RT: PESC 774 08/2021

Federal University of Rio de Janeiro

UFRJ

Technical Report: A New Interest-Based Technique to Hide and Protect Servers in IP Networks

Authors *Federal University of Rio de Janeiro (UFRJ/PESC)*:

Marco A. Coutinho
Evandro L. C. Macedo
Luís F. M. de Moraes
Victor Cracel Messner
Diego Dutra
Claudio L. de Amorim

Brazilian Center for Research in Physics (CBPF):

Valeriana Gomes Roncero
Nilton Alves Júnior
Marita Maestrelli
Marcio Portes de Albuquerque

Rio de Janeiro, August 9, 2021

Contents

Abstract

Security solutions are constantly developed to protect IP networks against many types of cyberattacks that appear daily. Some of these solutions include the use of powerful techniques based on machine learning, which applies statistical analysis to improve their accuracy and precision. However, even such advanced techniques are not sufficient to prevent systems from suffering service degradation attacks, such as Denial-of-Service (DoS), and more recently the Low-rate Denial-of-Service (LDoS).

We propose a new interest-centric and no-IP-based technique using the Radnet protocol to hide and protect the communication among servers and network appliances. In particular, we carry out experiments considering log servers protection, which contain 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 wavelet graphical analysis we demonstrate that our approach does not have a significant impact on the performance of applications in a real datacenter environment.

Resumo

Soluções de segurança estão em constante evolução para protegerem redes IP contra muitos tipos de ataques cibernéticos que aparecem diariamente. Algumas dessas soluções incluem o uso de técnicas poderosas baseadas em aprendizado de máquina, que aplicam análises estatísticas para melhorar sua exatidão e precisão. No entanto, mesmo essas técnicas avançadas, não são suficientes para evitar que os sistemas sofram ataques de degradação de serviço, como Denial-of-Service (DoS) e, mais recentemente, Low-rate Denial-of-Service (LDoS).

Propomos uma nova técnica centrada em interesses e sem base em IP usando o protocolo Radnet para ocultar e proteger a comunicação entre servidores e dispositivos de rede. Em particular, realizamos experimentos considerando a proteção dos servidores de log, que contém um dos ativos mais valiosos para administradores de rede e atacantes, uma vez que os primeiros podem auditar e aprender sobre os ataques, e os segundos podem cobrir suas ações durante um ataque. Usando a análise gráfica wavelet, demonstramos que nossa abordagem não tem um impacto significativo no desempenho dos aplicativos em um ambiente de datacenter real.

1 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 [Dutra et al. 2012, Lima et al. 2018] 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 wavelet 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 2 presents a background and the related previous work. In Section 3 we show the methodology we use to analyze our approach. The proposal analysis and discussions on obtained results are covered in Section 4. Finally, Section 5 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 retentively while these other elements are only reactive and its main function is to prevent a contamination or an attack from being carried out.

2 Background and related previous work

Different from IP networks, Interest-Centric Networks (ICN) does not rely on specific addresses that allows the identification and the location of network members. Instead, ICNs connects peers that share a common interest. An example of ICN is the Radnet [Dutra et al. 2012], 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 2 presents the components of the AP **(a)** message header **(b)** on Radnet.

Compared to others architectures of information/content-centric network or even Named Data Networking RADNET is a protocol more lightweight (Figure 1) applied to provide obfuscation and shadowing technique to protect critical elements of the infrastructure. The table 1 shows a quick comparison between RADNET add all alternatives architecture.One point is very relevant in terms of peformance. As proposed in [Zhang et al. 2014], the existence of FIB and PIT tables, essential to provide associative entrance of interesting message and content packet, NDN [Meisel et al. 2010] is very dependent of caching feature. Radnet hasn't this dependency which could be considered an advantage. Table 1 shows comparison approach of those protocols to Radnet.

