A New Interest-Based Protocol to Hide and Protect Servers in IP Networks

Marco A. Coutinho
High-Speed Networks Lab.
Federal Univ. of Rio de Janeiro
Rio de Janeiro, Brazil
marco.coutinho@ravel.ufrj.br

Evandro L. C. Macedo
High-Speed Networks Lab.
Federal Univ. of Rio de Janeiro
Rio de Janeiro, Brazil
evandro@ravel.ufrj.br

Luís F. M. de Moraes
High-Speed Networks Lab.
Federal Univ. of Rio de Janeiro
Rio de Janeiro, Brazil
moraes@ravel.ufrj.br

Victor Cracel Messner
Compasso Laboratory
Federal Univ. of Rio de Janeiro
Rio de Janeiro, Brazil
vcmessner@cos.ufrj.br

Diego L. Cadette Dutra
Compasso Laboratory
Federal Univ. of Rio de Janeiro
Rio de Janeiro, Brazil
diegodutra@lcp.coppe.ufrj.br

Claudio L. de Amorim
Compasso Laboratory
Federal Univ. of Rio de Janeiro
Rio de Janeiro, Brazil
amorim@cos.ufrj.br

Valeriana Gomes Roncero
Center for Research in Physics
Rio de Janeiro, Brazil
valeriana@cbpf.br

Nilton Alves Júnior
Center for Research in Physics
Rio de Janeiro, Brazil
naj@cbpf.br

Marita Maestrelli
Center for Research in Physics
Rio de Janeiro, Brazil
marita@cbpf.br

Marcio Portes de Albuquerque
Center for Research in Physics
Rio de Janeiro, Brazil
mpa@cbpf.br

Sandro Silva
Center for Research in Physics
Rio de Janeiro, Brazil
sandro@cbpf.br

2022 International Conference on Information Networking (ICOIN) | 978-1-6654-1332-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICOIN53446.2022.9687158

***Abstract*—In this paper, we propose a new interest-centric and no-IP-based technique using the Radnet protocol to hide and protect communication among servers and network appliances. In particular, we carry out experiments considering log servers protection, which contains one of the most valuable assets for both network administrators and attackers, since the former can audit and learn about the attacks, and the latter can cover their actions during an attack. Using graphical analysis, we demonstrate that our approach does not have a significant impact on the performance of applications in a real datacenter environment.**

***Index Terms*—network security, obfuscation, interest-centric networks, infrastructure protection**

I. Introduction

The commonly known IP networks provide the essential connectivity service applied to a multitude of today's networks. Any connected device can reach another device through an IP address, which aggregates enough information not only to identify a device but also to locate it. Nevertheless, from a security perspective, the fact that a device can be reachable simply by using the respective IP address of the device can put devices at risk, turning them vulnerable to cyberattacks that are based on IP. In particular, considering a private network of a corporate, or academic environment, an attacker can take advantage of IP addresses to discover information about the network topology, users' behaviors, routines, and other metadata that can help him/her to perform a successful attack. To sum up, if the attacker reaches the log servers of a network, a precious security asset becomes dangerously vulnerable, since the malicious user can compromise network infrastructure and servers without being noticed by deleting all of his/her actions logs.

Traditionally we protect computational resources from such threats using Intrusion Detection Systems (IDS), antivirus, and firewalls. Most of these methods are inherently proactive to avoid attacks. Once they identify anomalies, they promptly act based on prior information about attacks and network behavior to stop the attack. Additionally, all actions are registered in log servers to future audit processes in which network administrators can understand attackers' methodology, build new attack signatures, and provide information to forensic analysis.

Unfortunately, attackers also know the importance of audit traces the logs provide. Therefore, among other possible malicious actions, they usually attempt to compromise log servers. As logs are stored in servers that are reachable through IP addresses, servers end up vulnerable to attacks where the aggressors can locate and devastate these and other valuable security services and their data.

