Comparative Analysis of Single- and Multi-Interface Super-Sniffers in Wi-Fi Passive Monitoring

Mohammad Imran Syed, Anne Fladenmuller, Marcelo Dias de Amorim

Comparative Analysis of Single- and Multi-Interface Super-Sniffers in Wi-Fi Passive Monitoring

Mohammad Imran Syed, Anne Fladenmuller, and Marcelo Dias de Amorim
Sorbonne Université, CNRS, LIP6, Paris, France
{mohammad-imran.syed, anne.fladenmuller, marcelo.amorim}@lip6.fr

***Abstract*—Passive packet sniffing is a simple and low-cost method to collect Wi-Fi data in a specific geographic area. Nevertheless, sniffers may not capture all the Wi-Fi packets due to inherent characteristics of wireless communications, leading to incomplete data traces. We explore the idea of *absolute completeness* for Wi-Fi passive data capture and validate our findings with indoor and outdoor experimental measurements. We collect Wi-Fi data traces using a controlled source node and multiple sniffers about two meters from the source. We find that individual sniffers have limited capability to capture the traffic and that combining traces from different sniffers improves significantly the data completeness. Deploying redundant, co-located sniffers enhances the completeness but comes at a financial cost. We compare two ways of achieving redundancy: using multiple individual sniffers or using one sniffer with multiple Wi-Fi interfaces. Our experiments show that both ways have similar completeness levels and that we can achieve redundancy with lower cost by using one sniffer with various Wi-Fi interfaces.**

***Index Terms*—wireless, passive measurements, completeness**

I. Introduction

The pervasiveness of wireless networks has underscored the need for comprehensive understanding of their behavior to optimize their performance [1, 2, 3, 4]. However, analyzing wireless traffic poses inherent challenges due to the dynamic nature of wireless links [5]. Active traffic collection, involving probe deployment across multiple nodes, often proves cumbersome and may yield inadequate data due to user inconvenience or limited sampling.

Passive sniffing emerges as an efficient alternative, utilizing multiple *sniffers* (devices configured to capture wireless packets) strategically positioned across the target area [6, 7, 8]. This approach offers cost-effectiveness, scalability, and user privacy while providing valuable insights into network behavior.

The ANR Mitik project [9], which we contribute to, aims to infer contact traces through passive sniffing. However, single sniffers may not capture all transmitted packets due to wireless constraints, leading to incomplete traces. To address this limitation, we rely on *super-sniffers*, which combines multiple individual sniffers to increase the probability of capturing at least one packet for each transmitted frame. Our previous research demonstrated the effectiveness of super-sniffers in improving trace quality [10, 11, 12] using Raspberry Pi-based sniffers equipped with single Wi-Fi interfaces.

One question remains open, though. Deploying super-sniffers implies multiplying hardware, which increases cost. If the target area is big, the cost may be an issue. In this paper, *we investigate whether a single Raspberry Pi node with multiple Wi-Fi interfaces can achieve comparable results to multiple single-interface sniffers*, considering both performance and cost implications.

We use *absolute completeness* as a metric to assess trace completeness and evaluate it through real-world experiments. We measure the capture quality of individual and super-sniffers with redundancy levels of up to three (i.e., three co-located individual sniffers whose captures are combined as if they were a single node). The sniffers used in our experiments are based on Raspberry Pi 4B (RPi4 hereafter). We consider two distinct scenarios: dense (indoors) and sparse (outdoors) traffic environments[1]. The experimental findings indicate that both single- and multi-interface Raspberry Pi setups yield similar trace completeness levels. However, the multi-interface Raspberry Pi setup offers reduced hardware costs and simplified deployment, making it a more cost-effective and practical solution. In essence, the use of a single Raspberry Pi node with multiple Wi-Fi interfaces emerges as a viable alternative to multiple single-interface sniffers for passive wireless traffic capture, offering comparable performance and significant cost savings.

