirect.com/science/article/pii/S1877050917314047

[3] Unsupervised Anomaly Detection Based on Deep Autoencoding and Clustering

https://www.hindawi.com/journals/scn/2021/7389943/

[4] Internet Sharing – How to Get Revenge on the Cable Company
https://www.mrmoneymustache.com/2012/05/16/internet-sharing-how-to-get-revenge-on-the-cable-company/

[5] Bad idea - sharing Internet with neighbors in apartment?

https://forum.mrmoneymustache.com/ask-a-mustachian/bad-idea-sharing-internet-with-neighbors-in-apartment/

 