IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 9, 2021, accepted November 3, 2021, date of publication November 9, 2021,
date of current version November 18, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3127079*

# A Case Study on the Monitor Mode Passive Capturing of WLAN Packets in an On-the-Move Setup

**AJAY PRASAD[1], (Member, IEEE), SOURABH SINGH VERMA[2], (Senior Member, IEEE), PRIYANKA DAHIYA[3], AND ANIL KUMAR[3], (Senior Member, IEEE)**

[1]School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India
[2]Department of Computer & Communication Engineering (CCE), School of Computing and IT, Manipal University Jaipur, Jaipur 303007, India
[3]Data Science Research Group, DIT University, Dehradun 248009, India

Corresponding author: Anil Kumar (dahiyaanil@yahoo.com)

**ABSTRACT** Monitor mode packet capturing of WLAN is used to derive Access points and devices in the range for localization or occupancy purposes. The general modality of capturing and analysis in almost all available studies is to capture packets by being static (STT) at a location and indoors. In STT mode, the beacon and probe packets extract insights about the localization of devices and occupancy estimation. We propose scanning a predetermined path in an urban locality on the move (OTM) using monitor mode WLAN packet capturing. We also propose that in OTM, devices (STA) and Access Points (APs) can be traced from other packets like CTS, ATS, and ACKs apart from beacons and frames. We performed a case study of monitor mode packet capturing in an on-the-move and outdoor setup. The primary focus of the study was to validate the OTM modality and the methodology of detecting devices and APs. We studied all the packet types that were captured, including Beacons and Probes. The sensed devices and APs counts using probe and beacon packets were compared with the sensed devices, and APs counts using the new methodology. We found that considering other packets helps detect a more significant number of devices and APs. We also found that channel hoping strategy plays an essential role in maximizing the sensed items. The overall exercise revealed that the air is full of WLAN/Wi-Fi traffic, and using OTM can assimilate lots of valuable data and generate relevant information for various purposes. Essentially, on-the-move outdoor capture setups can be used to produce Wi-Fi access points and user devices related heat maps of the scanned locations. This can be useful in many governance and related matters. Briefly, we put forward an application architecture for the same.

**INDEX TERMS** Urban systems, Wi-Fi, WLAN, wireless sniffing, Wi-Fi packet capturing, heat map, monitor mode.

## I. INTRODUCTION

Connectivity is widespread, and almost everyone is connected via mobile devices like smartphones, tablets, etc. The possession of a smartphone can now be seen as a 1 to many mapping between people and devices. We can say in simple terms that almost every person holds at least one smart device. Almost every smart device is connected to the internet via one or other means. One such means is Wi-Fi. Majorly, Wi-Fi devices are categorized into an access point (AP) or router and Wi-Fi adapter in devices (STA). Mobile devices can be clients (STA) or even serve extended Wi-Fi (AP) using hotspots. The speed and spectral efficiency of Wi-Fi has been increasing since its formation. The access point routers can form interconnected extensions covering an area up to several kilometers. Wi-Fi services for WLAN/internet access are used in private homes, businesses, and public spaces. Wi-Fi hotspots or Access Points (APs) can be found everywhere in an urban locality and are generally identified by their unique service names called SSID. Looking at the SSIDs, one can easily identify these services as an Organization, individual, Community, enthusiasts, authorities, and businesses, such as airports, hotels, and restaurants.

The associate editor coordinating the review of this manuscript and approving it for publication was Jose Saldana.

With the advent of smartphones with strong communication capabilities and many embedded sensors, they can provide critical information about people's behaviour and mobility. Ubiquitous Wi-Fi also enables us to extract people-related information like their location, movement patterns, and many other activities by capturing and analyzing connectivity between mobile clients (people) and access points that can be spread throughout vast locality areas. Sniffing systems can sense intermediary data packets and can store the packets for later analysis. Wireless sniffers are also used to sense Wi-Fi packets and analyze wireless traffic [1]. The sniffed packets can help gain several insights like interactions happening between people, troubleshooting hints to network/system administrators to manage networks, and giving many insights into the type of devices and count of people taking part in communications [2]. The capability to monitor, intercept, and decode wireless data in transit makes sniffers useful for various needs. The sniffers capture both incoming and outgoing data packets in promiscuous mode, which is not needed sometimes. In monitor mode, the adapter set in monitor mode senses and collects all data that is flowing in the air.

We suggest here that, capturing WLAN packets passively can be done in two modes. They can be:

a) Fixing the sniffer at a particular location
b) Scan a location by moving the sniffer device at a particular speed.

We will call the former Static (STT) and later as on-the-move(OTM) captures. The sniffed packets in STT mode are widely used for sensing localization and occupancy status of APs and STAs. The main packet types that are used are beacon and probe frames. The Sender addresses in beacons are considered APs, and corresponding unique SSIDs are taken as a named AP. Also, in the case of Devices or STAs, the probe request frames are considered. The sender address in probe request frames is segregated as unique devices.

The paper presents two propositions, they are:

a) The outdoor and OTM passive scans of an urban stretch can also render substantial packets for information gathering.
b) The extraction of unique devices and access points can be enhanced by considering other packets apart from Probes and Beacons.

The basis for a) is that in a smart city and e-governance era several means of data capturing and processing must be explored. Also, in the advent of randomized MACs, identifying unique devices and subsequently predicting occupancy is hindered when adopting STT approach. However, if OTM approach is applied the factor of randomized MAC is suppressed since on the move capturing will capture a Randomized MAC at most once in a scan. The later sections in the paper will present a case study of the Wi-Fi/WLAN packet sniffing in an on-the-move setup. The Wi-Fi sensor adapter and the capturing system will be moving at a particular speed while capturing. We will perform capturing in these two modes (STT and OTM) and present statistics for further evaluation. As in b) we also propose in this paper that while Beacons and probe request frames help sense unique devices and APs, several other types of packets contain APs and STAs as either senders and receivers. Considering these packets as well is necessary for sensing more numbers of APs and devices as the scan durations are of short time and there's a high chance of missing many packets of beacons and probes.

As additional content in this paper, we will discuss one of the significant aspects of OTM capturing. That is, APs and Devices related heat maps. Such heat maps of a locality can provide lots of insights for governance-related matters. We present an architecture of one possible use of OTM scanning. Though, WLAN sniffing can be done for many unethical purposes. Our purpose is to focus on ethical aspects and assume that no unethical tips are drawn out of this exercise.

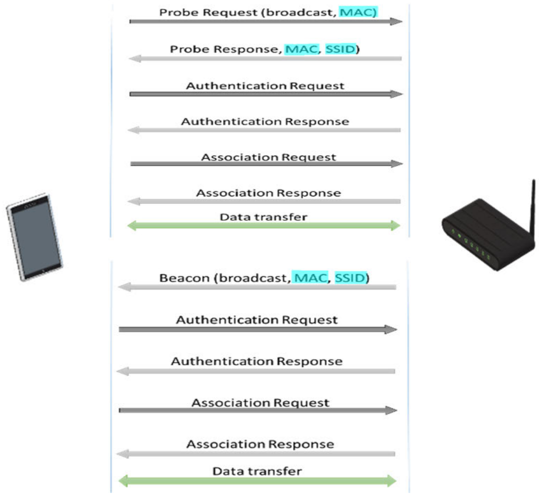


**FIGURE 1.** MACs and SSIDs in a wifi association.

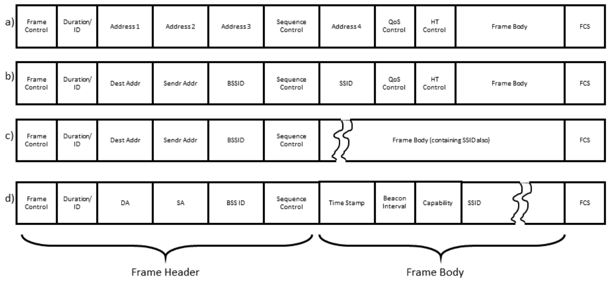


**FIGURE 2.** (a) General MAC layer frame. (b) Probe request frame. (c) Probe Response frame. (d) Beacon frame [4].

## II. BACKGROUND, RELATED LITERATURE, AND THE CASE OF OTM

### A. BACKGROUND

The initial wireless 'association' [3] in all means is purely plaintext. Figures 1 and 2 Show basic association frames and highlight those which can be helpful. The initial procedure involves 802.11 authentications and the association process.

