REVEAL: Real-time Evaluation and Verification of External Adversarial Links

Alexander Marder[1], Jon Larrea[2], kc claffy[3], Erik Kline[4], Kyle Jamieson[5],
Bradley Huffaker[3], Lincoln Thurlow[4], and Matthew Luckie[3]
[1]Johns Hopkins University, amarder@jhu.edu
[2]Revelare Networks, jon@revelarenet.com
[3]UCSD CAIDA, kc@caida.org, bradley@caida.org, mjl@caida.org
[4]USC/ISI, kline@isi.edu, lincoln@isi.edu
[5]Princeton University, kylej@cs.princeton.edu

***Abstract*—Department of Defense (DOD) use of commercial networks entails unprecedented reliance on untrusted third-party communications infrastructure, and the associated risk of exposing DOD communications to an adversary. Traversing adversary-controlled infrastructure allows DOD's adversaries to recognize, disrupt, or extract intelligence even from encrypted communications. The resulting arms race of obfuscation vs intelligence techniques has an inherent limitation: with each new obfuscation, DOD can never know if it fools the adversary, or if the adversary is simply lulling DOD into a false sense of security.**

We believe the next great capability leap for operating through commercial networks will likely come from sophisticated analytics that provide situational awareness of the threats within the communications infrastructure, and implementations that dynamically route communications along benign paths. These systems will restructure communication paths to avoid adversary-controlled infrastructure within the cellular networks and the broader Internet, adding depth to existing DOD defenses and keeping communications unobservable by the adversary.

In this paper, we describe our vision for this emerging conceptual framework. We first describe the threat model for DOD communications and use cases that motivate our approach. We then discuss specific threats for each component of the cellular communication infrastructure—–radio access network, mobile core, and Internet—–and our vision for securing communications against those threats. For the radio access network and Internet components, we also describe proofs-of-concept for our proposed approaches, demonstrating their feasibility.

***Index Terms*—mobile, wireless, security, 5G, emerging concepts**

I. Introduction

The near ubiquity of commercial wireless networks, and their continual advances in capabilities and coverage, present an opportunity to transform DOD mission-critical operations. These networks, now the most prevalent enabler of instantaneous communications to the entire Internet, offer DOD the compelling opportunity to leverage pervasive global infrastructure designed to withstand power outages and weather events, but for which someone else finances deployment, maintenance, and upgrades.

However, taking full advantage of this opportunity requires novel techniques to safely operate through non-cooperative commercial networks worldwide. DOD's use of commercial wireless infrastructure entails unprecedented reliance on untrusted third-party communications infrastructure (Figure 1), including the cellular base stations that connect the radio access network to user devices, the mobile core, and the Internet infrastructure that underlies wireless communications. The DOD is well aware this infrastructure is not always trustworthy. Our adversaries possess a vast array of sophisticated and complex communications intelligence capabilities they can easily turn against DOD assets. For example, the U.S. government recently disclosed its belief that base station vendors Huawei and ZTE have intentionally placed backdoors in their base stations at the behest of Chinese intelligence [1].

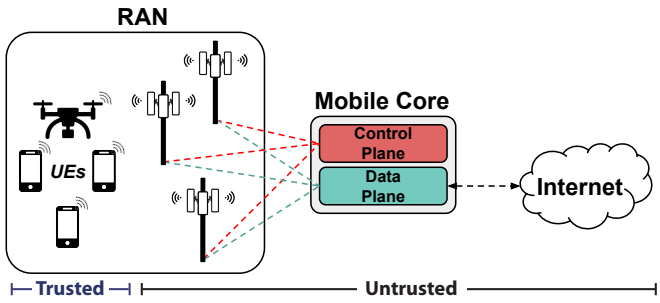

Fig. 1. User equipment (UEs) in cellular networks connect wirelessly to base stations in the radio access network (RAN). The base stations tunnel traffic to the mobile core, which authenticates users and forwards packets into the global Internet. All of these three components—base stations, mobile core, and Internet infrastructure—pose risks for DOD communications.