In summary, the contributions of this paper are:

- **Cost assessment.** Multiple single-interface sniffers improve the quality of traces captured but it comes at a financial cost. We do the evaluation of traces captured by single- and multi-interface sniffers simultaneously. It allows us to highlight that we achieve similar results with a multi-interface sniffer which decreases the number of hardware devices, resulting in a low financial cost.
- **Controlled experimental evaluation.** We adopt an experimental approach to assess the behavior of the completeness metric under various network conditions. We conduct experiments in scenarios where the traffic is known and controlled, allowing us to obtain an absolute measure of completeness, even though such setups may only apply to specific situations.
- **Environment dependence.** We demonstrate that the results are not influenced by hardware, but by the specific environment or scenario.

The remainder of this paper is organized as follows. In Section II, we outline our experimental methodology. In Section III, we define *absolute completeness* in passive measurements, while in Section IV we provide empirical evidence

[1]The dense environment observes ten times more traffic than the sparse environment [10].

supporting the need for redundancy when passively sniffing traffic. In Section V, we evaluate redundancy for sniffers with single and multiple Wi-Fi interfaces. We discuss related work in Section VI and conclude the paper, while identifying open research questions, in Section VII.

II. Sniffing Wi-Fi packets

In this section, we detail the experiments we run to collect Wi-Fi traces through passive measurements.

A. Composing a sniffer

As mentioned in Section I, we base our sniffers on RPi4 nodes. We have five RPi4 nodes in our measurement set-up [13]. We have four RPi4 nodes as sniffers, three with a single Wi-Fi interface, and one with three Wi-Fi interfaces.[2] We use one RPi4 node as a controlled source node to generate Wi-Fi traffic. All the nodes are set to channel 1 of the 2.4 GHz band. We use an external Wi-Fi adapter, Alfa AWUS051NH [14]. The advantage of this specific external Wi-Fi adapter is that it accepts to run in monitor mode. The monitor mode is a radio mode that makes it possible for the Wi-Fi card to listen to all Wi-Fi traffic in the wireless medium passively.

B. Trace collection and processing

Trace generation. We use `scapy` [15] at the sender node to generate Wi-Fi traffic. The average sending rate is 10 packets per second. This is the maximum possible sending rate to be able to differentiate the packets at the sniffers using sequence numbers.

Trace capture. Sniffers run `tcpdump` to collect traces [16]. We configure some filters to gather only the data generated by the source node, this allows us to not worry about any privacy issues. The outcome of the capture process is one `pcap` file per individual sniffer, whereas one file per interface for sniffer with multiple Wi-Fi interfaces.

Synchronization of reference frames and traces. The *beacon* and *probe response* frames are the closest representatives of real-time clocks. These frames lay the foundation for the synchronization process. We use `PyPal` as the tool to synchronize and merge traces [17]. It synchronizes two traces at a time. Therefore, a reference trace and the trace which has to be synchronized form the input to the tool. The first step is to extract the beacon and non-re-transmitted probe response frames from both traces independently. These frames are called *unique frames*. The next step is to extract the unique frames that are common in both traces. The coverage areas of the sniffers capturing these traces must overlap to execute this step. The common frames are referred to as *reference frames*. Next, the timestamps of reference frames are synchronized using *linear regression* over a sliding window of three frames.

[2]Although, a RPi4 node has four USB ports, it can support a maximum of three Wi-Fi interfaces for the purpose of sniffing. We tried to do the experimentation with four Wi-Fi adapters connected to a single RPi4 node but it did not work.