To address this issue, a secure transfer of log events

over non-secure channels of a computer network is needed, which motivates removing the IP-based communication among servers and network appliances to eliminate this potential vulnerability. The Radnet [1], [2] is an interest-centric opportunistic network protocol that does not use IP addresses. Hence, we propose in this paper a new interest-centric and no-IP-based technique using the Radnet protocol to hide and protect the communication among servers and network appliances. This way, we can provide network infrastructures with invisibility to any important appliance.

We run experiments considering a real datacenter environment to provide results about the efficiency of our approach. We use graphical analysis to demonstrate that our approach does not have a significant impact on the performance of the applications running on the real network. To the best of our knowledge, our proposal is the first attempt to protect servers and network appliances using an IP independent strategy.

The remaining of this paper is organized as follows. Section II presents a background and the related previous work. In Section III we show the methodology we use to analyze our approach. The proposal analysis and discussions on obtained results are covered in Section IV. Finally, Section V concludes the paper.

Radnet complements the functions of traditional security elements such as firewalls. These elements are dedicated to protection and reactivity to security attacks. Radnet acts proactively while these other elements are only reactive and its main function is to prevent a contamination or an attack from being carried out.

II. Background and Related Previous Work

Different from IP networks, Interest-Centric Networks (ICN) does not rely on specific addresses that allow the identification and the location of network members. Instead, ICNs connects peers that share a common interest. An example of ICN is the Radnet [1], an interest-centric opportunistic network protocol, originally proposed for MANETS. Instead of using IP addresses, Radnet uses an active prefixes (APs) that has two components: a prefix and a name of interest. The AP enables the probabilistic message forwarding, the node identification, and make a reference to an application in a node. Figure 1 presents the components of the AP **(a)** message header **(b)** on Radnet.

Compared to other architectures of information/content-centric networks or even Named Data Networking, Radnet is a more lightweight protocol that provides obfuscation and shadowing techniques to protect critical infrastructure elements. The table I shows a quick comparison between Radnet and all alternatives architecture. One point is very relevant in terms of performance. As proposed in [3], the existence of FIB and PIT tables, essential to provide associative entrance of interesting message and content packet, NDN is very dependent on caching feature. Radnet does not have this dependency which could be considered an advantage.

Figure 2 shows a possible communication scenario between two devices on a four-node network using the Radnet protocol, where the wireless transmission range is delimited by the dashed circumference, each AP with two numeric fields, and a single interest registered at the network layer. The communication begins with Node A that sends a message with prefix $\{5\}$ and interest $\{\text{Football}\}$. Node B receives the message from A (since it is within the transmission range of A) but, as Node B has a different interest $\{\text{Lift}\}$, it does not consume the message. However, Node B forwards the message because there is a prefix matching between A and B, namely, $\{5\}$. Since Node B also transmits in broadcast, A receives again the message forwarded by B but it detects that the message was already sent and discards it. Similar to Node B, Node C receives and forwards the message from B given that the prefix also matches, but does not consume the message. When Node D receives the message broadcast by Node C, it detects that there is an interest match $\{\text{Football}\}$ and consumes the message, delivering it to the respective application. Different from previous nodes, Node D does not forward the message since its prefix is $\{4\}$, which does not match with the message prefix.

Radnet is a protocol that aims to protect the infrastructure Using IP connection obfuscation technique for this, and it has by definition a content orientation that allows only unauthorized nodes. It guarantees confidentiality in the communication that uses this protocol. Compared to a traditional tunneling technique, Radnet is superior in performance and does not cause impact such as overhead.

To provide more realistic results in terms of the efficiency of our proposal, we consider a real datacenter environment of the Brazilian Center for Research in Physics (CBPF). The network topology of CBPF is organized according to the hierarchical model called the collapsed backbone, which stands for points of the local network spread through access switches and centralized through a core switch, similar to a star topology. These switches are structured in stacks and gather all traffic generated by VLANs. Through the experiment, first, we measure the switch interface metrics without the Radnet activated to know what is the normal pattern. Then, we activate the Radnet to protect the logs and hide the destination of log traffic to obfuscate it. Figure 3 depicts the topology considered in the experiment. For security reasons, a new network segment was

Table I
Comparison among content-based network architectures

	Protocols			
Feature	NDN [3]	ICN, CCN [4] [5]	Tunneling [6] [7]	RADNET
Hierarchy	Highly dependent	Highly dependent	NA	NA
Overhead	High	High	30%	No
Control & User Plane	Separated	Separated	At Endpoint	NA
Digital Signature	Yes	Hash	Yes	Possible
Routing	Normal IGP, eGP	Normal IGP, eGP	NA	NA
Caching	Yes	Yes	No	No

created with a new VLAN in the CBPF environment, which does not mean that this intervention of a new network segment is necessary for Radnet to work properly.