In this, the client device's Wi-Fi adapter scans (via probe request frames) for available frequencies in search of SSIDs to join. In IEEE 802.11 wireless local area networking standards (including Wi-Fi), a service set is a group of wireless network devices which share a service set identifier (SSID) [4]. The basic service set is defined by a primary service set identifier (BSSID) shared by all devices within it. Access points in proximity reply with probe response frames that contain the SSID and BSSID, which corresponds to the access point's MAC address.

Probes can be of two types, directed and broadcast; directed probes are pointed towards specific SSID, whereas the broadcast probes ping all the nearby APs to send a probe response [4]. In the former case, additional information is sniffed about the client and the client's known AP. This information can be of forensic importance, which can be explored further. The triggered response from all nearby APs provide an opportunity for the sniffers to detect and record all nearby APs and their SSIDs. This is of utmost importance in estimating occupancy. Both probe request and probe response frames contain vital MAC addresses, which will help detect different devices [5] near the sniffer and subsequently be analyzed to measure the occupancy status and the mobility traces of people holding the client devices. Another item that can be sensed is the beacons. The beacons are signal frames sent by APs at regular intervals to notify the clients of their presence and possible connectivity. The beacon frames also hold relevant information like SSID and BSSID of the AP. Collecting the beacons and analyzing them can give almost a clear picture of available APs at a given locality [4]. It is also an essential means to know whether many APs at a given locality work in tandem to support a particular SSID and BSSID. Analysis of beacons can give a range and extent of a particular SSID. Almost all packets, including beacon and probe frames, contain vital radio information known as RSSI. Wireless communications received signal strength indicator (RSSI) indicates power present in a received radio signal [6]. The RSSI value is represented in a negative form (e.g., −76). It is assumed that the greater the RSSI value, the stronger the signal. Thus, nearer to 0, the RSS is deemed to be perfect. However, devices can capture packets with strengths as low as 90. RSSI is used as an indicator for localization purposes in many research. It is available in almost all wireless transmitters, and receivers and readings can be obtained without additional hardware requirements [7]. Many packet capture and analysis tools are available. Among them, one is Wireshark [8]. Packets and transmissions captured in Wireshark can be handy for analysis [9] as they contain every bit of information transmitted in the form of probes, beacons, broadcasts, and other associations. Packets of data transfers to and from the client to APs can be traced for many forensic activities. Reaching or finding appropriate and relevant packets can be done by looking at WLAN Traffic and conversations in the statistical menu of Wireshark [10]. The WLAN traffic puts the packets in the context of WLANs setups in a particular zone. Conversations put into perspective all packets captured because it gives the source and destinations into communications. The I/O graphs in Wireshark [10] also give a good sense of activities at zones and can be correlated with conversations.

### *B. RELATED LITERATURE*

Literature using Wi-Fi sniffing as one of the tools for various objectives was studied. The mechanism for Wi-Fi monitor mode capturing for exact OTM type modalities was not found in any literature. Table 1 gives a structured view of several related works using passive monitoring one way or another. Table 1 presents several pieces of literature in terms of their adopted Capture Modality, their study location (whether Indoor or Outdoor), and their Investigating purposes and subjects in packet captures. The General captured modality used in most of the work was static multiple installations indoors as well as outdoors. Mostly the investigating subject in all work was probe requests as they majorly aimed to track occupancy in some way or other. In few cases, the subject was refined to the RSSI for localization purposes. Overall, the methodology of 'scanning an urban location', that is, OTM outdoors was not being tried and tested in works of literature so far. However, the works of literature gave a good insight into the usefulness of the proposed methodology. For example, the authors in [11] adopted a methodology to get an idea of the duration of stay in a coach terminal waiting room by detecting Wi-Fi probe requests from passengers' Wi-Fi devices. The method employs a passive monitoring tool with certain add-on features specifically for probe requests packet analysis. For a different objective, a similar methodology is adopted by authors in [12]. The purpose was to count public transport boarders in the vehicle on transit. Ref. [13] is another work in this direction that used a similar methodology to track public transport occupancy. Many works related to crowd mobility detection have used passive monitoring as a tool such as [14] and [15] where authors aimed to achieve real-time monitoring of people flows in public environments either indoors or outdoors, [16] where authors performed Highway traffic flow measurement, [13] is focusing on estimation of public transport occupancy, [9] worked to prepare Digital footprints, etc.

Authors in [17] discuss De-anonymization of large crowds through smartphone Wi-Fi probe requests. Here, they applied analysis of significant probe responses collected over a considerable period at different large gatherings. This was done using the collected dataset by Wigle.net (Wireless Geographic Logging Engine) [18]. WiFiTrace [27] approach exploits Wi-Fi network logs gathered by enterprise Networks for performance and security monitoring and utilizes them for reconstructing device trajectories for contact tracing. In [17]–[19], the Wi-Fi sniffing is carried out by methods not viable for our purpose. However, [3], [10], [17], [20]–[23], [28], [30] uses sniffing tools conducive to use in our purpose (table 1). Authors in [3] use RPi and Pycom LoPy4 development boards with features of an inbuilt WLAN adapter that can be set in monitor mode. Though RPi 3

**TABLE 1. Various studies of similar nature from literatures.**

| SNo. | Literature | Capture Modality | OTM? | Indoor/Outdoor | Purpose | Investigating subject |
|---|---|---|---|---|---|---|
| 1. | (Yan Li et al, july 2020) | Multiple installations (STT) | N | Indoor/Outdoor | Performance Evaluation of sniffing | Probe Requests and Channels |
| 2. | (Yan Li et al, july 2020) | Multiple installations (STT) | N | Indoor/Outdoor | Performance Evaluation of sniffing | Probe Requests and Channels |
| 3. | (C. Zhang et al, 2019) | Road-side volunteered probes through Mobile devices | Partial | Outdoor | Measurement Study | RSSI |
| 4. | (Edwin Vattapparamban et al, 2016) | Multiple installations (STT) | N | Indoor | Occupancy Tracking | Probe Requests |
| 5. | (Kristof Friess, 2018) | Multiple installations (STT) | N | Indoor | multi-channel-sniffing-system | Channels |
| 6. | (Francesco Potortì et al, 2016) | multiple installations of fogsense sensors (STT) | N | Indoor | analysing crowd movements in indoor areas | Probe Requests |
| 7. | (Di Luzio et al., 2017) | Multiple installations (STT) | N | Outdoor/confined | analysis of WiFi probe request management frames | Probe Requests |
| 8. | (Hong, H. et al., 2016) | Multiple installations (STT) | N | Indoor | extract social behavior and interaction patterns | Probe Requests |
| 9. | (Martin W. Traunmueller et al., 2018) | Multiple installations (STT) | N | Outdoor | model urban mobility trajectories | Probe Requests |
| 10. | (Álvarez Salgado C.F. et al., 2013) | Multiple installations (STT) | N | Outdoor/Confined | measurement process of the distance from AP to a device | RSSI |
| 11. | (P. Fuxjaeger et al., 2014) | positioned two antennas pointing towards vehicles that are driving on the three lanes (STT) | N | Outdoor | road traffic analysis | Probe Requests |
| 12. | (L. Oliveira et al. 2019) | 5 interfaces sensing separate set of channels (STT) | N | Indoor | estimating the number of mobile devices | Probe Requests |
| 13. | (Lin Sun et al, 2017) | sensing devices while moving in horizontal, vertical and diagonal directions in an experimental setup | Partial | Indoor, Outdoor | Localizing mobile devices | Probe Requests |
| 14. | (L. Mikkelsen et al., 2016) | Sensing Probe requests while in moving bus. | Partial | Outdoor/confined | public transport occupancy | Probe Requests |
| 15. | (Yohan Chon et al., 2014) | Multiple moving participants in mobility using a cellular module, WiFi, WPS, and GPS | Partial | Outdoor/Confined | mobile sensing systems for urban life monitoring | Probe Requests |
| 16. | (Tor A. Myrvoll, et al, 2017) | Single STT installation at entry | N | Outdoor/Confined | public transport occupancy | Probe Requests |
| 17. | (Luiz Oliveira,et al. 2018) | Multiple moving volunteers having a sensing device. | N | Outdoor/Confined | sensing urban mobility realtime | Probe Requests |
| 18. | (Takahiko Kusakabe et al., 2018) | Single STT installation at entry | N | Outdoor/Confined | public transport occupancy | Probe Requests |