The core problem when operating through non-cooperative commercial infrastructure is that the *unknown* infrastructure potentially exposes communications to an adversary. When communications traverse adversary-controlled infrastructure, it allows DOD's sophisticated adversaries to recognize, disrupt, or extract intelligence from the communications. Even encrypted communications reveal the communicating source and destination IP addresses, and remain vulnerable to advanced analysis techniques able to extract information directly from the encrypted payload. Adversaries can also employ post-quantum store-and-decrypt attacks, where they record DOD communications traversing infrastructure they control with the

Funded in part by NSF ITE-2326928.

intent of decrypting with future quantum computers.

A natural response to the powerful threats posed by the *unknown* communication infrastructure is to disguise traffic in hopes of evading adversary detection. Such disguises create an arms race with ever more sophisticated disguises and advanced network intelligence techniques to detect them. We already know that our adversaries expend great resources to combat traffic obfuscation, with the well-publicized ability to detect nearly all of the most sophisticated disguises used today; e.g., application mimicry [2], Shadowsocks [3], commercial VPN offerings [4], and Tor with its pluggable transports [4]. This problem with this approach is that with each new obfuscation attempt, DOD will never know if the disguise fools the adversary or if the adversary is simply lulling them into a false sense of security. Worse still, once an adversary learns DOD's obfuscation approaches, the disguises themselves can unintentionally draw unwanted attention from that adversary. Fundamentally, traffic obfuscation cannot provide meaningful security guarantees when the underlying infrastructure is an unknowable black box.

But communications infrastructure is not *unknowable*. We believe that the next great capability leap for operating through commercial wireless networks should not come from trickier disguises, but from systems that combine sophisticated analytics to identify threats *within* the communications infrastructure, with techniques that dynamically route communications along benign paths. These systems will restructure communication paths to avoid adversary-controlled base stations, networks, and territory, adding depth to existing DOD defenses and keeping communications unobservable by the adversary.

In this paper we describe our vision for this emerging conceptual framework. §II describes the threat model for DOD communications, and use cases that motivate our approach. Then, discuss specific threats for each component of cellular communication infrastructure—RAN (§III), mobile core (§IV), and Internet (§V)—and our vision for securing communications against those threats. For the RAN and Internet components, we also describe proofs-of-concept for our proposed approaches, demonstrating their feasibility.

II. Threat Model and Use Cases

DOD plans for the most sophisticated attackers in the world, including nation-state adversaries. We envision an attacker capable of intercepting, disrupting, modifying, or recording for later decryption any communication that traverses infrastructure controlled—or able to be controlled—by the attacker. Based on our threat model, and discussions with DOD personnel, we motivate our discussion with three high-impact DOD use cases that illustrate the benefit of leveraging commercial wireless networks and the need for robust defense against communication subversion.

Wireless DOD Sensors: Cellular infrastructure is highly attractive for wireless sensors due to its low latency, high throughput, and low power consumption. However, an adversary controlling network infrastructure might recognize a sensor that communicates with known DOD devices or address space, or that sends conspicuous traffic due to obfuscation attempts. Once identified, a sensor's communication is at the mercy of the adversary, who can disrupt the communication at a critical moment.

Protection of Service Members in Foreign Territories: When ships arrive at overseas ports of call or when service members take liberty in other countries, the service members' phones will connect to the local cellular networks. Adversaries could gain insight into DOD operations by tracking device movements across cell towers, tracking troop movements, or capturing plaintext communications like phone calls or text messages. The adversary would likely recognize any obfuscation-based approaches, since the network would be flooded with unusual traffic soon after a ship docked or when typical weekend liberty commences.

Covert Communications for Clandestine Operatives: Covert DOD operatives must ensure that their communications do not reveal their presence or allow an adversary to identify them. Most obviously, network traffic to DOD or known DOD devices likely reveals the presence of a DOD operative, putting critical missions in jeopardy. Intelligent adversaries may even be able to detect sophisticated obfuscation methods based on observing traffic on the adversary's infrastructure. Once detected, the adversary can likely physically locate the operatives, creating threats to the operatives themselves.