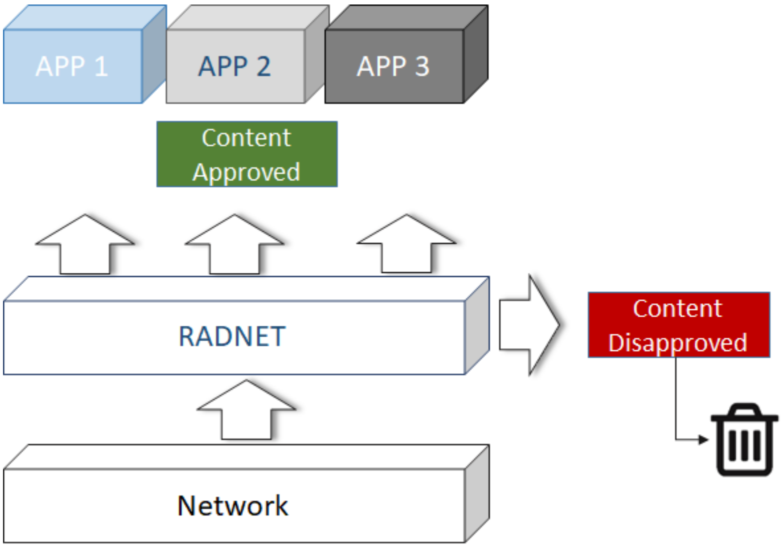


Figure 1: RADNET block diagram

Figure 3 shows a possible communication scenario between two devices on a four-node network using the Radnet protocol, where the wireless transmission

Table 1: Comparison among content-based network architecture Protocols

Feature	NDN	ICN, CCN	Tunneling	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

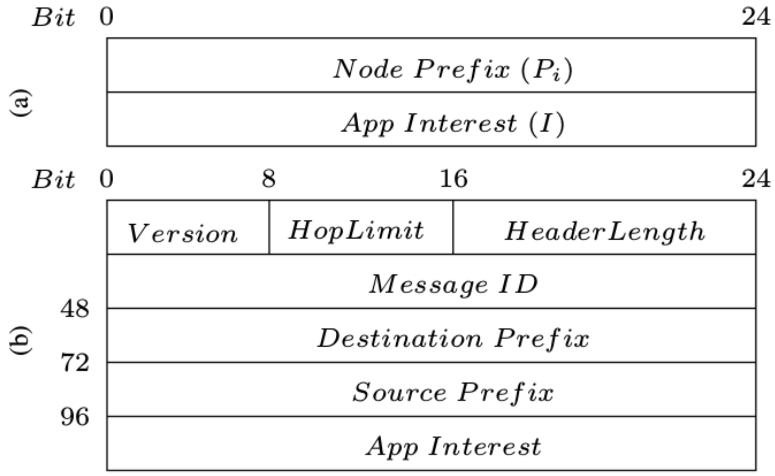


Figure 2: Radnet Message: (a)Active Prefix and (b) Message Header

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 {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 {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 {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 which allows only unauthorized nodes This guarantees confidentiality in the communication that uses this protocol. Does not use the tunneling technique plus direct communication based on the interests of the elements involved in the communication. Compared to a traditional tunneling technique, RADNET is superior in terms of performance and does not impact the local network that uses this protocol. This work aims to demonstrate the efficiency of net radio and the low impact produced in a real production environment.

In this work will be demonstrated how RADNET protocol can be used without impacting the local environment and A technique known as Black will be applied to identify low frequency attacks and impacts on communication throughput.

Thus radinet is a protocol that uses content-oriented techniques such as the more traditional techniques known as ICN/NDN.

For security reasons, a new network segment was 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.