Model B used in the study doesn't support monitor mode directly but, via Nexmon [24] patches, it can be done quickly. For storage [3] makes use of cheap SD cards. In our case, we can't use SD cards alone as the number of packets captured will be very large, and SD cards may sometimes overflow. This paper only tests the feasibility; hence, the storage model is not discussed here. However, ideas about that are to be explored anyhow. The tests in [3] were done using varied channel hopping strategies, and the results will provide extensive food for thought and help strategize our channel hop strategy. Experiments in [20] use a mobile app (WiFiTracer) that uses the device's Wi-Fi adapters to capture packets. Volunteered captures are then synchronized at a repository hosted on a cloud platform by the data collection module. The approach, though, doesn't use monitor mode adapters and packet analyzers, but have a partial similarity to our study, i.e., the OTM. Essentially all the volunteer WifiTracer hosts are on the move while the app captures packets. Researchers in [21] used Wi-Fi Pineapple(PA) setup to collect probe requests. It deploys 8 PAs to carry out packet capturing, and the data is maintained via a Linux server centrally. Studies in [3], [20], [21] utilize RSS for sensing crowds and use Wireshark or Tcpdump to capture packets. They all are static (STT) installation base approaches. Research in [22] demonstrates multichannel sniffing by using 20 RPis with external monitor mode adapters. Authors in [23] collected probes via a network of sniffing devices, namely FogSense [25] devices distributed by Cloud4Wi®, Inc. To sense the crowd, it uses range-free algorithms based on RSS. All surveys and similar research on Wi-Fi tracking uses RSS as a means to estimate user positioning. Table 1 presents a listing of the literature survey keeping focus on the aspects of setups and capture modality. The setups include the h/w and s/w used, and the capture modality is all about placing the sensors in the location of study, including the way sensing is carried out. Whether the captures are made being OTM or STT and in Indoor, outdoor, or any other place. Several similar works [2], [3], [21]–[23], [26]–[29], and [16], the probes were sensed from static locations. In [13], [15], [20], and [30] there is a feel of OTM capturing in an outdoor setup, which gave many insights into modeling our study. It is observed that most of the research [2], [3], [13], [15], [16], [20]–[23], [26]–[30] have utilized off-the-shelf equipment along with Tcpdump [31] or Wireshark [8], while few have used professional and propriety packages for their experiments. Our study also finally decided to use a wireless adapter supporting monitor mode and Wireshark to capture packets.

### C. CASE OF OTM

The literature survey leads us to work [15], where a definite suggestion was made regarding feasibility in using sniffing systems to understand mobility in urban areas. The case is, how? Mostly all work of outdoor capturing like in [2], [3], [13], [15], [16], [20], [26], [29], and [30] adopted means like static deployments or volunteers with mobile phones. While capturing packets in monitor mode has been studied in many research, the primary modality of capturing almost all was positioning the sniffer device at a static location or using volunteered probe sensing [15], [20]. The primary ethical objective in doing this can be the localization of devices in the ambit, troubleshooting WLAN issues, and many others. However, in OTM mode or scanning of a locality, WLAN sniffing is hardly discussed anywhere in our knowledge in literature. We bring in the modality where, rather than several volunteers scanning randomly in an area, we can have a single sensor scanning in predetermined paths. We submit that it is hard to build a complete scan of an urban setup. However, if principally prime and significant areas of an urban system can be scanned in a systematic (rather than random) approach, many areas of information exploration can be derived. OTM scans can provide many insights about a locality and render support in crisis management and other aspects of governance like crime control, etc. Therefore, the case in this work is for OTM, and, majorly, we will focus on 2 aspects. a) people or users and b) named Wi-Fi services (Access Points or APs) in every scan. We, at this moment, build a test case for the OTM scans. To compare the STT and OTM scans, we will perform packet capturing in both the modes. We will use off-the-shelve h/w and s/w as in many studies. The significant attributes of data collection will be:

1) Packets.
2) packet types.
3) Ratio of each packet type.
4) Probe Requests.
5) Beacons.
6) RSSI measures.
7) Randomized MACs.

Table 2 gives an idea of the essential items captured in monitor mode and the sensed information that can be inferred. In many circumstances, we  assume that while scanning in OTM, we may come across conditions that a device probe request frame is not captured. Lots of Probe requests might get missed while OTM. However, other frames types can be captured, which may contain the device address. This prompts us to believe that not only probe requests, probe responses from an AP, and other packets that emanate from an STA can be considered for finding unique devices. In many cases, the captured packets emanating from APs can also contain unique devices present at the locality that didn't get identified in other packets. Table 2 gives an idea about what needs to be considered while identifying unique devices while in OTM. To identify unique devices, we will consider other packets as well. The methodology will be as follows:

i. Transmitter addresses in all packets except beacons, CTS, probe response and ACKs (including Block ACKs).
ii. Receiver addresses in probe responses, CTS, and Block ACKs.

$$UniqueDevices = UniqueDevicesin\{(i) \cup (ii)\},$$

That is, if

$$\begin{aligned} L &= \{Beacons\} \cup \{CTS\} \cup \\ &\quad \{ProbeResponses\} \cup \{ACKs\} \cup \{BlockACKs\} \\ D_t &= Transmitteraddressesin\{\{Packets\} - \{L\}\} \end{aligned}$$

where,

$$\begin{aligned} D_t &= DevicesasTransmitters \\ D_r &= Recieveraddressesin\{\{Beacons\} \cup \{CTS\} \\ &\quad \cup\{ProbeResponses\} \cup \{BlockACKs\}\} \end{aligned}$$

where,

$$\begin{aligned} D_r &= DevicesasRecievers \\ UniqueDevices &= D_t \cup D_r \end{aligned}$$

In most cases, SSIDs in packets other than beacons and Probe responses may not depict local APs. When the SSIDs are not part of beacons or Probe responses, they should not be considered local to the place of capturing. Hence, when we consider getting unique SSIDs, Both,

i. Transmitter Addresses in beacons and,
ii. Transmitter Addresses in probe responses might be considered.

$$UniqueSSIDsorAPs = Uniqueaddressesin\{(i) \cup (ii)\}$$

**TABLE 2. Various packet types and the relevant information that can be extracted from them.**

| | Data items of interest | | | | | transmission | | |
|---|---|---|---|---|---|---|---|---|
| Packet type | RSSI | SSID | BSSID | SA | RA | From | To | Information that can be interpreted |
| Beacon | Y | Y | Y | Y | | AP | Broadcast | Named WIFI services, area of coverage, Number of APs |
| Probe Req | Y | Y | Y | Y | Y | STA | AP | Unique users, User device, frequent SSIDs the device connects to. |
| Probe Res | Y | Y | Y | Y | Y | AP | STA | Named WIFI services, Number of APs |
| Probe Req Broadcast | Y | Y | | Y | | STA | Broadcast | Unique users, User device |
| Null Frame | Y | Y | Y | Y | Y | STA | AP | Control information (generally power management), can give power status of the user device. |
| ACK | Y | | | Y | | NA | NA | Unique users, User device |
| RTS | Y | | | Y | Y | STA | AP | Unique users, User device |
| CTS | Y | | | Y | | AP | STA | Unique users, User device |

That is,

$$\begin{aligned} BA_t &= Transmitteraddressesin\{Beacons\} \\ PA_t &= Transmitteraddressesin\{ProbeResponses\} \\ AccessPoints(APs) &= BA_t \cup PA_t \end{aligned}$$

The same principle will be followed in the case of STT also.

We are not performing the tests for performance in this study. Performance of packet captures and channel selections will be studied and compared with existing literature as future work. However, we do present a comparison for two modes of channel selection a) capturing for channels 1 to 13 (being used in most of the world [32]), b) capturing for channels 1 to 11. The case is not to put forward any comparisons as such. The metrics are meant to provide a visualization of the validity of the OTM modality. If OTM scans are done, then, there is a significant chance that we could get lots of data to build relevant information in the tracks of Localization/Tracking/Density, De-Anonymization, Users/Device Profiling as suggested in [2]. We do not conform that our case is really to target De-Anonymization and Users/Device Profiling. Majorly, through this case study, we suggest that the collected information can help build useful localized heat maps that can help in urban planning and management in several aspects.