This way, the central aspect of our proposal is the protection of servers by hiding them from IP attacks using Radnet. Solutions based on server hiding are a common theme of discussion, and one of the first proposed solutions for the theme was published in 1981 [8]. Chaum discussed a solution for email services using public-key cryptography.

Eavesdroppers can use other tools to scan the IP and MAC address of a victim. An idea proposed by Jafarian *et. al* [9] consists of making an Openflow controller dynamically changing the real IP of the end hosts to a random virtual IP that will be translated to the real IP later. By doing so, the real IP addresses obfuscate attackers and, since the real IP remains unchanged, the IP change is transparent to the server. This idea tries to maximize the distortion and the unpredictability for the attackers. A similar idea was proposed by [10]. This proposed hiding the IP and the MAC address protecting external scanning, eavesdropping, and from internal compromised hosts.

Another way of protecting server communications from eavesdropping is by mimic traffic and famous protocols as shown in [11]. In that way, attackers cannot tell when and where the wanted information, for instance a registry of events, were sent. This kind of approach has problems which are exposed in [12].

Restricting access to a server is another way to protect it. The idea proposed by many others authors have the basis of a port-knocking, in which the one who is authorized to request information for a server has the code of how many times he/she has to knock. In this context, a recent work that makes use of chaos-based hash functions has been proposed [13]. This is a cutting-edge theme and makes bold claims that the proposed method protects servers from attacks ranging from port scans to zero-day attacks.

Anonymity has become a concern in the community, and ideas of preserving anonymity from users and servers through routing has been proposed. This kind of routing has been called onion routing and the ideas, as well as other ways to discover hidden servers, are discussed in [14]. Solutions that use onion routing are know by their delay, which makes them unviable for real-time applications.

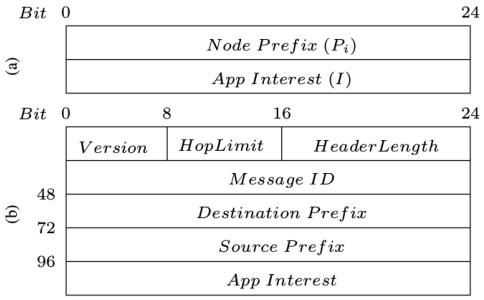

Figure 1. Radnet Message: (a)Active Prefix and (b) Message Header

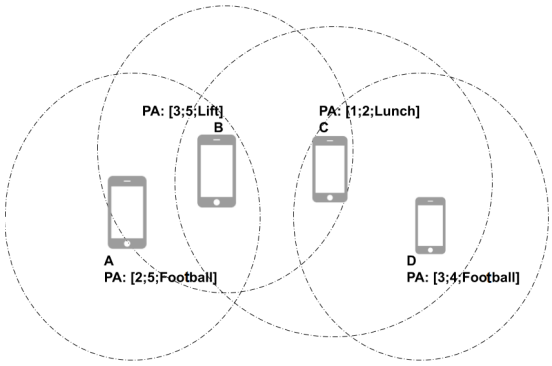

Figure 2. Radnet communication example with four nodes

Table II
COMPARISON BETWEEN RELATED WORK AND THIS PROPOSAL

Work	Technique	Broadcast	IP independent
J. Park *et. al* [10]	Proxy/Invi-based	No	No
Jafariam *et. al* [9]	Dynamic IP change	No	No
Wang *et. al* [11]	Traffic Mimic	No	No
Major *et. al* [13]	Port Knocking	No	No
Almaini *et. al* [15]	SDN	No	No
Kumar *et. al* [16]	Blockchain	Yes	No
Makinda *et. al* [17]	Scada	No	No
This proposal	Interest-based	Yes	Yes

In [15], authors reiterates the intelligent controllers that control switches get overloaded and become prone to failure in an *SDN*, and proposes an edge-based solution for the problem. This solution delegates part of the control that does not require global knowledge to the own switches. Instead of using a regular port-knocking, authors expose the advantages of their method with a service that monitors firewall logs.