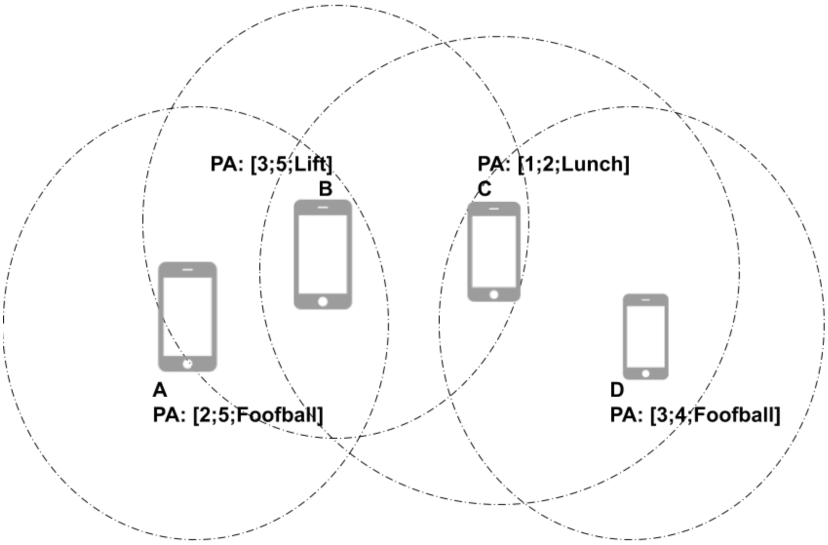


Figure 3: Radnet communication example with four nodes

To protect the integrity of security events logs provided by Syslog servers is essential to avoid possible access of unauthorized users to the log server. Hence, to protect these servers from intruders, we make use of Radnet, which is an interest-based protocol, to transmit sensitive event logs to Syslog servers through unsafe channels.

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 4 depicts the topology considered in the experiment.

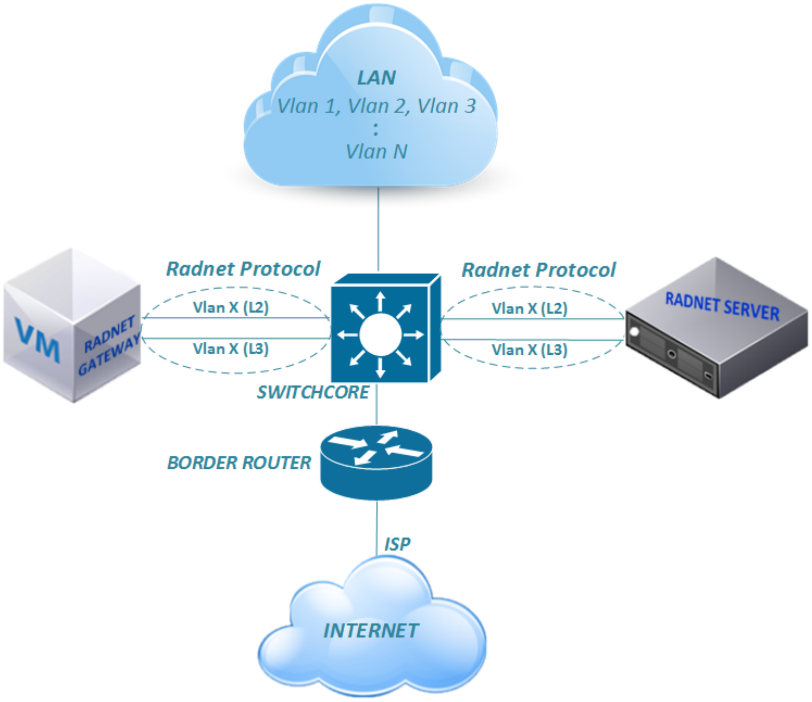


Figure 4: Network topology of CBPF

This way, the main 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 [Chaum 1981]. 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* [Jafarian et al. 2012] 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 [Park et al. 2017]. 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 [Wang et al. 2012]. 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 [Houmansadr et al. 2013].

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 [Major et al. 2020]. 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 [Overlier and Syverson 2006]. Solutions that use onion routing are know by their delay, which makes them unviable for real-time applications.

Table 2: Comparison between related work and this proposal

Work	Technique	Broadcast	IP independent
J. Park *et. al* [Park et al. 2017]	Proxy/Invi-based	No	No
Jafariam *et. al* [Jafarian et al. 2012]	Dynamic IP change	No	No
Wang *et. al* [Wang et al. 2012]	Traffic Mimic	No	No
Major *et. al* [Major et al. 2020]	Port Knocking	No	No
Almaini *et. al* [Almaini et al. 2020]	SDN	No	No
Kumar *et. al* [Kumar et al. 2018]	Blockchain	Yes	No
Makinda *et. al* [Mekinda et al. 2018]	Scada	No	No
This proposal	Interest-based	Yes	Yes

In [Almaini et al. 2020], 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 time. [Kumar et al. 2018] proposes a blockchain solution to this problem that can be used in cloud systems.

In [Mekinda et al. 2018], 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 2.