III. Threats in the Radio Access Network (RAN)

In cellular networks, the radio access network (RAN) is responsible for providing wireless access to users. The main components of the RAN are the base stations that mediate access to the shared wireless channel and ensure that user equipment (UEs) do not interfere with each other or the base station's associated cell. Due to a combination of signal propagation and timing constraints, operators deploy the base stations close to users at the edge of the wireless network.

A. Threats: Eavesdropping and Surveillance

Adversaries can compromise DOD communications in the RAN in two ways: exploiting backdoors in legitimate carrier base stations, or deploying surveillance equipment.

1) Exploiting Backdoors: A critical concern in the RAN is the potential for adversaries to place backdoors in 4G and 5G base stations made by certain vendors [1]. These backdoors are intentional, long-lived, and provide adversaries with the ability to monitor, modify, and exfiltrate traffic for offline analysis and future operations. The U.S. government released strong unclassified evidence that the Chinese base station vendors Huawei and ZTE—comprising 1/3 of the global base station market—have compromised supply chains [5]. This backdoor access could potentially allow our adversaries to eavesdrop on communications worldwide.

2) Surveillance Equipment: Surveillance base stations, which exploit the openness of the wireless channel, can take several forms. The most common type is an International Mobile Subscriber Identity (IMSI) catcher, which tricks UEs into connecting long enough to record identifiers tied to the

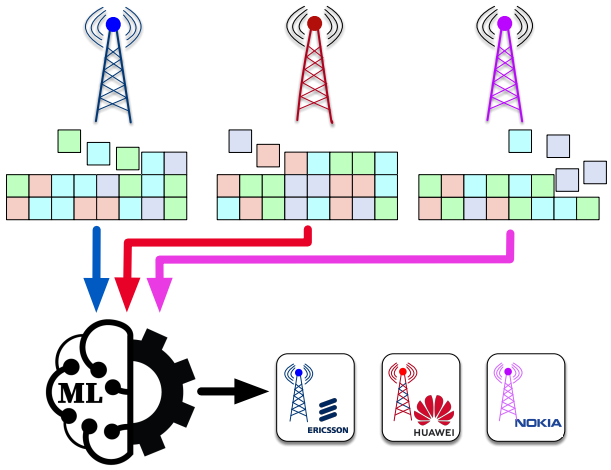

Fig. 2. Classifiers can use decoded RRC and MAC layer information to classify LTE and 5G base stations.

subscriber or device. IMSI catchers could be used to tie service members to devices or learn patterns of life. A more sophisticated attack could attempt to authenticate subscribers and trick UEs into transmitting data across the surveillance base station.

B. Current Behavior: Connect Opportunistically

Modern UEs select RAN infrastructure based on a combination of human preference and signal quality. Users install a carrier's SIM card and the phone will generally attempt to connect to whichever base station it can reach with the highest signal quality. After attaching, the carrier might instruct or nudge a UE to connect to a different cell. If a UE is equipped with multiple SIM cards, the user is expected to manually select the active carrier.

This operating mode leaves users susceptible to eavesdropping through base stations with backdoors and surveillance equipment. Users cannot distinguish the base station vendors used by different carriers, so selecting the carrier with benign base stations is impossible. Even if users had some insight into the base station vendors, carriers often use different vendors in different regions, so achieving protection would require users to manually switch SIM cards as they travel. Similarly, modems and phone operating systems cannot distinguish one base station vendor from another, or surveillance equipment from legitimate base stations.

C. Proposed Approach: Classify Vendors Based on Behavior

3GPP specifies much of the base station behavior to ensure interoperability, but it remains possible to classify base station vendors based on how they are configured and act. Design decisions and proprietary algorithms differ across base station vendors, and UEs can observe differences in the Radio Resource Control (RRC) configurations and Medium Access Control (MAC) layer (Figure 2). By creating classifiers that map these differences to vendors, UEs can classify vendors with high confidence and detect when surveillance equipment deviates from expected behavior. In fact, open source software can even classify devices with software defined radios [6]–[10], allowing UEs to detect malicious RAN infrastructure without transmitting or connecting to the cellular network.