## III. EXPERIMENTAL SETUP, RESULTS, AND DISCUSSIONS

### A. EXPERIMENTAL SETUP

We used a cheap Wireless USB Wi-Fi Adapter employing Ralink RT5370 chipset for 2.5GHz WLANs supporting Monitor mode. The manufacturer claims a 3dBi power antennae, which was installed on the vehicle's glass window (figure 3) used for capturing test data. The Wi-Fi adapter connects in 'managed mode but can be switched to 'monitor mode easily in kali Linux. The Wireshark was used to capture packets, and the collected information was analyzed both in raw form and from generic statistics extracted in it.

The channel hoping strategy was also the simplest among all, where we hopped each channel (ch 1 to ch 13) in equal intervals of 0.1 seconds. The code for the channel hoping was derived from the portal [33]. It is also to be noted that channel hoping can be further refined to gain maximum throughput in packet capturing. In the case of OTM, the study was done on a 4 Km stretch of a busy road in Dehradun City in the morning rush hour. The experimental sniffer setup consisting of a Wi-Fi adapter over a laptop running kali was placed in a vehicle. The vehicle was moved at a speed of 15-25 kmph. Almost all the vehicle was kept at the leftmost end of the road (figure 3). In the case of STT, the captures were done stationed at a busy crossroad in Dehradun city of India. Both the OTM scan and the STT captures were made through the Wireshark, and the captures were saved for analysis in pcapng file format. Recording of packet captures was done for 15-minute durations in both OTM and STT modes. The STT capture was made at a busy crossroad on the same road for the same 15-minute duration. The capturing was for longer than 15-minute duration. The actual 15-minute test data were extracted from the Wireshark pcapng file discarding packets few minutes from start and end of captures using 'editcap' commands for both OTM and STT captures. We also experimented on the same stretch of road with a channel hopping strategy of 0.1 seconds on channels 1-11. The results of both the setups are presented for the OTM case. The results for channel hoping strategy 1-13 were used for both STT and OTM cases, and results are put forward for further studies.

### B. RESULTS AND DISCUSSION

Figure 4 shows the overall view of both the captures in the form of I/O graphs derived from Wireshark. The raw data in the pcapng file were further analyzed. General metrics that were compared are 1. The number of packets, 2. The number of probes. 3. Number of beacons. 4. I/O metrics. 5. the Approximate number of user devices (Probes). 6. The approximate number of Wi-Fi Services/APs (Beacons). 7. RSSI values Since there was no previous data for the above metrics on the outdoor front for the static case, we recorded data for both cases ourselves for the comparison mentioned in the previous section.

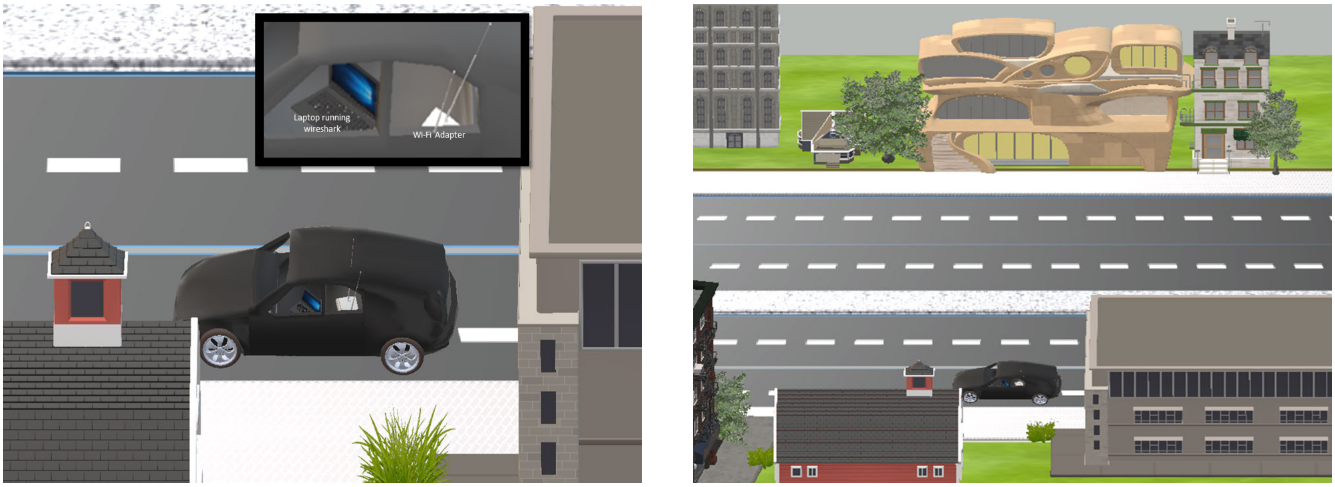


**FIGURE 3.** View of the experimental setup for OTM. Close up and inset view shows the onboard laptop and wifi sensor. The OTM view on a streetview shows the vehicle was kept at one side of the road.

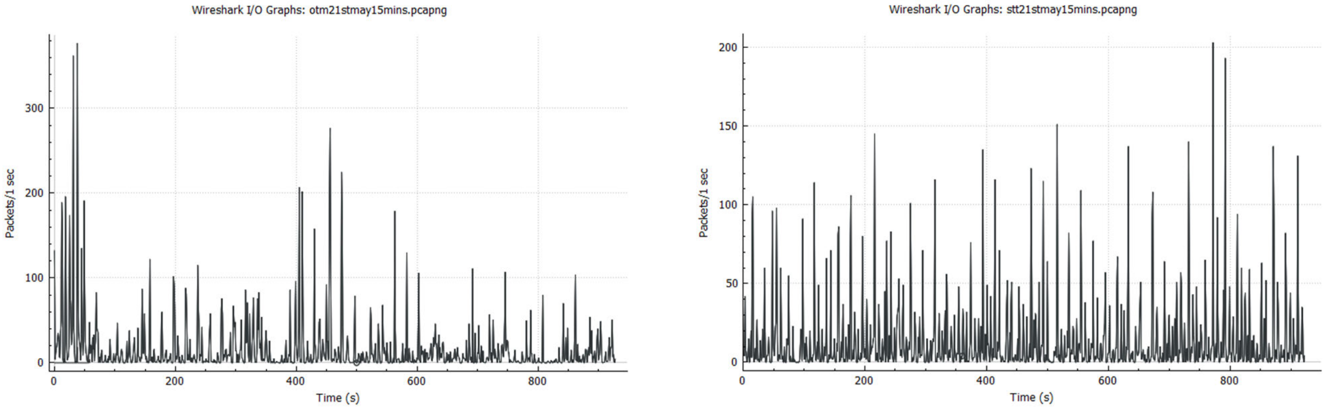
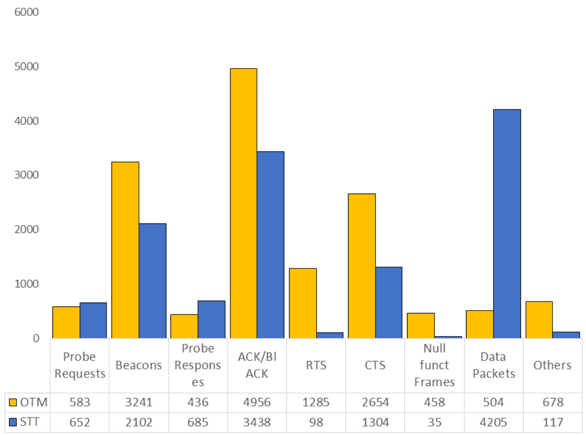


**FIGURE 4.** I/O graphs in OTM and STT captures.

OTM captured around 15% more packets, which may be due to its scan nature. The comparison of captures in both modalities is shown as a bar graph in figure 5.

Both STT, as well as OTM, were able to capture sufficient numbers of packets. The major significant difference was in the number of data packets. The STT captured a much larger number (figure 5 and 6) of data packets than in OTM. This can be due to the static nature of the capturing and also because mostly data packets may appear at only a few Locations while on the moving scan.