3 Analysis methodology

In this section we provide an analysis of our proposal through a methodology based on wavelets. According to [Barford et al. 2002], we may apply various techniques to compromise the security aspect of any application or infrastructure. By security aspects, we consider [Schneier and Sutherland 1995]:

- restrict access to critical content;
- 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.

At the end of the 90's [Fernandes et al. 2019], Intrusion Detection Systems (IDS) started to use Machine Learning (ML) algorithms. In terms of accuracy, precision, and processing response, we can list a few algorithms used to detect and identify malware's activities:

- Support Vector Machine (SVM), very efficient in separating main components and categorize from a training base;
- Artificial neural networks (ANN), also known as universal classifier, since its architecture is very suitable to address changes in pattern classification of network traffic rules;
- Latent Dirichlet Allocation (LDA), applied for inference over log database [Lee et al. 2018], with text processing and identification of digital signatures by using Natural Language Processing (NLP).

These techniques are more appropriate and efficient for high-volume traffic because they statistically learn the pattern classified as normal behavior. The accuracy of these techniques depends on the number of available log samples on the database: the more significant the log database, the more effective the algorithm is in detecting misbehaving in local traffic. As an example of a massive high traffic situation, we have attacks known for using brute force to generate denial service (DoS) situations with as many as possible distributed sources. All methods mentioned above are still sufficient to detect DoS traffic but unsuitable in a low traffic scenario with just a few volumes of discrete traffic, easily characterized as usual by administrators.

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. For the purpose of demonstrating the low impact of the Radnet protocol, low-intensity traffic was simulated that could go unnoticed if we were to use only traditional techniques. Known as Low Denial of Services attack this kind of malicious behaviour It can be used to simulate the traffic protected by net radio as it maintains the same characteristics of low packet transmission rate and low data volume in each transmission.

Fourier analysis is a way to implement such low-rate traffic analysis, which is effective to determine which frequencies are the most significant independently of their occurrence. Another alternative is Short-Time Fourier Transform (STFT), which can determine the set of main frequencies in a given time. Therefore, to detect low-rate traffic with periodically transmission sources the correlation between malicious patterns could be associated with low frequencies, despite main traffic dispersion over the high frequencies spectrum.

The STFT approach has some downsides, such as the time it takes to execute, the precision to lock the right frequency associated with the source of attack, and the impossibility to get precision in time and frequency at the same time [Yan et al. 2019]. Authors in [Yan et al. 2019] and [Wu et al. 2018] indicate the use of wavelet algorithms to detect low-rate traffic because of the ease to stretch and compress wavelet scale (scaling feature) to capture low frequencies (scaling down) or higher frequencies (scaling up), whilst the wavelet base slides over time to precisely track the time when the most significant frequencies are detected. Indeed, in terms of mitigation effort against a DoS attack, time is crucial to successfully protect either services or infrastructures.

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.

In recent years, a new type of attack called Low-rate Denial of Service (LDoS) [Zhang et al. 2019a, Yan et al. 2019, Wu et al. 2018] has emerged as a new category in which a malicious user can directly affect critical parts of network infrastructures, such as SDN controllers (within control plane), data center resources, log servers, among others. According to [Zhang et al. 2019a], this type of attack is characterized by low traffic rate and periodically packet bursts (usually TCP) with relatively low average value, what leads to a minimal impact to the total traffic at the end of the day. This characteristic implies a non-adherence to ML common algorithms mentioned before, once those methods depend on the profile of a huge amount of collected data.

Many works have applied a bunch of ML methods to analyze low-rate traffic in the middle of network services to detect and prevent malware, seeking for the presence of any malicious or suspect behavior. Different performance levels were obtained with different techniques, however, analysis of the spectrum of principal frequencies [Zhang et al. 2019b] applied to detect low-rate traffic is proving to be a good candidate to detect anomalous events, which revels misbehavior associated with network attacks.

More information about wavelet transformation can be found in [Stéphane 2009].

3.1 Types of Attacks

In this work, we represented some possibilities to attack infrastructure protected by Radnet and we proposed three types of test just to check the capacity of Radnet to absorb impacts and provide resilience to the application supported by it. The goal of each proposed scenario is to produce overload over infrastructure protected by Radnet protocol. Either using force brute attack like DoS and scanning or intelligent eavesdropping technique, we aim to show the robustness and resilience possible to obtain through Radnet implementation. In order to clarify the results, we describe each attack and how they were designed.