While transmission fingerprinting could play a role in vendor classification, features found in the RF transmissions identify the wrong RAN component. Features that differentiate RF transmissions would be based on design choices made at the radio unit; e.g., manufacturing the antenna, converting digital IQ to analog signals, and beam forming. However, the threats we address are not based in the radio unit, but in the base station. The RRC and MAC layer information that we use for classification are directly determined and configured on the base station.

The vendor classifiers could help advanced reconnaissance teams assess risks posed by the RAN before deploying personnel or equipment in an area, and inform SIM card selection. It could also help detect custom private deployments by adversary forces, since those base stations will likely appear different in the control channel than carrier equipment. The most ambitious use of vendor identification is to automatically avoid malicious vendors by placing intelligence on the UE that will only connect and transmit through benign base stations.

D. Proof of Concept: AVOID Puck Prototype

We created an initial prototype of the proposed RAN solution—called Automatic Verification of Internet Data-paths (AVOID) Puck—that combines a modem, SDR, and Wi-Fi to create a tactical bubble. AVOID Puck can be used to secure communications inside a vehicle, or from inside an equipment backpack. The puck presents a Wi-Fi network to user equipment (UEs) and backhauls through commercial LTE and 5G networks, securing the backhaul with a base station vendor classifier and decision making. Our classifier uses multiple features found in the RRC and MAC protocols to distinguish base stations made by each of the five main vendors; i.e., Ericsson, Nokia, Samsung, Huawei, and ZTE.

Figure 3 shows the prototype design. The centralized controller orchestrates the system and implements the *AVOID-Vendor* strategy. The puck uses multiple cellular modems and a software-defined radio (SDR) to gather RRC and MAC layer information, and passes that data to the classifier for analysis. The Wi-Fi access point allows nearly any phone or other wireless device to connect securely to the RAN, and preserves the ability to make phone calls with Wi-Fi calling.

Based on the base station vendor classification, AVOID Puck will either blacklist a cell, switch carriers, or take no action. When the classifier returns a base station vendor prediction with low confidence, the AVOID controller will instruct the modem controller to blacklist the cell to avoid connecting to surveillance equipment. A low confidence prediction suggests the base station vendor is not known to the classifier, and therefore presents a potential risk to communications. If the classifier has high confidence that a cell is Huawei or ZTE, AVOID Puck immediately switches carriers to avoid sending data through adversary-controlled base stations, by changing