In terms of devices (figure 7), the OTM could sense more devices than STT when the device identification was made using the process described in the previous section. Whereas, if only probe request was considered, the number of devices sensed in both cases was almost identical. The approach of identifying devices and APs in the previous section was used considering other relevant packets. Table 3 presents the intermediate counts following the approach. It is evident that, while STT, the number of devices will be lesser than OTM. However, the device density in the case of STT will be much higher as it captures devices at only one location. The randomized MACs in the case of OTM are proportionately



| | Probe Requests | Beacons | Probe Respons es | ACK/BI ACK | RTS | CTS | Null funct Frames | Data Packets | Others |
|---|---|---|---|---|---|---|---|---|---|
| OTM | 583 | 3241 | 436 | 4956 | 1285 | 2654 | 458 | 504 | 678 |
| STT | 652 | 2102 | 685 | 3438 | 98 | 1304 | 35 | 4205 | 117 |

**FIGURE 5.** Various packet types in OTM and STT.

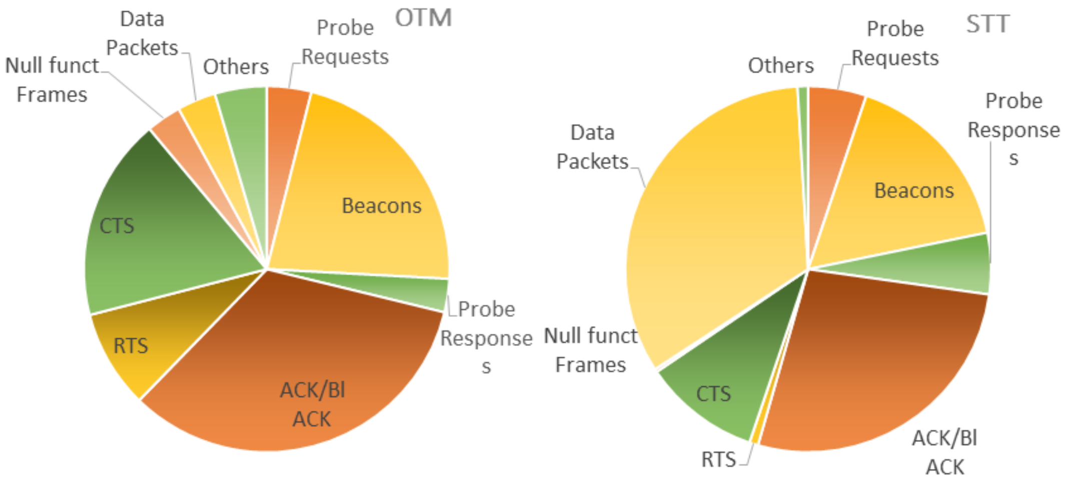


**FIGURE 6.** Pie graph view of OTM and STT captures.

**TABLE 3.** Observed counts of Devices and APs observed considering various other packets. (a) Devices. (b) APs.

| Devices | OTM2 | | STT | | OTM1 | |
|---|---|---|---|---|---|---|
| | $D_t$ | $D_r$ | $D_t$ | $D_r$ | $D_t$ | $D_r$ |
| Total Packets | 3526 | 5853 | 5107 | 3927 | 2567 | 4503 |
| $D_t \cup D_r$ | 808 | | 335 | | 667 | |

b) APs.

| APs | OTM2 | STT | OTM1 |
|---|---|---|---|
| | $BA_t and PA_t$ | $BA_t and PA_t$ | $BA_t and PA_t$ |
| Total Packets | 3677 | 2787 | 5536 |
| $BA_t \cup PA_t$ | 421 | 42 | 476 |

**TABLE 4.** RSSI values in OTM and STT.

| RSS | Average | Min | Max |
|---|---|---|---|
| in Probe Requests(OTM) | -64.66 | -85 | -17 |
| in Beacons(OTM) | -63.82 | -83 | -35 |
| in Probe Requests(STT) | -62.35 | -83 | -19 |
| in Beacons(STT) | -63.63 | -83 | -41 |
| All packets(OTM) | -65.81 | -87 | -17 |
| All packets (STT) | -60.15 | -85 | -19 |

higher than that of STT. The randomization frequency in most devices is more than an hour, as mentioned in [34]. Hence we Assume that every Randomized MAC is representing one unique device. Thus, it is not a significant hindrance in building heat maps. As expected, the randomized MACs in STT are a significant part of overall unique devices. In the case of OTM, it's not major; however, quite significant.

In APs in both the captures (figure 8), OTM showed a more significant number of APs identified as expected. This is because the scan covers a larger area and thus senses much more beacons than in STT. Also, the beacons and other packets emanating from APs will be from a more extensive range of APs than in STT.

The Received signal strengths were also almost similar and enough for capturing substantial packets in both OTM and STT. The RSS was almost similar while sensing in OTM and STT. Table 4 gives the average signal strengths in probe requests and beacons in both STT and OTM. The overall packets show a slight variation in average RSSI such that, in STT its little on the higher side as expected. However, minimum and maximum values are similar. Thus, the signal strengths in the case of OTM are quite enough and conducive for capturing sufficient packets.

### C. COMPARING CHANNEL HOPPING

We performed OTM using two modes of channel hopping. a) Hopping 0.1s each from channel 1 to channel 11 (ch A). b) Hopping 0.1s each from channel 1 to channel 14 (Ch B). The scans were done for 15 minutes on the same stretch of road on different days. Surprisingly, in Ch A and Ch B, the packets captured were almost identical to Ch B, recording meagerly higher numbers of packets. In Ch A, i.e., OTM1,

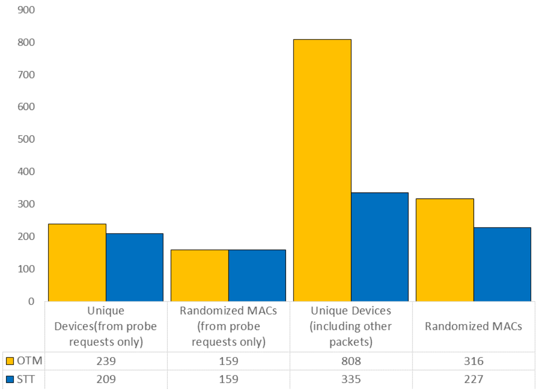


FIGURE 7. Devices identified in both OTM and STT.

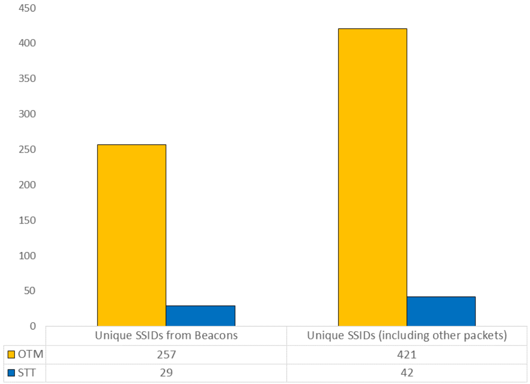


FIGURE 8. Devices identified in both OTM and STT.

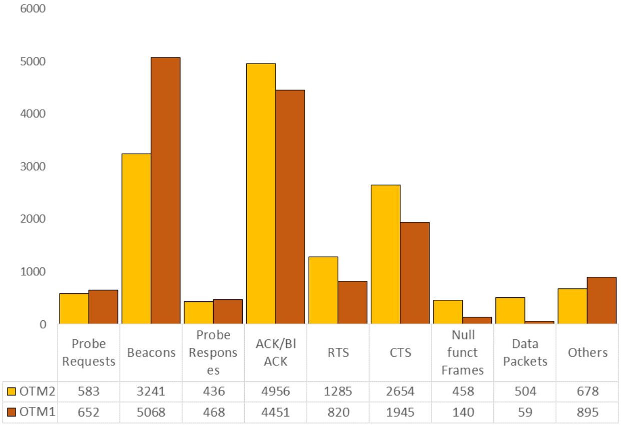


FIGURE 9. Various packet types in OTM1 and OTM2.

the total packets captured were 14498, and in the case of Ch B, i.e., OTM2, it was 14795. Beacons, probe responses, and probe requests were little on the higher side in OTM1 (figure 9). Figure 9 gives the collected counts of various packet types in both the captures. Even while spending a reasonable amount of time on channels 12-14, it is found that almost similar captures occurred. The reasons can be a good amount of services are in channels 12 and 13 also in this part of the world. A total of 1335 out of 14795 packets in OTM2 belonged to channels 12,13 and 14. A fact that can't be ignored is the social factors surrounding the dreadful Covid19 situation in India, as the OTM1 was recorded on 26th of April 2021 and the OTM2 was recorded on May 21st 2021. The Covid19 situation at these two dates was drastically different, and hence the lockdowns and mass movement were also variable on these dates. We, however, do not make any claims in this matter and will leave this for later studies on channel hoping strategies.