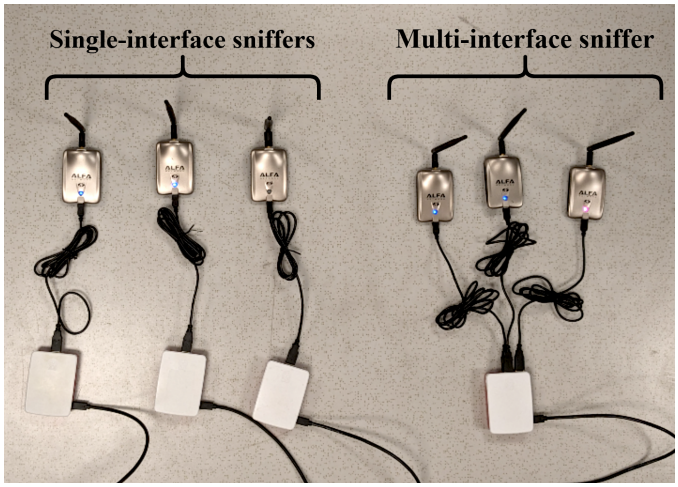


Fig. 1: Experimental setup. 3 RPi4 nodes with one Alfa AWUS051NH adapter each and 1 RPi4 node with three Alfa AWUS051NH adapters.

The synchronized reference frames are then used to synchronize the complete trace. The tool provides an additional option of concatenating or merging the synchronized traces.

Trace merging. The principle behind a super-sniffer is its ability to merge traces collected by its individual sniffers. The merging process requires that input traces be synchronized so that a packet that appears in multiple individual traces is identified unambiguously. `PyPal` also performs such an operation.

C. Experimental set-up

There is no guarantee that a single sniffer can capture 100% of the traffic because of losses due to inherent characteristics of the wireless medium. We choose sparse and dense traffic scenarios because of different traffic loads [10] and run experiments indoors and outdoors for both scenarios to examine the traces collected by the individual sniffers. We place a stationary source node at a distance of two meters from the sniffers for these experiments. We run each test 10 times in the target scenarios to rule out anomalies. Each test lasts five minutes, and the sniffers remain stationary for the whole capture period. Figure 1 shows our experimental setup in an indoors environment.

III. Absolute Completeness

The effectiveness of a passive measurement system is enhanced with an increase in the redundancy level of a super-sniffer. The redundancy level of the super-sniffer is determined by the number of co-located sniffers. However, as discussed previously, the augmentation of sniffers within a super-sniffer incurs financial costs. As depicted in Figure 2, illustrating a typical sniffing scenario, it is possible to acquire the complete trace only through the combination of all three sniffers s_1, s_2, and s_3 in the case of single-interface sniffers. Similarly, for the multi-interface sniffer S, we get the complete trace only by the combination of all three interfaces.

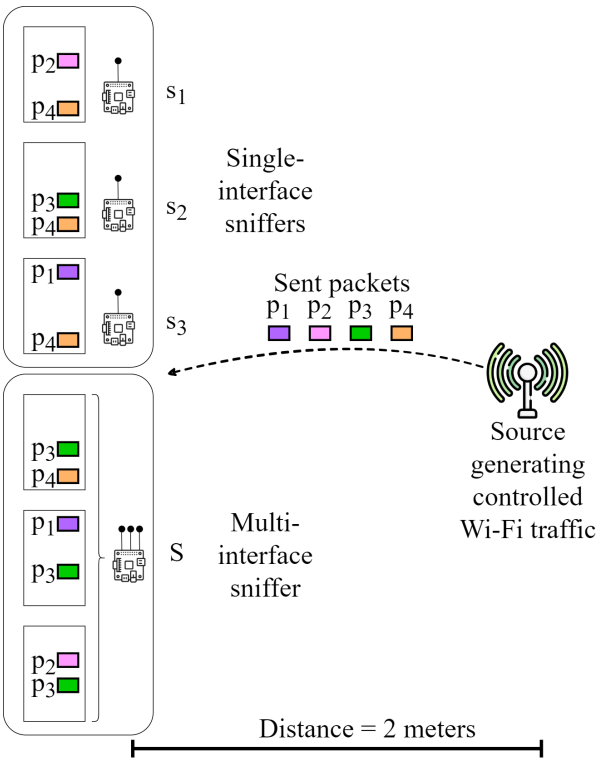


Fig. 2: Trace completeness. Single-interface sniffers represent multiple sniffers each having a single Wi-Fi interface, whereas, multi-interface sniffer indicates a single sniffer with multiple Wi-Fi interfaces. Because of the nature of the wireless medium, sniffers miss some packets. We need to combine individual traces to get as close as possible to the complete trace. In this paper, we investigate the impact of distance on such a sniffing strategy.