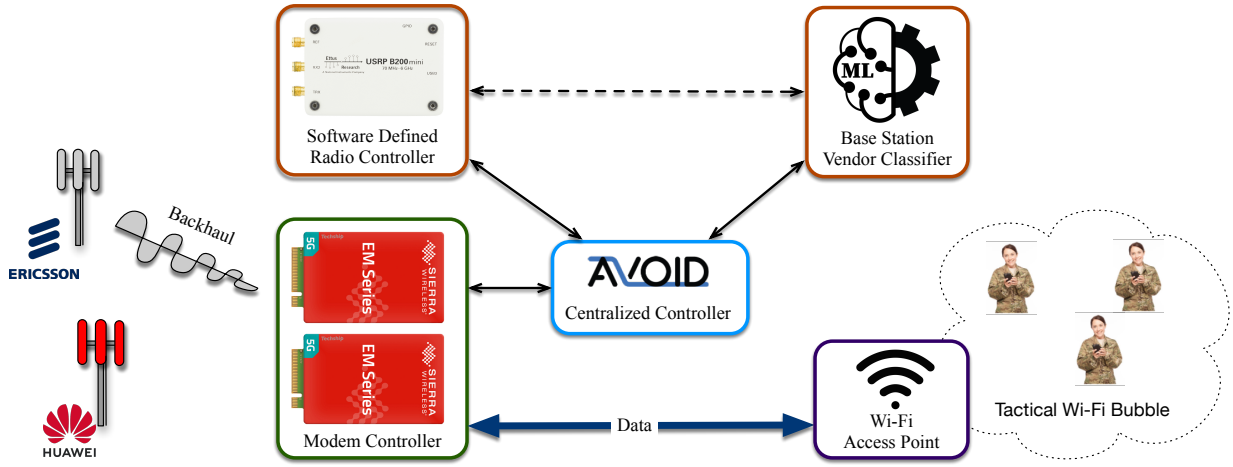

Fig. 3. The AVOID Wi-Fi Puck ensures that communications for devices in the tactical bubble only traverse benign commercial cellular network base stations.

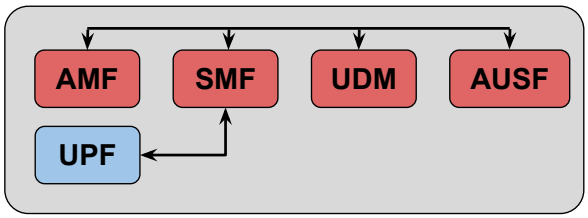

Fig. 4. Simplified 5G Core architecture with the most relevant network functions (NFs). In the control plane, the AMF serves as the hub that connects the RAN with other network functions, the SMF interacts with the core's data plane, the UDM handles subscriber data, and the AUSF authenticates users. The data plane consists of the UPF, which forwards IP packets between the wireless network and the Internet.

the active SIM and/or modem. The classifier takes ≈ 200 ms to return a prediction on an Intel i7-12700H mobile processor.

IV. Threats in the Mobile Core

The mobile core handles subscriber authentication, handovers, network policies, and packet forwarding. When a user connects to the cellular network, the base station passes the user's information to the core so that the core and user can mutually authenticate each other. Following successful authentication and the establishment of a data session, the user can transmit and receive data. The base station receives transmissions from UEs and tunnels them to the mobile core, which in turn forwards the IP packets to the broader Internet.

Because mobile cores do not participate in transmitting or receiving RF, they can be far more centralized than the base stations. A single core can handle thousands of base stations in commercial cellular networks. While base station vendors typically bundle hardware and software into a single product, modern mobile cores are typically software products designed to run in either data centers or clouds which are composed of multiple different network functions resembling a microservice-based architecture (Figure 4).

A. Threats: Exploitable Software & Insiders

As with base stations, the primary threat is exploitable software in the mobile core that allows an adversary to eavesdrop on users of the cellular network. Commercial carriers typically harden the core to industry security standards, but DOD's threat models typically require a higher standard. An adversary could gain access through intentionally placed backdoors in software provided by certain vendors, or exploit a vulnerability, e.g., zero-day exploit. Unlike base stations, the centralized and software-based mobile core presents a tractable target for software exploits. Compromised access could allow an attacker to disrupt, observe, or tamper with packets forwarded in the data plane.

Adversaries could also attack the mutual authentication, using software exploits or insiders to obtain the authentication keys used by the mobile core. The assumption in LTE and 5G is that only the legitimate carrier can access the authentication keys and that the data plane is secure against attack. After obtaining the keys, the adversary could set up surveillance equipment that is able to authenticate users, and likely trick users into sending data and locations over the rogue surveillance core.

B. Current Behavior: Trust the Mobile Core

In LTE and 5G, UEs are designed to trust any mobile core that successfully completes the mutual authentication, leaving UEs exposed to eavesdropping. After a UE attaches to a base station and authenticates with the core, it sends data and does not reevaluate the legitimacy or security of the core. An adversary that can either compromise the core software or obtain authentication keys can observe DOD communications, locate DOD personnel, or selectively disrupt DOD traffic.

C. Proposed Approach: Unique Features Identification

It is possible to gain insight into the mobile core that would allow users to detect anomalous core configurations or behaviors. Some of these distinguishing configurations might manifest in the UE authentication procedure; e.g., supported

encryption algorithms. Alternatively, classifiers could observe how the core responds to different events (handovers, switch off, detach, etc) or errors (unknown IMSI, timeouts, etc) to identify the core software vendor.