3.1.1 Scanning attack

Many types of tools can be used to attack internal infrastructure checking for vulnerabilities available to exploit by using malwares and others resources in order to appropriate of critical information or even to block services and affect infrastructure of providers of several orders. Most use it tool and known by community is NMAP. By using this one could start a process of reconnaissance to detect the possibilities to explore the Environment.

3.1.2 Eavesdropping

In the case of a penetration from external network had happened to the infrastructure one could check by using probe just like a sniffer application to check the information transmitted into the environment of a local network. Again one strategy based on obfuscation could help to protect critical data add mitigate the impact from one invasion of this nature.

3.1.3 Low-Rate traffic

The most common and known attacked based on denial of service off the infrastructure involve large amount of packets in order to over process the resources of a service provider. but in some cases low -rate malicious traffic could affect in the same away the local infrastructure but without disturb the local environment so traditional tools like IDS could not that act the disturbance generated by this kind of flow. in this case one technique based on advanced analysis of the frequence of the local traffic is more indicated and, this work will suggest a test using wavelet method to provide visibility of this situation.

Network traffic's main characteristics are non-stationary signals with significant variations in time due to tendency and repetition periods but without stationary moments observed. Therefore, we consider using a scalogram form to represent components of non-stationary signals with significant variations in time. When a network asset is under the influence of any abnormality, it is possible to detect average profile variations with no visible pattern modification, especially for low-rate flows. Scalogram applied to intrusion detection methods allows us to associate attacks to some detectable variables:

- Impacts in terms of throughput: which component has more impact in terms of packets per seconds;
- Hidden components of traffic: It is possible to identify which components are present and trigger an alarm;
- To this work, the default wavelet function used to compute the transform was $CGAU1$ (Complex Gaussian wavelets). We observed that Morlet's wavelet delivers better results considering the input data.

3.2 Clean-Up data

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.

$$\begin{aligned} S_t = \alpha \big[Y_t + (1-\alpha) Y_{t-1} + (1-\alpha)^2 Y_{t-2} + \cdots \\ \cdots + (1-\alpha)^k Y_{t-k} \big] + (1-\alpha)^{k+1} S_{t-(k+1)} \end{aligned} \tag{1}$$

Next, Data Cleaning step is essential to make easier 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 [Di Bella et al. 2007], 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 previously benchmark. Hence, the processing to generate wavelet coefficients and the graphic output become smooth due to the data optimization process of CBPF traffic and the elimination of outliers.

Moving forward in our analysis methodology, we find the final step to process information from scratch: generation of Continous Wavelet Transform (CWT) and the graphical representation of the traffic under analysis, using scalogram tool to provide a visual representation of the results (further references about this method in the next session) . Figure 5 depicts each step mentioned before of the methodology we use in our analysis.