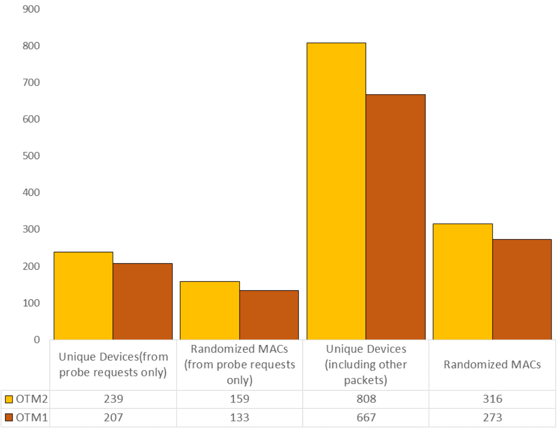


FIGURE 10. Devices identified in OTM1 and OTM2.

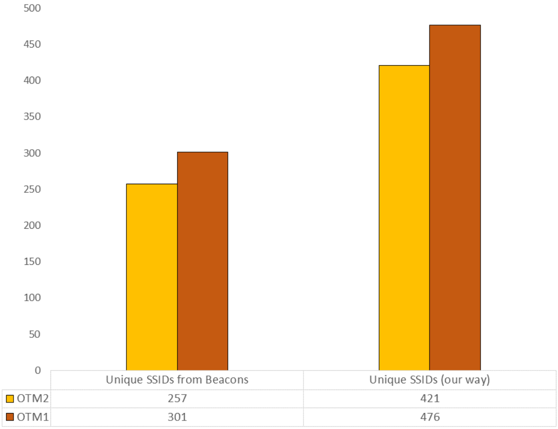
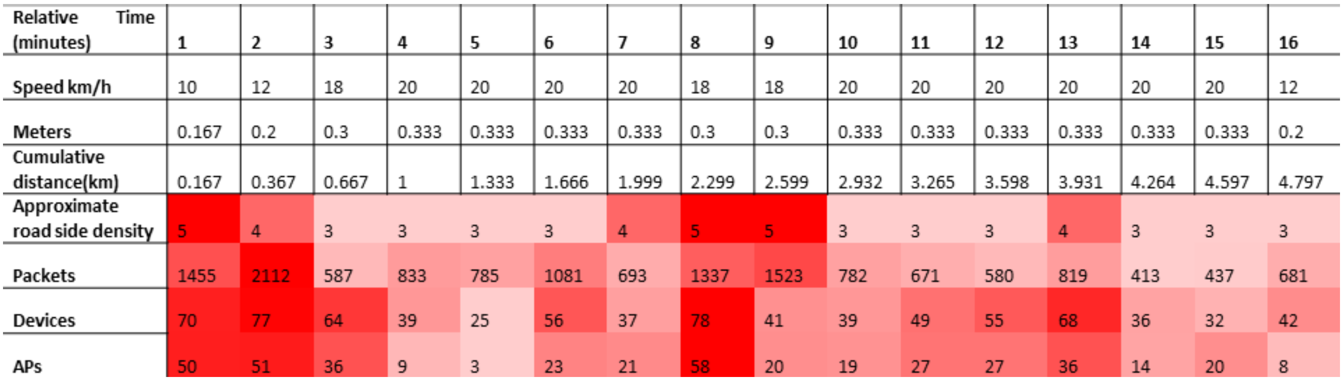


FIGURE 11. APs identified in OTM1 and OTM2.

Looking at the unique devices identified in both scans, again. OTM2 was on the higher side (figure 10). The prime reason might be a little higher number of packets captured in the later case. In the case of identified APs, OTM1 was on a higher side (figure 10). We are not suggesting any particular reason for this. However, if we bring in these two scans' social conditions, we certainly get more clues to ponder upon. This boosts the idea that OTM can be a powerful way to read and study social patterns in a locality. Also, it confirms that each scan of a locality will add valuable unique data in the knowledge bank, and the collected data can be used to



| Relative Time (minutes) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Speed km/h | 10 | 12 | 18 | 20 | 20 | 20 | 20 | 18 | 18 | 20 | 20 | 20 | 20 | 20 | 20 | 12 |
| Meters | 0.167 | 0.2 | 0.3 | 0.333 | 0.333 | 0.333 | 0.333 | 0.3 | 0.3 | 0.333 | 0.333 | 0.333 | 0.333 | 0.333 | 0.333 | 0.2 |
| Cumulative distance(km) | 0.167 | 0.367 | 0.667 | 1 | 1.333 | 1.666 | 1.999 | 2.299 | 2.599 | 2.932 | 3.265 | 3.598 | 3.931 | 4.264 | 4.597 | 4.797 |
| Approximate road side density | 5 | 4 | 3 | 3 | 3 | 3 | 4 | 5 | 5 | 3 | 3 | 3 | 4 | 3 | 3 | 3 |
| Packets | 1455 | 2112 | 587 | 833 | 785 | 1081 | 693 | 1337 | 1523 | 782 | 671 | 580 | 819 | 413 | 437 | 681 |
| Devices | 70 | 77 | 64 | 39 | 25 | 56 | 37 | 78 | 41 | 39 | 49 | 55 | 68 | 36 | 32 | 42 |
| APs | 50 | 51 | 36 | 9 | 3 | 23 | 21 | 58 | 20 | 19 | 27 | 27 | 36 | 14 | 20 | 8 |

**FIGURE 12.** Heat maps for packets, identified devices and APs.

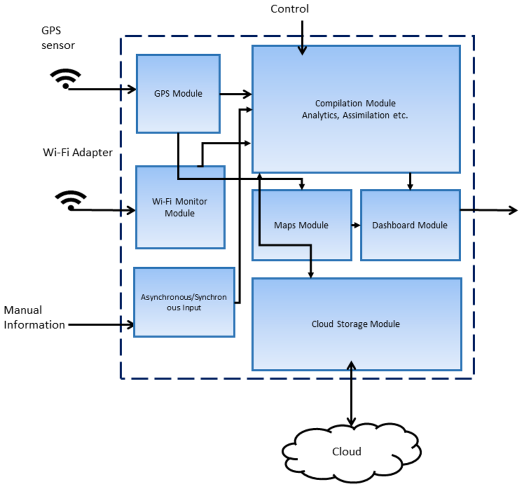


**FIGURE 13.** Architecture of the proposed application.

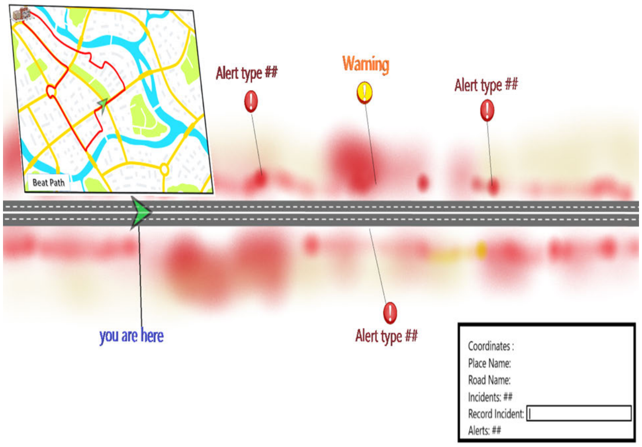


**FIGURE 14.** A generic view of the dashboard with alerts and heat maps.

establish factual knowledge of the locality that can render benefits in several ways.

### D. HEAT MAPS OF VARIOUS ITEMS OF INTEREST

We propose that, essentially, the OTM scans can yield output in the form of heat maps that can be useful in providing assistance in town planning, policing, disaster management, etc. To demonstrate this, the output packets, Devices, and APs were segregated and counted in terms of the time of captures, and the cells were given colors relative to their frequencies. That is, the intensity of color increases with the relative lowest to highest frequencies in the series. Figure 12 gives a heat map view of the packets, Devices, and APs. To get a deeper feel of their relation to the subject, we have also given a heat map view of the approximate roadside density (population) on the scale of 0-5 (this is merely based on manual observation). The vehicle's speed at a 1-minute interval was also recorded to give an additional idea of the conformance of the captures. Figure 14 in the next section depicts that this heat map can be synced with the actual map with other information on a dashboard.

The heat maps of APs and Devices are expectedly similar. They both match to a reasonable extent with the roadside density. However, the device population might be very different at few places, which has to be equated with the social factors of the region. The exact maps can be made when the tests are carried out, accompanied by a GPS and the time tallied GPS and Packets, thus leading us to more accurate heat maps of the locality than on locality maps.