To address this, we rely on the concept of *absolute completeness*, which quantifies the proportion of packets captured by a sniffer in relation to the maximum number of packets transmitted by a controlled source node. This analysis is essential for comprehending the constraints of a passive measurement system. We articulate the term *absolute completeness* to denote the comprehensive nature of the trace in relation to controlled source traffic. This definition is valuable not only for understanding system limitations but also for situations where evaluating wireless network coverage is necessary without deploying expensive measurement devices. In such cases, the target traffic is predetermined. Algorithm 1 provides our algorithm for the measurement of absolute completeness.

Algorithm 1 Completeness for a super-sniffer of size m

Input:

Set of sniffers $S = \{s_1, s_2, \ldots, s_M\}$ where M is the number of sniffers.

Traces captured by each sniffer T_{s_i} for $s_i \in S$.

Set of all traces $\mathcal{T} = \{T_{s_1}, T_{s_2}, \ldots, T_{s_M}\}$.

Generate Combinations:

Define $\pi_{\cdot}^{m}$ as a subset of m elements of $\mathcal{T}$.

Define Π^m as the set of all instances of different combinations of $\pi_{\cdot}^{m}$:
$\Pi^m = \{\pi_1^m, \pi_2^m, \ldots, \pi_{\binom{M}{m}}^m\} = \{X = \{x_1, x_2, \ldots, x_m\}, x_1, x_2, \ldots, x_m \in \mathcal{T}, x_1 \neq x_2 \neq \ldots \neq x_m\}$

Outcome Trace:

Define the outcome trace $A^{\pi_i^m}$ as the union of the traces $\pi_i^m \in \Pi^m$:

$A^{\pi_i^m} = T_a \cup T_b \cup \ldots \cup T_m, \quad T_a, T_b, \ldots, T_m \in \pi_i^m$, where $T_a \neq T_b \neq \ldots \neq T_m$.

Completeness:

Let A_{total} be the set of packets that actually circulated in the network at the time of capture.

Calculate the absolute completeness $C(A^{\pi_i^m})$ as:
$C(A^{\pi_i^m}) = \frac{|A^{\pi_i^m}|}{|A_{\text{total}}|}$.

IV. One sniffer is not enough

In this section, we present an analysis of the absolute completeness per individual sniffer and experimental evidence for the need for super-sniffers. Table I presents the average absolute completeness of each single- and multi-interface sniffer trace for both the sparse and dense traffic scenarios.

Sparse traffic environment. We observe that with a low traffic load in the sparse traffic environment [10], the average absolute completeness is high. We see in Table I that the average absolute completeness for indoors testing is in the high nineties in indoors environment, whereas it falls below 90% in the worst case in outdoors environment. The completeness values are:

- Indoors environment
  - 99% for both single- and multi-interface sniffers in the best case.
  - 96% and 95% for single- and multi-interface sniffers respectively in the worst case.
- Outdoors environment
  - 94% and 92% for single- and multi-interface sniffers respectively in the best case.
  - 89% and 85% for single- and multi-interface sniffers respectively in the worst case.

Dense traffic environment. In the case of the dense traffic scenario where we have heavy traffic presence in the medium, the completeness falls below 80% for the indoors environment, whereas it is below 70% for outdoors testing. The completeness values are as follows:

- Indoors environment
  - 78% and 79% for single- and multi-interface sniffers respectively in the best case.
  - 77% and 75% for single- and multi-interface sniffers respectively in the worst case.
- Outdoors environment
  - 68% for both single- and multi-interface sniffers in the best case.
  - 67% for both single- and multi-interface sniffers in the worst case.