D. Proposed Approach: Control the Core

Another option is for DOD to operate their own mobile core, and partner with commercial carriers to share the commercial RAN infrastructure [11]. Detecting anomalous behavior can help protect against malicious software and surveillance cores, but it cannot defend against all software exploits or insider attacks. Controlling the core can better protect the authentication keys and increase packet forwarding security. Sharing the RAN with commercial carriers significantly reduces the complexity and cost of operating a wireless network, since the RAN is widely distributed while the core is centralized.

Controlling the mobile core is best done in combination with UE-side analytics to secure communications against base station threats and potential surveillance core attacks. Even in private 5G networks, surveillance equipment that masquerades as legitimate infrastructure remains a critical threat, and UEs must be able to defend themselves. Looking for threats in the RAN also allows DOD to trust-but-verify infrastructure claims and modification made by commercial partners overseas.

V. Threats in the Broader Internet

Commercial cellular networks are primarily access networks for the broader Internet, and once traffic leaves the mobile core it enters the opaque cloud of Internet routing. For service members overseas trying to reach services hosted in the U.S., traffic will typically traverse multiple commercial Internet networks all configuring and controlling their infrastructure independently. The paths that packets take result from a combination of traffic engineering and business policy decisions by each of the individual Internet networks.

A. Threats: Sophisticated Network Intelligence Systems

Transmitting information through the untrusted public Internet might expose DOD communications to the sophisticated traffic recognition and disruption capabilities that our adversaries possess. As soon as DOD hands off a packet to a commercial wireless network for transmission over the public Internet, the DOD loses control over how that packet reaches the destination. Any Internet Service Provider (ISP) headquartered in an adversarial nation-state, any ISP infrastructure residing in adversary-controlled territory, and potentially even routers manufactured by certain vendors, can be compelled to subject traffic to the adversary's intelligence regime. These capabilities are advanced and complex, using a combination of passive and active techniques to thwart attempts at traffic obfuscation [3], including VPNs and Tor's pluggable transports [4].

B. Current Behavior: Encrypt Data

UEs have no control over the Internet paths that transmitted data takes. Routing through the Internet generally uses destination-based forwarding. While a UE can decide which services to communicate with, the path itself is determined by Internet routers, since ISP networks rarely support source routing. Moreover, UEs have an extremely limited ability to understand the infrastructure along the paths they use. Traceroute-style probing is the only mechanism available to revealrouters, but it only provides a list of IP addresses without any accompanying geographic or hardware vendor metadata.

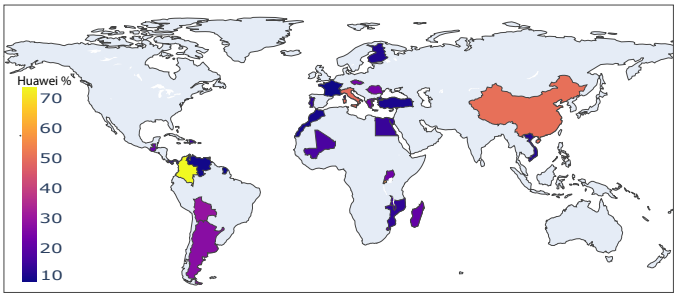

Fig. 5. Fraction of observed routers in each country inferred to be Huawei in April 2024, based on measurements from CAIDA's Ark platform. Extracting the information to create this map requires combining router fingerprinting [12] with router geolocation [13]. Methodologies for both objectives are continually evolving.