Preserving logs for a long period of time while ensuring the integrity and the login process has been a problem for long

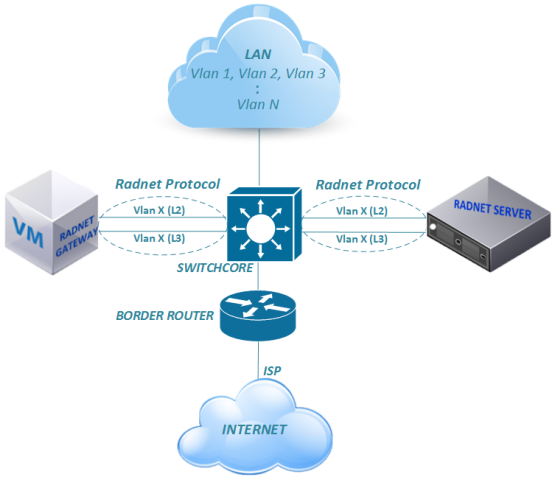

Figure 3. Experimental network topology of CBPF

time. [16] proposes a blockchain solution to this problem that can be used in cloud systems.

In [17], authors propose a public-key infrastructure for Karabo, where every user shall access the SCADA using a token signed by a certification authority which signs the public key of device servers. In this paper, since users communicate their session token encrypted with the device server public key, and only communicates with certified device servers, authors argue that the token is only known by the certification authority, the user, and the certified device servers.

We show a comparison among the related works in Table II.

III. Analysis Methodology

In this section, we provide an analysis of our proposal through a methodology based on performance analysis. According to [18], we can find many issues that lead one system to be compromised in terms of security aspects for any application or infrastructure. By security aspects, we consider [19]:

- restrict access to critical content;One Radnet server
- infrastructure availability to support any application with critical mission or not;
- identity assurance with capacity to deny any unauthorized access and revoke any suspect identity;
- account every change or activity for further analysis on suspect behavior.

A. Impact visualization

The Wavelet technique is widely used for low intensity traffic demonstrations and its impact on local network infrastructure. For the purposes of this work wavelet will be used to demonstrate the low impact of Radnet traffic since the syslog protocol was chosen to be encapsulated using the Radnet protocol.

Continuous Wavelet (CW) is a type of transform that uses a process to generate variable scaling to unlock different coefficients from a sliding sample of time. Wavelet coefficients are the final product of transformation consisting of values gathered from the combination of frequency and the time in which frequency was collected.

More information about wavelet transformation can be found in [20].

B. Data Clean Up

The first step of our methodology is the Data Sampling step. We sampled de CBPF's traffic using SNMP protocol in intervals of 5 minutes. To smooth and clarify the graphic information about CBPF's network traffic, all collected data were preprocessed using the exponentially weighted moving average (EWMA) algorithm as represented in equation 1.

$$S_t = \alpha \left[Y_t + (1-\alpha) Y_{t-1} + (1-\alpha)^2 Y_{t-2} + \cdots \right. \\ \left. \cdots + (1-\alpha)^k Y_{t-k} \right] + (1-\alpha)^{k+1} S_{t-(k+1)} \quad (1)$$

Next, the Data Cleaning step is essential to make more accessible the information extraction from the data collected. Useless samples could be most straightforward discarded once they have no impact on results. The Outliers step uses Normal distribution analysis, in which values above percentile 0.9 and below 0.1 were considered outliers and discarded. Both percentiles are estimations obtained from testing impacts over output precision of analysis, and this study does not consider any previous benchmark. Hence, the processing to generate graphic output becomes smooth due to the data optimization process of CBPF traffic and the elimination of outliers.