We observe that the values of absolute individual completeness achieved by single- and multi-interface sniffers are

TABLE I: Average absolute completeness of sniffers with multiple and single interfaces.

	Sparse traffic area				Dense traffic area			
	Multi-interface sniffer		Single-interface sniffers		Multi-interface sniffer		Single-interface sniffers	
	Best	Worst	Best	Worst	Best	Worst	Best	Worst
Indoors	99	95	99	96	79	75	78	77
Outdoors	92	85	94	89	68	67	68	67

comparable. Even though the individual performance is similar, there is still a room for improvement in the quality of traces, particularly in the dense traffic environment. In the next section, we implement the concept of trace completeness as a function of redundancy and study its impact on the level of improvement in the quality of the traces.

V. Super-sniffer: single- vs multi-interface

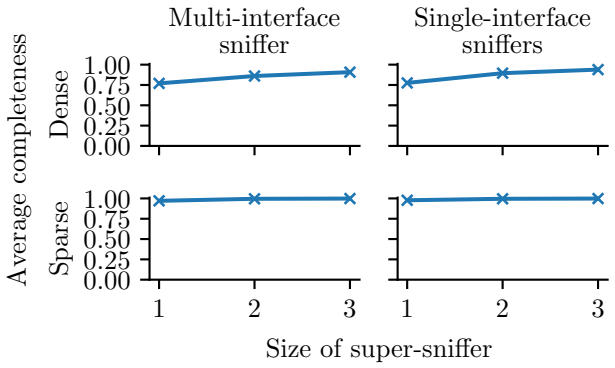
We investigate the importance of grouping individual sniffers to build a super-sniffer. Firstly, we present the impact of all combinations of $m = \{1, 2, 3\}$ sniffers on trace completeness. Secondly, we compare the results for single- and multi-interface sniffers.

Figure 3 shows the average completeness for all combinations of m sniffers. The x-axis represents the size m of the super-sniffer, while the y-axis gives the completeness for a combination of up to three sniffers or interfaces for indoors and outdoors testing in both the sparse and dense traffic scenarios.

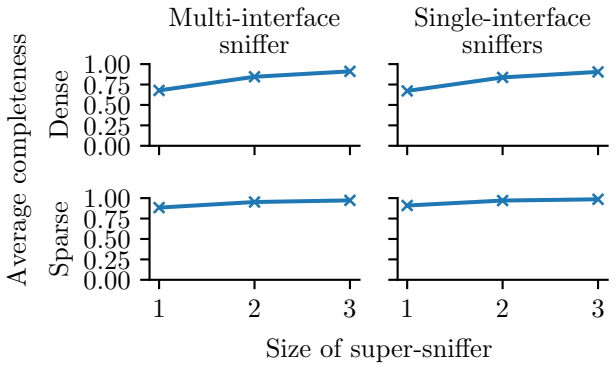
When m equals 1, the completeness values are identical to the ones given in Table I. It is interesting to note that, the completeness keeps increasing as the size of the super-sniffers grows. The level of increase is similar for sniffers for based on both multiple and single Wi-Fi interfaces. We obtain the maximum completeness for the super-sniffer of maximum size, i.e., $m = 3$. This means a super-sniffer always benefits from combining an extra sniffer.

We notice in Figure 3a that the completeness achieved by the use of either single- or multi-interface sniffers in an indoors environment is of a similar level. The completeness of the individual sniffers is comparatively lower in the dense traffic scenario. We see a similar trend of single- and multi-interface sniffers achieving a similar completeness level in an outdoors scenario in Figure 3b. The individual sniffers, however, attain a lower level of completeness in an outdoors environment as compared to an indoors environment. As we keep increasing m, we notice an improvement in completeness for each incremental value. We achieve the desired results using a single multi-interface sniffer, which helps us reduce the cost of a super-sniffer because we need less hardware in this case.