## IV. OTM-BASED MONITORING APPLICATION ARCHITECTURE

Overall, the results show that OTM can also be a mode that can be useful in many senses. The heat map application can be suitable for governance and statistical agencies and thus can be modeled. Figure 13 gives an architectural overview of the application. The GPS and Wi-Fi monitor modules will sense the geolocations and the packets in the air, respectively. The GPS module will use GPS devices or sensors to get the geolocation in high-frequency intervals. The Wi-Fi adapter (monitor mode capable) will sense the Wi-Fi bands and capture packets using Wireshark [8] or any suitable packet capture tool. The sensed data will be synchronized by time and sent to the compilation module in real-time. The compilation module will assimilate the received data with previous data and send the compiled data to the maps module and dashboard for visualized output. It will also send the data to cloud storage using appropriate APIs like JSON etc. Another form of input can be the Manual information about any location. It can be any incident or notes that the user wants to make. These notes can help generate appropriate alerts while scanning prompting for a pause or a small halt for data captures for further probing. The compilation module will also compile this information in sync with time and location.

A generic view of the dashboard can be shown in figure 14. Majorly, the dashboard will show the current position on the map and the collected heat map based on previous records/scans. The dashboard will also be having prompts to input records or notes. Other aspects like graphical visualizations etc., will also be viewed through the dashboard. By presenting this architecture, we aim to give an application perspective to the study to be taken up further by developers. In general, many application areas can be explored using the OTM modality like Measure of occupancy status, Location tracking of suspicious mobiles, Track of named and public SSIDs like malls, hotels, restaurants, etc. and their extent in a locality on the map, Vulnerability Assessments of public Wi-Fi's in localities, Maintain historical records: Forensics, seized mobile phones and captured location tracking and history relooking, Tracking sudden movements or exodus, Beats/patrolling by building Wi-Fi hotspots, Managing emergency evacuations, Managing lawful closures and lockdowns, Conducting rescue operations, Detect suspicious Wi-Fi traffic, etc.

## V. CONCLUSION

The On-the-move modality of passive Wi-Fi packet captures was studied and compared with the static model. Both the OTM and STT modality of outdoor packet capturing in an urban stretch were able to capture sufficient packets of WiFi/WLAN. The OTM was able to capture a much larger count of unique devices and APs as compared to STT. The unique devices and APs conformed to a good extent with the estimated population alongside the urban stretch. The unique devices and APs count have no effect due to MAC randomization in the case of OTM. The study revealed that some circumstantial aspects of the urban population can be sensed and managed by studying and analyzing OTM scans and records. The RSS values in OTM scans were found to be feeble yet enough for the receivers to capture packets. The methodology of OTM can be invariantly called 'scans' and can be very useful in many ways. Regular scans of a locality can refine the heatmaps as well as can give several insights into the people and mass behavior in terms of mobility, density, sudden changes, crime localization, etc. However, if forensic requirements are to be considered then STT can be more useful as it can lead to capturing a lot more data packets than OTM for analysis. With a simple approach of channel hopping and off-the-shelf equipment, we were able to sense a good amount of devices and access points throughout the road in the city of Dehradun, India. We also found that the amount of identified devices and APs is much more if we look deeper into other packets rather than only probe requests and beacons. Channel hoping, or other proven channel selection methodologies can be adopted for better capturing. Two different strategies adopted (OTM and STT) in the study showed little or less significant difference in the overall captures. However, the reason is unclear and needs more exploration and study. Capturing equipment of better-receiving strengths can be employed to get enhanced counts of packets and thus will significantly increase the number of devices, and APs identified. Using the new methodology to identify unique devices from the captured packets was found to sense a much more number of devices and APs in both OTM and STT modalities. This can help other works to optimize their approach and objectives. In this study we have confined the scope to 2.5 GHz which is mostly used and has a longer range than 5 GHz which can be sensed passively on the move. However, as a future work 5 GHz channels and WiMax can be brought under the scope. The study also includes building a time-based heat map of packets, devices, and APs. The results were promising and validate the usefulness of the OTM passive capturing of Wi-Fi packets. Lastly, an application architecture for a proper OTM-based scanning system is put forward for further exploration. The whole intention of the work is to bring readers/researchers little attention to this possibility. This approach can bring in many leads towards rendering support in smart city applications, disaster management, emergency evacuations, etc.

## REFERENCES

[1] N. T. Anh and R. Shorey, "Network sniffing tools for WLANs: Merits and limitations," in *Proc. IEEE Int. Conf. Pers. Wireless Commun. (ICPWC)*, Jan. 2005, pp. 389–393, doi: 10.1109/ICPWC.2005.1431372.

[2] A. E. C. Redondi and M. Cesana, "Building up knowledge through passive WiFi probes," *Comput. Commun.*, vol. 117, pp. 1–12, Feb. 2018, doi: 10.1016/j.comcom.2017.12.012.

[3] Y. Li, J. Barthelemy, S. Sun, P. Perez, and B. Moran, "A case study of WiFi sniffing performance evaluation," *IEEE Access*, vol. 8, pp. 129224–129235, 2020, doi: 10.1109/ACCESS.2020.3008533.

[4] M. S. Gast, *Framing in Detail* (802.11 Wireless Networks: The Definitive Guide), 2nd ed. Newton, MA, USA: O'Reilly Media, 2005, ch. 4. [Online]. Available: https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html

[5] P. Torkamandi, L. Kärkkäinen, and J. Ott, "An online method for estimating the wireless device count via privacy-preserving wi-fi fingerprinting," in *Passive and Active Measurement*, O. Hohlfeld, A. Lutu, and D. Levin, Eds. Cham, Switzerland: Springer, 2021, pp. 406–423.

[6] Z. Tang, Y. Zhao, L. Yang, S. Qi, D. Fang, X. Chen, X. Gong, and Z. Wang, "Exploiting wireless received signal strength indicators to detect evil-twin attacks in smart homes," *Mobile Inf. Syst.*, vol. 2017, Jan. 2017, Art. no. 1248578, doi: 10.1155/2017/1248578.

[7] A. Alhasanat, B. Sharif, C. Tsimenidis, and J. Neasham, "Efficient RSS-based collaborative localisation in wireless sensor networks," *Int. J. Sensor Netw.*, vol. 22, no. 1, p. 27, 2016, doi: 10.1504/IJSNET.2016.079335.

[8] Wireshark. *About Wireshark*. Accessed: Feb. 1, 2021. [Online]. Available: https://www.wireshark.org/

[9] Y. Orzach. *Network Analysis Using Wireshark Cookbook*. Packt. Dec. 2013. [Online]. Available: https://www.packtpub.com/product/network-analysis-using-wireshark-cookbook/9781849517645

[10] Gitlab.com. *Wireshark Statistics*. Accessed: Mar. 1, 2021. [Online]. Available: https://gitlab.com/wireshark/wireshark/-/wikis/Statistics

[11] T. A. Myrvoll, J. E. Håkegård, T. Matsui, and F. Septier, ''Counting public transport passenger using WiFi signatures of mobile devices,'' in *Proc. IEEE 20th Int. Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2017, pp. 1–6, doi: 10.1109/ITSC.2017.8317687.

[12] T. Kusakabe, H. Yaginuma, and D. Fukuda, ''Estimation of bus passengers' waiting time at a coach terminal with Wi-Fi MAC addresses,'' *Transp. Res. Proc.*, vol. 32, pp. 62–68, Jan. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352146518301637

[13] L. Mikkelsen, R. Buchakchiev, T. Madsen, and H. P. Schwefel, ''Public transport occupancy estimation using WLAN probing,'' in *Proc. 8th Int. Workshop Resilient Netw. Design Modeling (RNDM)*, Sep. 2016, pp. 302–308, doi: 10.1109/RNDM.2016.7608302.

[14] L. Oliveira, J. Henrique, D. Schneider, J. de Souza, S. Rodriques, and W. Sherr, ''Sherlock: Capturing probe requests for automatic presence detection,'' in *Proc. IEEE 22nd Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2018, pp. 848–853, doi: 10.1109/CSCWD.2018.8465207.

[15] Y. Chon, S. Kim, S. Lee, D. Kim, Y. Kim, and H. Cha, ''Sensing WiFi packets in the air: Practicality and implications in urban mobility monitoring,'' in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, New York, NY, USA, Sep. 2014, pp. 189–200, doi: 10.1145/2632048.2636066.