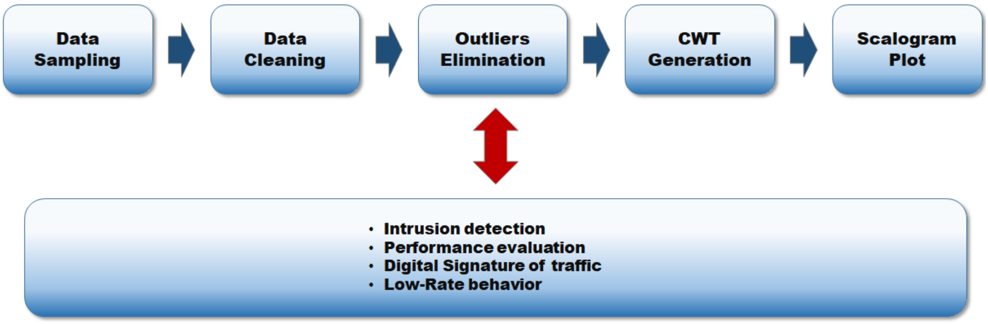
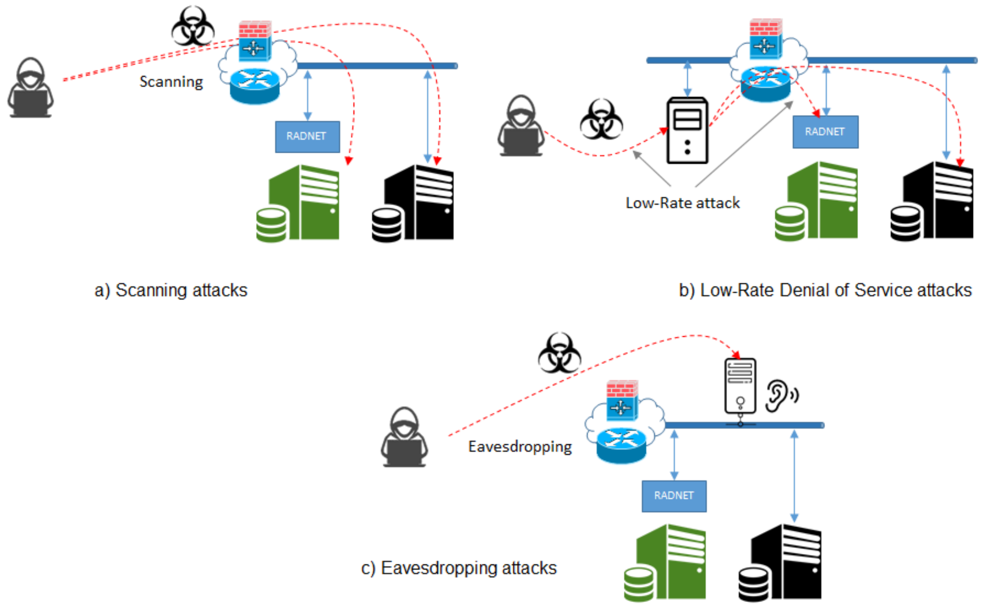


Figure 5: Representation of the methodology used in this work: data extraction from network, data cleaning and wavelet processing to detect abnormalities

4 Proposal analysis and discussion

As we mentioned in Section 2, with Radnet it is possible to hide any server in a network without using IP based addressing. This hidden status allows servers to communicate with each other through broadcast flow in a total stealth mode. Hence, in such a context, Radnet has advantages against the majority of cyberattacks, which relies on IP address to be performed. In fact, the attack will not succeed, only being possible if the attacker knows and has access to the physical location of the server. Figure 6 presents the way we address the attack protection problem with Radnet traffic evaluation.



a) Scanning attacks

b) Low-Rate Denial of Service attacks

c) Eavesdropping attacks

Figure 6: Representation of how methodology can be applied to prevent attacks with DoS characteristics applying sniffer, log analysis and wavelet to process spectral profile of the traffic. *a*): This step specifies the knowledge one attacker could extract from scanning the infrastructure in a *reconnaissance* process . Our experiment sampled log traffic between nodes (represented by gateway server) and log server, protected by Radnet protocol. *b*): Represents one compromised element internal to network under analysis. As mentioned before, log traffic in CBPF's network presents characteristics of low-rate average throughput and low frequency. *c*): Conclusions after analyzing data by applying eavesdrop method, such as sniffing a specific segment of the network: evaluation of traffic sampled (log with Radnet protection) or performance impacts due to overload of data transmitted or signature generation of the traffic analyzed.

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

To evaluate possible impacts caused by our approach, we adopted the following metrics to monitor its behavior: number of data packet in different queues, such as arriving packets, number of output packets, number of broadcast packets, number of packet errors, CPU consumption impact, system memory demanded and number of packet drops. To avoid installing our protocol stack in sensitive elements running in 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 storage the logs sent by other nodes.