Figure 4. Representation of the methodology used in this work: data extraction from network, data cleaning and wavelet processing to detect abnormalities

IV. Proposal Analysis and Discussion

Radnet uses broadcast to transmit content between nodes that share the same interest. Since broadcast traffic might impact network performance, it is critical to demonstrate that Radnet will not impact the overall performance if applied to a usual network with lots of services and users. We test the Radnet with an intensive and critical service to tackle this challenge, namely, the Syslog transport. Without compromising network performance, our goal is to protect the communication between log servers and network nodes (e.g., routers, switches, and other servers).

To evaluate possible impacts caused by our approach, we adopted the following metrics to monitor its behavior: number of broadcast packets, CPU consumption impact, system memory demanded, and number of packet drops. To avoid installing our protocol stack into sensible elements running in a production environment, we design a topology consisting of:

- One Radnet gateway to collect the logs using conventional UDP/514 port from other elements in datacenter;
- One Radnet server to store the logs sent by other nodes.

We consider three assumptions:

1) Radnet might generate a huge amount of data that will significantly change CBPF traffic profile. The first goal here is to identify any potential damage on CBPF infrastructure in such a way that it would characterize Radnet as an intrusive protocol. CBPF concentrates most of the research in applied physics and, therefore, variable traffic is expected throughout the day, with a greater concentration of work during business hours.
2) Radnet may produce increasing consumption of resources of the elements involved, such as CPU, system memory, and others. Moreover, that exceeding consumption could

lead the whole environment to exhaustion and compromise services and performance of users in general. Tests and collections of SNMP and logs will demonstrate how valid these assumptions are. According to the authors' expectations, no impact could be detected even with Radnet implemented to protect the CBPF nodes' communication fully.

3) Radnet may produce increasingly low-rate traffic that cannot be detected using any high-rate traffic analysis tool. In this case, we apply the wavelet's method to detect whether Radnet traffic is relevant enough to compromise the quality of services in the CBPF environment simply due to its potential low impact probability. In fact, by using broadcast to keep the information within the protected channel hidden, Radnet does not impact the overall performance once the interest traffic (in our case, log UDP) is relatively low compared to the total traffic managed during regular working days.

Figures 5, 6 and 7 show how the traffic of service and specific broadcast were not impacted with Radnet being used to protect Syslog between server and gateway servers. We could not identify any disturbing provoked by the obfuscation process due to Radnet implementation. Other variables also were not impacted, as we can see in the graphics. No infrastructure aspect was significantly affected (CPU, free memory, the throughput of interfaces, for example) compared to the same workload before and after Radnet activation. All measurements indicate that Radnet does not compromise the environment as expected. However, we investigate in more detail using the wavelet technique (as described further) to confirm our impressions about the results in other ways. As we could not notice any deviation, we also observed that the number of packets corresponding to the Syslog service kept its tendency to grow as the demand from users was growing over the time we applied the collection and observation process. CPU consuming of the nodes also keeps on track, which means we cannot note anomalous behavior due to Radnet utilization. Memory allocation behaved as expected for the observed traffic.

Morlet wavelet [20] can capture and brakes down the frequency components over time, plotting its amplitude, or individual energy, or, in our situation, packets per second. Plotting this distribution of frequencies over time sampling is known as scalogram graphic. It is a valuable method to intuitively glimpse belief about the dynamic relationship of traffic and its components. Different colors indicate that the amplitude range is more intense in terms of impact (or traffic intensity) is close to red; otherwise, the lower impact is close to blue.

For this work, we adopted the Python library called PyWavelet [21] which makes it easy to construct the scalogram of any time series. Each component's impact can be determined once we set window variance to consider the fundamental frequencies range. Figure 8 shows the scalogram of Radnet

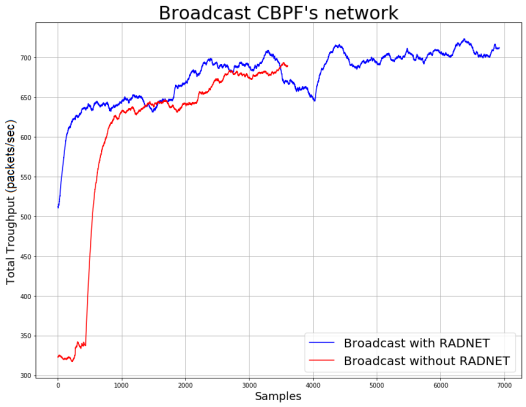

Figure 5. No impact on broadcast traffic due Radnet protocol over the CBPF network