C. Proposed Approach: Underlay-Aware Overlay Routing

DOD needs communications infrastructure equivalent to clean supply chains. Advances in obfuscation and VPN architectures cannot fully overcome the fundamental challenge of an untrustworthy underlying infrastructure substrate. DOD needs overlay technology that is not only aware of the underlying network topology, but also geopolitical and economic attributes of that topology. The highly distributed nature of autonomous networks that make up the Internet prevents per-router-hop control of traffic crossing independent commercial networks. But one essential feature of global IP networks—the pervasive use of ubiquitous destination- or flow-based forwarding—means that with sufficiently rich understanding of the underlying topology, one can use strategic selection of source and destination IP addresses to indirectly choose an end-to-end path.

Recent advances in Internet path analytics provide the foundation for performing risk assessments of Internet paths, allowing the overlay to select an acceptable gateway into the overlay for each UE. For example, Figure 5 combines geolocation with router vendor fingerprinting to infer which countries have extensive Huawei deployments.

1) Revealing Benign Network-Level Paths: Discovering the network-level path that communications take can reveal which paths traverse infrastructure operated by adversarial Internet networks. New open source tools can convert the IP addresses in traceroute-style output into network-level paths with high fidelity [14]–[17]. This approach can also incorporate information from router interface hostnames [18], [19], as well as handle unique challenges posed by layer 3 virtual private networks [17] and cloud networks [20].

2) Geolocating Network Infrastructure: Geolocating network infrastructure would allow the DOD to determine which

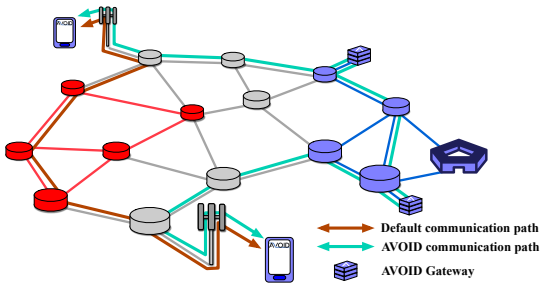

Fig. 6. The AVOID system will recognize adversary-controlled infrastructure (red) and route communications along benign paths to the AVOID gateways in the DOD network (blue).

paths enter adversary-controlled territory and thus inform rerouting of traffic to minimize exposure risk. Recent research overcame longstanding challenges in geolocating network infrastructure, including training a machine learning model to extract location information from hostnames [13] and using topological constraints to geolocate routers [20].

3) Fingerprinting Router Vendors: Some router vendors are inherently untrustworthy because of the potential for backdoor access and data exfiltration. New advancements in the Internet measurement community allow for remote router vendor fingerprinting using SNMPv3 and probing a router with a variety of ICMP, TCP, and UDP packets [12].

D. Proof of Concept: AVOID Path Prototype

We implemented an initial prototype of a topology-aware overlay, called *AVOID-Path*. Our prototype focuses on the overlay framework, which will incorporate specific analytics. On initial connection, the UE reaches out to a bootstrapping server that instructs the UE to connect to a specific overlay gateway node. These gateway nodes are implemented as Docker containers and can be placed anywhere there is a secure path to the rest of the DOD network; e.g., forwarding operating bases. If path analytics indicate that the path to the initial gateway includes potentially adversary-controlled infrastructure, we included functionality that can instruct the UE to connect to another gateway reachable over benign paths.

This prototype design has three features that make it especially compelling as a platform to support secure cellular communications over the Internet. First, the *AVOID-Path* architecture accommodates layering nearly any obfuscation approach above it, complementing a wide range of other efforts to secure application communications. Second, UEs can use *AVOID-Path* to securely and reliably communicate with DOD and any other DOD cellular devices. As long as a 5G device has a benign path to an AVOID gateway available, its communications with any other AVOID-connected device will evade adversary observation (Figure 6). Third, *AVOID-Path* works with any application, requires no modification Internet or DOD network routers, and does not rely on cooperation from any other network.

VI. Conclusion

For the first several decades of the Internet, conventional threat models did not include adversaries *inside* the network infrastructure. Consequently, little attention was paid to inferring the presence of such adversaries, or creating protocol support to route around them. Today, we live in a world where adversaries potentially exist in each network component our traffic touches, and it is time for the "Internet as a black box" assumption to yield to an emerging conceptual framework that can leverage informed inferences of infrastructure properties to improve the security and privacy of DOD communications. We see short-term opportunities in this direction, such as base station fingerprinting and router-level geolocation capabilities. But we also see a longer-term research and development agenda for DOD that could provide a more transparent and accountable communications substrate for everyone.