[16] P. Fuxjaeger, S. Ruehrup, H. Weisgrab, and B. Rainer, ''Highway traffic flow measurement by passive monitoring of Wi-Fi signals,'' in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Nov. 2014, pp. 396–401, doi: 10.1109/ICCVE.2014.7297578.

[17] A. Di Luzio, A. Mei, and J. Stefa, ''Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests,'' in *Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2016, pp. 1–9, doi: 10.1109/INFOCOM.2016.7524459.

[18] Wigle. *Wireless Geographic Logging Engine: All the Networks. Found by Everyone*. Accessed: Apr. 1, 2021. [Online]. Available: https://www.Wigle.net

[19] A. Trivedi, C. Zakaria, R. Balan, A. Becker, G. Corey, and P. Shenoy, ''WiFiTrace: Network-based contact tracing for infectious diseases using passive WiFi sensing,'' *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 5, no. 1, pp. 1–26, Mar. 2021, doi: 10.1145/3448084.

[20] C. Zhang, X. Hei, and B. Bensaou, *A Measurement Study of Campus WiFi Networks Using WiFiTracer*. Cham, Switzerland: Springer, 2019, pp. 19–42, doi: 10.1007/978-3-319-92564-6_2.

[21] E. Vattapparamban, B. S. Çiftler, I. Güvenç, K. Akkaya, and A. Kadri, ''Indoor occupancy tracking in smart buildings using passive sniffing of probe requests,'' in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, May 2016, pp. 38–44, doi: 10.1109/ICCW.2016.7503761.

[22] K. Friess, ''Multichannel-sniffing-system for real-world analysing of Wi-Fi-packets,'' in *Proc. 10th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2018, pp. 358–364, doi: 10.1109/ICUFN.2018.8436715.

[23] F. Potortì, A. Crivello, M. Girolami, E. Traficante, and P. Barsocchi, ''Wi-Fi probes as digital crumbs for crowd localisation,'' in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Oct. 2016, pp. 1–8, doi: 10.1109/IPIN.2016.7743599.

[24] Github. (Sep. 2017). *The C-Based Firmware Patching Framework for Broadcom/Cypress WiFi Chips That Enables Monitor Mode*. [Online]. Available: https://github.com/seemoo-lab/nexmon

[25] Fogsense. (May 2015). *Cloud4wi Unveils the Industry's Smallest IoT WiFi Device*. [Online]. Available: https://cloud4wi.com/industrys-smallest-iot-wifi-device/

[26] C. F. Á. Salgado, L. E. P. Maestre, L. A. Noriega, and J. R. Castro, ''Distance aproximator using IEEE 802.11 received signal strength and fuzzy logic,'' in *Advances in Computational Intelligence*, I. Batyrshin and M. G. Mendoza, Eds. Berlin, Germany: Springer, 2013, pp. 411–420.

[27] H. Hong, C. Luo, and M. C. Chan, ''SocialProbe: Understanding social interaction through passive WiFi monitoring,'' in *Proc. 13rd Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, New York, NY, USA, Nov. 2016, pp. 94–103, doi: 10.1145/2994374.2994387.

[28] L. Oliveira, D. Schneider, J. De Souza, and W. Shen, ''Mobile device detection through WiFi probe request analysis,'' *IEEE Access*, vol. 7, pp. 98579–98588, 2019, doi: 10.1109/ACCESS.2019.2925406.

[29] M. W. Traunmueller, N. Johnson, A. Malik, and C. E. Kontokosta, ''Digital footprints: Using WiFi probe and locational data to analyze human mobility trajectories in cities,'' *Comput., Environ. Urban Syst.*, vol. 72, pp. 4–12, Nov. 2018, doi: 10.1016/j.compenvurbsys.2018.07.006.

[30] L. Sun, S. Chen, Z. Zheng, and L. Xu, ''Mobile device passive localization based on IEEE 802.11 probe request frames,'' *Mobile Inf. Syst.*, vol. 2017, Jan. 2017, Art. no. 7821585, doi: 10.1155/2017/7821585.

[31] Tcpdump. *Tcpdump*. Accessed: Feb. 1, 2021. [Online]. Available: https://www.tcpdump.org/

[32] *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks-Specific Requirements—Part 11: Wireless Lan Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2016 (IEEE Standard 802.11-2012), 2016, pp. 1–3534, doi: 10.1109/IEEESTD.2016.7786995.

[33] C. Godawita. *Channel Hopping Code for Linux*. Accessed: Mar. 1, 2021. [Online]. Available: https://gist.github.com/chinthakagodawita/5041eb0d8f1f68e9e23f

[34] C. Ansley. (2019) *MAC Randomization in Mobile Devices*. [Online]. Available: https://www.nctatechnicalpapers.com/Paper/2019/2019-mac-randomization-in-mobile-devices

**AJAY PRASAD** (Member, IEEE) received the M.Tech. and Ph.D. degrees in computer science and engineering. He is currently a Senior Associate Professor with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India. He has more than 21 years of experience in faculty positions at reputed institutions with substantial industrial exposure. He specializes in computer architecture, simulation and modeling, network/data security principles, system programming, cloud systems, compilers, and digital forensics. His research contribution is toward fine-grained centralized monitoring in cloud computing and many allied areas of security and others. His research interests include the area of security and digital forensics and security issues in the IoT. He has authored many research papers including a book on *Digital Forensics* and several book chapters. He is a continuous contributor toward society through cyber-awareness lectures and seminars to people and the Government agencies like the Uttrakhand Police Department, India. He is a Life Member of IETE, ISTE, and other prominent bodies in India. He has contributed to several different MOOC courses at the national level. He is a Section Editor of the prestigious journal, *Space and Culture, India* (SACI). He has been guiding doctoral scholars working in the areas like security in SCADA systems, IEE802.11a-e, automated video surveillance, human aura, energy bio-field, and the IoT.

**SOURABH SINGH VERMA** (Senior Member, IEEE) received the M.Tech. degree in CSE and the Ph.D. degree in CSE. He has more than 17 years of experience as an academician serving for reputed institutions in India. His research areas include machine learning, networking protocols, the IoT security, and human–computer interactions. He is currently working as an Assistant Professor with the School of Computing and IT, Manipal University Jaipur. He is guiding Ph.D. scholars under research opportunities like vehicular ad hoc networks, image processing, disease diagnosis and prognosis, and the IoT securities models. He authored various research articles in reputed international journals and international conferences. He also has a various intellectual property right (IPR) under his name that includes copyrights and patents. He is a Senior Member of the ISTE. He has served as an editor to edited authored books and also as a reviewer for various international journals and conferences. He is a continuous contributor to knowledge sharing platforms and has given various invited talks and guest lectures at the Faculty Development Programs (FDP), conferences, and workshops for reputed organizations. He was also honored as the Best Young Researcher (Male) by Global Education and Corporate Leadership Awards (GECL), India, in 2018.

**PRIYANKA DAHIYA** received the master's degree in computer science and engineering from the Sikkim Manipal Institute of Technology, Sikkim, India, and the Ph.D. degree from Manipal University Jaipur, Rajasthan, India. She joined the School of Computing, Dehradun Institute of Technology, as an Assistant Professor, in August 2018. She is having more than ten years of experience in the organization, like Manipal University Jaipur and Mody University. She has published various patents, research papers, and invited as the session chair for reputed conferences. Her current research interests include data mining, deep learning, intrusion detection, cryptography, and big data. She is certified as the Publons Academy Supervisor.

**ANIL KUMAR** (Senior Member, IEEE) received the M.Tech. degree from the Delhi College of Engineering, New Delhi, and the Ph.D. degree from Manipal University. He is currently working as a Professor of computer science and engineering, an Accreditation Coordinator, and the Head of Data Science Research Group at DIT University, India. He has more than 25 years of teaching and industrial experience. He served various reputed origination, like Manipal University, Bharti Vidyapeeth, Mody University Science and Technology, and DRDO. He has guided over ten research scholars. He has published more than 200 research articles and patents. He has organized various international/national conferences/workshop. His research interests include image processing algorithm, cryptography, artificial intelligence, signals and systems, neural networks, genetic algorithm, and machine learning. He has done various Indian government projects as a Principal Investigator. He is a Senior Member of ACM and CSI; also worked as an Executive Committee Member of the IEEE Computer Society India Council, in 2015 and 2016, and the IEEE Rajasthan Sub-Section, in 2018. He has also been a consultant to various industries. He is a reviewer of many international journals of IEEE, Elsevier, Springer, and ACM.