We can observe the impact of the Radnet on CBPF infrastructure in the following ways: (*i*) by analyzing traffic patterns; and (*ii*) by checking the impact on users applications and services. The former is not efficient since traffic patterns might not significantly change, and the latter is not recommended, given that we do not want any kind of interference on corporate networks. To address the inherent challenges in traffic patterns analysis, we consider three assumptions:

1. Radnet might generate a huge amount of data that will significantly change CBPF traffic profile. In this case, we may apply one of the detection methods for DoS situation, since the change caused will be the increased volume of packets/seg. We propose to apply an universal pattern recognition algorithm just like an ANN, recognizing the difference in traffic profile based on a historical database of the traffic monitoring process. Alternatively, one could try for better results applying a different algorithm (i.e. SVM as mentioned before). 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. Figure 10 demonstrates a typical traffic collected from CBPF network over the last six months, with Radnet service disabled. We can see a normal broadcast with average behavior as expected for a network with

such size. 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 to such as CPU, system memory and others. And that exceeding consumption could lead the whole environment to a situation of exhaustion and compromise services and performance of users in general. Tests and collections of SNMP and logs will demonstrate how valid is this assumptions and, according to expectations of the authors, no impact could be detected even with Radnet implemented to fully protect the communication between nodes of the CBPF's nodes.

3. Radnet may produce increasingly low-rate traffic that would not be possible to detect 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 CBPF environment, simply due to its potential low impact probability. In fact, by using broadcast to keep the information within protected channel hidden, and only that, 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 normal working days. To validate this hypothesis we proceed to assume two assumptions then check them out with real measurements:

    - Since logs are commonly sent in periodic bursts of data, Radnet would have the same behavior, like a periodic low-rate pulse. In this case, it could be detected through a principal components analysis of the traffic using Morlet wavelet, illustrated in Figure 7
    - Radnet may be detected as an incremental broadcast component and malicious users could notice it as normal traffic without additional interest to inspect more details about.

Therefore, a good way to verify if the Radnet traffic is significant to compromise network resources, we apply the methods described before to analyze the digital spectral of signal formed by the broadcast traffic of the Radnet protocol. This way, it is possible to determine the assertive influence of this hidden service over the whole network from the specific perspective of the broadcast component. Indeed, all communication between Radnet server and the network elements that are sending logs are made through broadcast packets. So, we can take both spectrum of the total traffic of the service and spectrum of the communication created by network elements with Radnet server. Comparing these two frequency domains could allow to detect how significant is the later inferring how impactful Radnet is on the performance of CBPF's network.

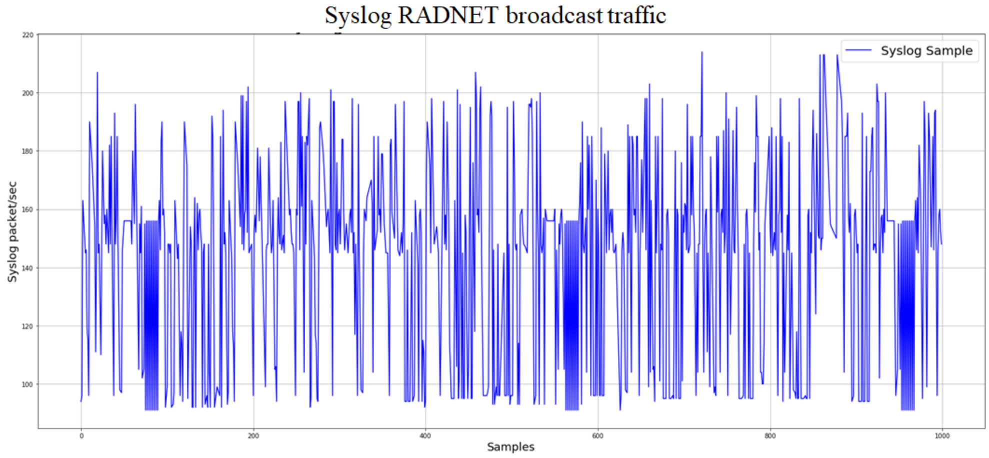


Figure 7: Syslog traffic sample: Syslog is the service covered by Radnet protocol and that is why its pattern is very important for further analysis

Figures 8 and 9 show how the traffic service and specific broadcast were not impacted with Radnet being used to protect Syslog between server and gateway servers. We couldn't identify any disturbing provoked by obfuscation process due Radnet implementation. Others variable also were not impacted, as we can see in the further figures.