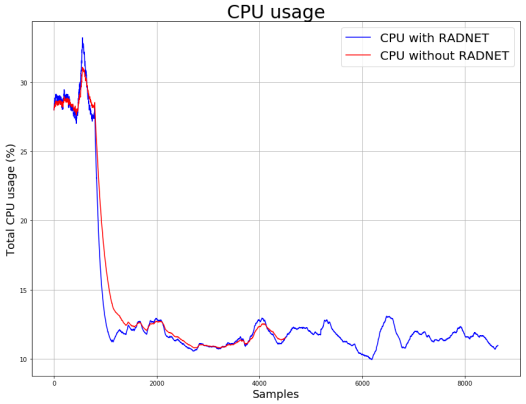

Figure 6. CPU consumption without any impact considering the same workload and peak of charge at the beginning of the process

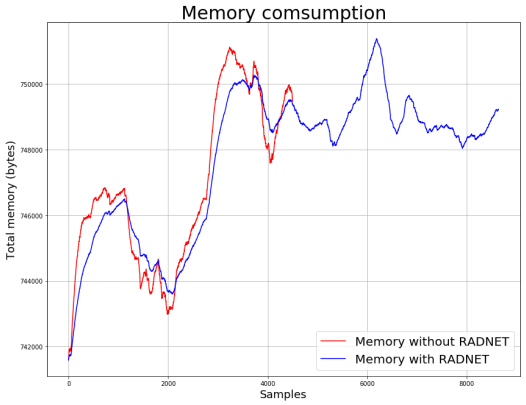

Figure 7. Memory consumption evolution

log generated.

1) Radnet/Syslog has lower frequency components, but with no trend or periodic component
2) The components intensity is considerably low compared to the total traffic (Figure 5). That is a promised method to be applied in detection systems.

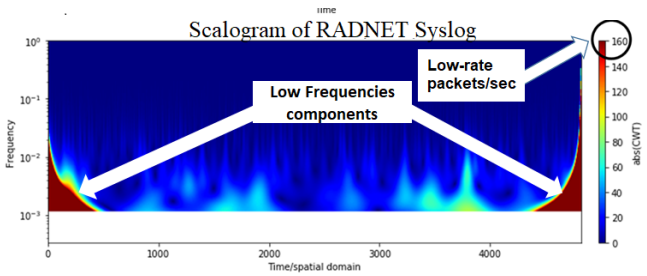

Figure 8. Representation of Syslog Radnet using CWT method

V. Concluding Remarks and Future Work

Radnet is a protocol designed to protect the conventional IT and network infrastructure by removing the dependability of IP addressing communication. We demonstrated that it could be adopted to hide any critical component that, otherwise, could be attacked by a malicious user.

In this work, we presented an efficient method to protect critical information using the Radnet protocol. We consider Syslog as a critical service to be protected. We collected results from one active corporate environment, and they can help in a decision-making process to plan how to protect critical infrastructure in real industrial networks.

According to our results, we could apply all benefits of using Radnet in any data center or network environment.

As future works, we propose applying Radnet in other critical components such as DNS servers and AAA/DHCP services to analyze the protocol's behavior and measure its impacts. We also consider implementing a real-time analysis of wavelets to evaluate our method's performance in terms of processing overload and overall computing requirements.

Another approach to implement Radnet as protection for additional perimeters would be new methods of attack, just like Ransomware and Low-rate denial of service in more details considering aspects of the infrastructure dedicated to IoT, Edge computing for offloading of critical applications, such as video on-demand, VR, health care monitoring, and many others.

References

[1] R. C. Dutra, H. F. Moraes, and C. L. Amorim, "Interest-centric mobile ad hoc networks," in *2012 IEEE 11th International Symposium on Network Computing and Applications*, pp. 130–138, 2012.