Discussion. The use of more number of hardware devices (RPi4 in our case) increases the financial cost of building a super-sniffer for the improvement of traces captured in passive measurements. To build a super-sniffer of size three with the help of three single-interface sniffers, we need three RPi4 nodes, three Alfa AWUS051NH Wi-Fi adapters, and three power-banks powerful enough to power the RPi4 nodes. If we use a single multi-interface sniffer to build a super-sniffer of size three, we would bring the cost down by about 55% (with



(a) Indoors.



(b) Outdoors.

Fig. 3: Average absolute completeness of each super-sniffer, aggregating m single-interface sniffers and m interfaces in the case of a multi-interface sniffer. The results are for both indoors and outdoors testing in the dense and sparse traffic scenarios.

the costs of the market at the time of the writing of the paper). The more redundancy we introduce in the super-sniffer, the bigger the savings. We, therefore, achieve the desired results at reduced cost, without any compromise in the quality of results.

VI. Related Work

Xu et al. merge the individual traces into a single and then run an inference procedure to reconstruct the missing packets [18]. It needs at least one packet of a conversation in a trace to infer the missing packets, and its accuracy also depends on the capture percentage. The evaluation is dependent on a simulation where the process removes packets from the trace randomly whereas, we keep the packet with

the best RSSI value. Wit is a tool to merge multiple traces and then reconstruct the missing packets by inferring if they were received by the destination by making use of frames like Association Request and Response [7]. PMSW is a passive monitoring system that relies on sequence numbers to infer the missing packets in a wireless sensor network. However, it only captures data and acknowledgment packets, leading to a complex synchronization solution [19]. There is no conversation, data, or association frames as we rely on probe requests for the purpose of contact traces. Sammarco et al. rank the traces collected from multiple sniffers based on similarity to determine which traces should be merged to achieve maximum completeness. It decreases the number of merge operations [20].

Schulman et al. estimate the number of missed packets using sequence numbers and re-transmission bit [21] but rely on CRAWDAD (now part of IEEE DataPort) [22] datasets. LiveNet provides a platform for monitoring and processing passive traces, but the transfer of packets to the serial port seems to result in packet loss and the validation is also based on the data measured in a controlled environment [23]. Our work stands distinctive as we focus on redundancy for trace completeness based on real-world experiments with a controlled source node in an uncontrolled environment and do an exhaustive analysis for different scenarios. Moreover, our solution is more oriented towards contact traces.

VII. Conclusion

In this paper, we evaluate two different ways of composition of a super-sniffer. Our analysis centers on traces concurrently captured by multiple single-interface sniffers and a single multi-interface sniffer. Our findings reveal that the enhancement of trace quality achieved through a single multi-interface sniffer is equivalent to that of multiple single-interface sniffers in the context of passive measurements. At the same time, we are able to reduce the financial cost of the constitution of a super-sniffer by a significant amount.

VIII. Acknowledgment

This work has been partially funded by the ANR Mitik project, French National Research Agency (ANR), PRC AAPG2019.

References

[1] A. Galanopoulos, V. Valls, G. Iosifidis, and D. J. Leith, "Measurement-driven analysis of an edge-assisted object recognition system," in *IEEE ICC*, 2020.

[2] W. Zhou, Z. Wang, and W. Zhu, "Mining urban WiFi QoS factors: A data driven approach," in *IEEE BigMM*, 2017.

[3] P. De Vaere, T. Bühler, M. Kühlewind, and B. Trammell, "Three bits suffice: Explicit support for passive measurement of internet latency in QUIC and TCP," in *Internet Measurement Conference*, New York, NY, USA, 2018.

[4] J. Wang, Y. Zheng, Y. Ni, C. Xu, F. Qian, W. Li, W. Jiang, Y. Cheng, Z. Cheng, Y. Li, X. Xie, Y. Sun, and Z. Wang, "An active-passive measurement study of TCP performance over LTE on high-speed rails," in *ACM Mobicom*, New York, NY, USA, 2019.