References

[1] B. Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256, 2020.
[2] A. Houmansadr, C. Brubaker, and V. Shmatikov, "The Parrot is Dead: Observing Unobservable Network Communications," in *IEEE S&P*, 2013.
[3] J. Beznazwy and A. Houmansadr, "How China Detects and Blocks Shadowsocks," in *ACM IMC*, 2020.
[4] D. Xue, R. Ramesh, A. Jain, M. Kallitsis, J. A. Halderman, J. R. Crandall, and R. Ensafi, "OpenVPN is Open to VPN Fingerprinting," in *USENIX Security*, 2022.
[5] C. Reichert, "U.S. finds Huawei has backdoor access to mobile networks globally, report says," https://www.cnet.com/tech/mobile/us-finds-huawei-has-backdoor-access-to-mobile-networks-globally-report-says/.
[6] Y. Xie and K. Jamieson, "Ng-scope: Fine-grained telemetry for nextg cellular networks," *PAMACS*, 2022.
[7] H. Wan and K. Jamieson, "Evolving mobile cloud gaming with 5g standalone network telemetry," *arXiv preprint arXiv:2402.04454*, 2024.
[8] N. Ludant, P. Robyns, and G. Noubir, "From 5G Sniffing to Harvesting Leakages of Privacy-Preserving Messengers," in *IEEE S&P*, May 2023.
[9] R. Falkenberg and C. Wietfeld, "FALCON: An accurate real-time monitor for client-based mobile network data analytics," in *IEEE GLOBECOM*, Waikoloa, Hawaii, USA, Dec 2019.
[10] D. T. Hoang, C. Park, M. Son, T. Oh, S. Bae, J. Ahn, B. Oh, and Y. Kim, "LTESniffer: An Open-source LTE Downlink/Uplink Eavesdropper," in *ACM WiSec '23*, 2023.
[11] B. Shores, "Network Sharing Program Considerations," OUSD(R&E) FutureG Team, 2024.
[12] T. Albakour, O. Gasser, R. Beverly, and G. Smaragdakis, "Illuminating router vendor diversity within providers and along network paths," in *ACM IMC*, 2023.
[13] M. Luckie, B. Huffaker, A. Marder, Z. Bischof, M. Fletcher, and K. Claffy, "Learning to Extract Geographic Information from Internet Router Hostnames," in *ACM CoNEXT*, Dec. 2021.
[14] A. Marder and J. M. Smith, "MAP-IT: Multipass Accurate Passive Inferences from Traceroute," in *ACM IMC*, 2016.
[15] M. Luckie, A. Dhamdhere, B. Huffaker, D. Clark, and K. Claffy, "bdrmap: Inference of Borders Between IP Networks," in *ACM IMC*, 2016.
[16] A. Marder, M. Luckie, A. Dhamdhere, B. Huffaker, K. Claffy, and J. M. Smith, "Pushing the Boundaries with bdrmapIT: Mapping Router Ownership at Internet Scale," in *ACM IMC*, 2018.
[17] A. Marder, M. Luckie, B. Huffaker, and K. Claffy, "vrfinder: Finding Outbound Addresses in Traceroute," *SIGMETRICS*, 2020.
[18] M. Luckie, A. Marder, B. Huffaker, and K. Claffy, "Learning Regexes to Extract Network Names from Hostnames," in *AINTEC*, Dec. 2021.
[19] M. Luckie, A. Marder, M. Fletcher, B. Huffaker, and K. Claffy, "Learning to extract and use ASNs in hostnames," in *ACM IMC*, 2020.
[20] A. Marder, K. Claffy, and A. C. Snoeren, "Inferring Cloud Interconnections: Validation, Geolocation, and Routing Behavior," in *PAM*, 2021.