[2] L. Lima, P. C. Filho, D. L. C. Dutra, C. L. Amorim, E. L. C. Macedo, R. S. Silva, M. A. Coutinho, and L. F. M. de Moraes, "Radnet-s: Um mecanismo para transmissão segura e secreta de registros syslog," in *Anais do XXIII Workshop de Gerência e Operação de Redes e Serviços*, (Porto Alegre, RS, Brasil), SBC, 2018.

[3] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *SIGCOMM Comput. Commun. Rev.*, vol. 44, p. 66–73, July 2014.

[4] Y. Yu, Y. Li, X. Du, R. Chen, and B. Yang, "Content protection in named data networking: Challenges and potential solutions," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 82–87, 2018.

[5] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos, "A survey of information-centric networking research," *IEEE Communications Surveys Tutorials*, vol. 16, no. 2, pp. 1024–1049, 2014.

[6] S. Khanvilkar and A. Khokhar, "Virtual private networks: an overview with performance evaluation," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 146–154, 2004.

[7] X. Liu and W. Trappe, "Overlay tunneling as a policy tool for defending mobile ad hoc networks," *Security and Communication Networks*, vol. 9, no. 17, pp. 4482–4494, 2016.

[8] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, p. 84–90, Feb. 1981.

[9] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "Openflow random host mutation: Transparent moving target defense using software defined networking," in *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*, HotSDN '12, (New York, NY, USA), p. 127–132, Association for Computing Machinery, 2012.

[10] J. Park, J. Noh, M. Kim, and B. B. Kang, "Invi-server: Reducing the attack surfaces by making protected server invisible on networks," *Computers & Security*, vol. 67, pp. 89–106, 2017.

[11] Q. Wang, X. Gong, G. T. K. Nguyen, A. Houmansadr, and N. Borisov, "Censorspoofer: Asymmetric communication with IP spoofing for censorship-resistant web browsing," *CoRR*, vol. abs/1203.1673, 2012.

[12] A. Houmansadr, C. Brubaker, and V. Shmatikov, "The parrot is dead: Observing unobservable network communications," in *2013 IEEE Symposium on Security and Privacy*, pp. 65–79, 2013.

[13] W. Major, W. J. Buchanan, and J. Ahmad, "An authentication protocol based on chaos and zero knowledge proof," *Nonlinear Dynamics*, pp. 1–23, 2020.

[14] L. Overlier and P. Syverson, "Locating hidden servers," in *2006 IEEE Symposium on Security and Privacy (S P'06)*, pp. 15 pp.–114, 2006.

[15] A. Almaini, A. Al-Dubai, I. Romdhani, M. Schramm, and A. Alsarhan, "Lightweight edge authentication for software defined networks," *Computing*, pp. 1–21, 2020.

[16] M. Kumar, A. K. Singh, and T. V. Suresh Kumar, "Secure log storage using blockchain and cloud infrastructure," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–4, 2018.

[17] L. Mekinda *et al.*, "Securing Light Source SCADA Systems," in *Proc. of International Conference on Accelerator and Large Experimental Control Systems (ICALEPCS'17), Barcelona, Spain, 8-13 October 2017*, no. 16 in International Conference on Accelerator and Large Experimental Control Systems, (Geneva, Switzerland), pp. 1142–1148, JACoW, Jan. 2018. https://doi.org/10.18429/JACoW-ICALEPCS2017-THBPA02.

[18] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment*, IMW '02, (New York, NY, USA), p. 71–82, Association for Computing Machinery, 2002.

[19] B. Schneier and P. Sutherland, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. USA: John Wiley & Sons, Inc., 2nd ed., 1995.

[20] M. Stéphane, "Chapter 4 - time meets frequency," in *A Wavelet Tour of Signal Processing (Third Edition)* (M. Stéphane, ed.), pp. 89 – 153, Boston: Academic Press, third edition ed., 2009.

[21] G. R. Lee, R. Gommers, F. Wasilewski, K. Wohlfahrt, and A. O'Leary, "Pywavelets/pywt: Pywavelets v1.0.3," Apr. 2019.