[5] M. D. Corner, B. N. Levine, O. Ismail, and A. Upreti, "Advertising-based measurement: A platform of 7 billion mobile devices," in *ACM Mobicom*, Snowbird, UT, USA, Oct 2010.

[6] F. Garcia, R. Andrade, C. De Oliveira, and J. Souza, "EPMOSt: And energy-efficient passive monitoring system for wireless sensor networks," *Sensors (Basel, Switzerland)*, vol. 14, pp. 10 804–10 828, 06 2014.

[7] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Analyzing the MAC-level behavior of wireless networks in the wild," in *Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. New York, NY, USA: Association for Computing Machinery, 2006.

[8] Y.-C. Cheng, J. Bellardo, P. Benkö, A. C. Snoeren, G. M. Voelker, and S. Savage, "Jigsaw: Solving the puzzle of enterprise 802.11 analysis," in *Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*. New York, NY, USA: Association for Computing Machinery, 2006.

[9] "ANR MITIK," https://project.inria.fr/mitik/.

[10] M. I. Syed, A. Fladenmuller, and M. Dias De Amorim, "Assessing the completeness of passive wi-fi traffic capture," in *2022 International Wireless Communications and Mobile Computing (IWCMC)*, 2022, pp. 961–966.

[11] M. I. Syed, A. Fladenmuller, and M. Dias de Amorim, "How much can Sniffer Redundancy Improve Wi-Fi Traffic?" in *2022 IEEE 95th Vehicular Technology Conference: VTC2022-Spring*, Helsinki, Finland, Jun. 2022.

[12] M. I. Syed, A. Fladenmuller, and M. Dias de Amorim, "Unity is strength: Improving wi-fi passive measurements through sniffer redundancy," *Ad Hoc Networks*, vol. 151, p. 103287, 2023.

[13] "Raspberry Pi 4 model B," https://tinyurl.com/2p89uund.

[14] "AWUS051NH Wi-Fi adapter," https://tinyurl.com/yk8vk3vz.

[15] P. Biondi, "Scapy," https://scapy.net/.

[16] The Tcpdump Group, "Tcpdump and libpcap," https://tcpdump.org.

[17] M. I. Syed, A. Flandenmuller, and M. Dias De Amorim, "PyPal: Wi-Fi Trace Synchronization and Merging Python Tool," LIP6 UMR 7606, UPMC Sorbonne Université, France, Technical Report, Mar. 2022. [Online]. Available: https://hal.archives-ouvertes.fr/hal-03618014

[18] X. Xu, C. Tong, and J. Wan, "Improve the completeness of passive monitoring trace in wireless sensor network," in *2010 Asia-Pacific Services Computing Conference (APSCC 2010)*. Los Alamitos, CA, USA: IEEE Computer Society, Dec 2010.

[19] X. Xu, J. Wan, W. Zhang, C. Tong, and C. Wu, "PMSW: A passive monitoring system in wireless sensor networks," *International Journal of Network Management*, 2011.

[20] M. Sammarco, M. E. M. Campista, and M. D. de Amorim, "Trace selection for improved wlan monitoring," in *Proceedings of the 5th ACM Workshop on HotPlanet*. New York, NY, USA: Association for Computing Machinery, 2013.

[21] A. Schulman, D. Levin, and N. Spring, "On the fidelity of 802.11 packet traces," in *Proceedings of the 9th International Conference on Passive and Active Network Measurement*. Berlin, Heidelberg: Springer-Verlag, 2008.

[22] C. team, "Crawdad," https://ieee-dataport.org/collections/crawdad.

[23] B.-r. Chen, G. Peterson, G. Mainland, and M. Welsh, "LiveNet: Using passive monitoring to reconstruct sensor network dynamics," in *Distributed Computing in Sensor Systems*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.