As we can check by analyzing the graphics is that performance wasn't affected by the use of Radnet to protect the Syslog service. Neither any infrastructure aspect was significantly affected (CPU, free memory, the throughput of interfaces, for example) nor user's experiences showed any disturbing related. All measurements indicate that Radnet doesn't compromise the environment as expected. However, we investigate in more detail using the wavelet technique (as described further) to confirm in other ways our impressions about the results. The throughput of broadcast didn't change with the application of Radnet to the transport of Syslog protocol. As we couldn't notice any deviation, we also will observe that amount of packets corresponding to the Syslog service kept its own tendency of growing as the demand from users was growing over the time we applied the collection and observation process. CPU consuming off the nodes also keeps on track which means we can't note anomalous Behavior as a result of Radnet utilization. Memory allocation behaved as expected for the observed traffic. Despite the positive aspect

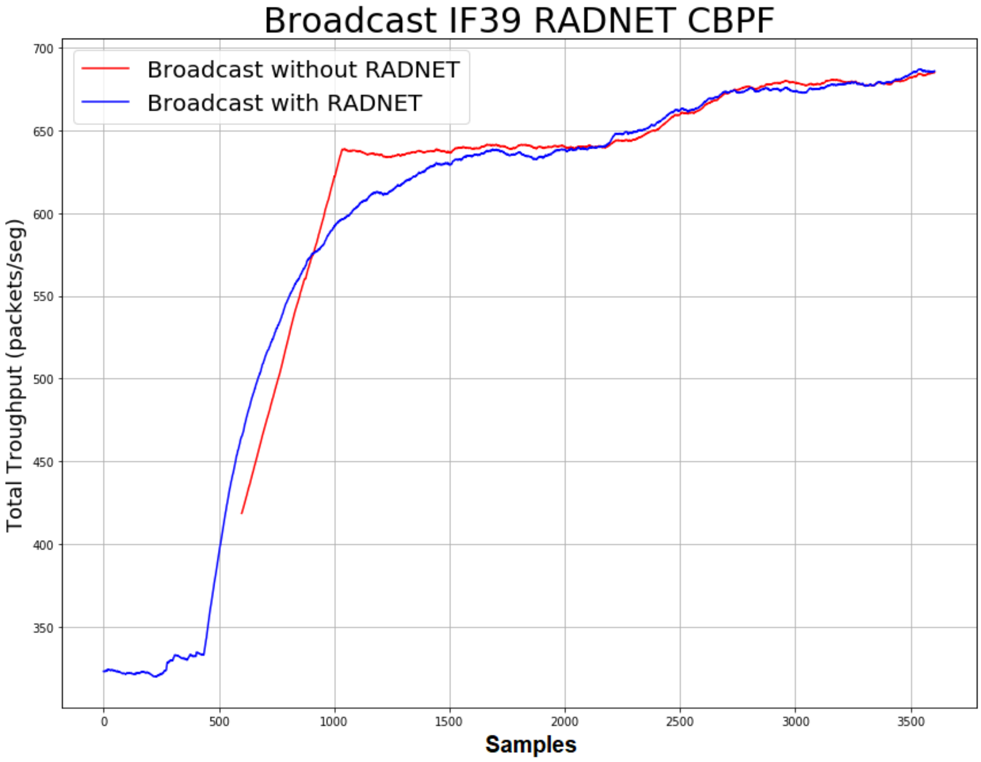


Figure 8: No impact on broadcast traffic due Radnet protocol over the CBPF network

of this scenario, this situation could bring a specific problem in terms of anomalous detection since the traffic profile of syslog servers represents a low charge on the network and a lower chance to detect any attack with the same characteristics. Low-rate denial of service attacks could not be detected the same way.

Figure 10 demonstrates the analysis of total traffic in CBPF environment (for now on we will adopt the term signal to represent traffic analysis in wavelet technique) using wavelet technique. Morlet wavelet is able to capture and brakes down the frequency components over the time, plotting its amplitude, or individual energy, or, in our situation, packets per second. This method simultaneously vary the width of the sample window and the position of the window in time. The broader the window is the more lower frequencies of the signal are identified. On the other hand, short sample window will detect the higher components of the same signal, therefore composing the complete spectrum analysis. Plotting this distribution of frequencies over time sampling is known as scalogram graphic [Stéphane 2009]. It is a useful method to intuitively take a glimpse of belief about the dynamic relationship

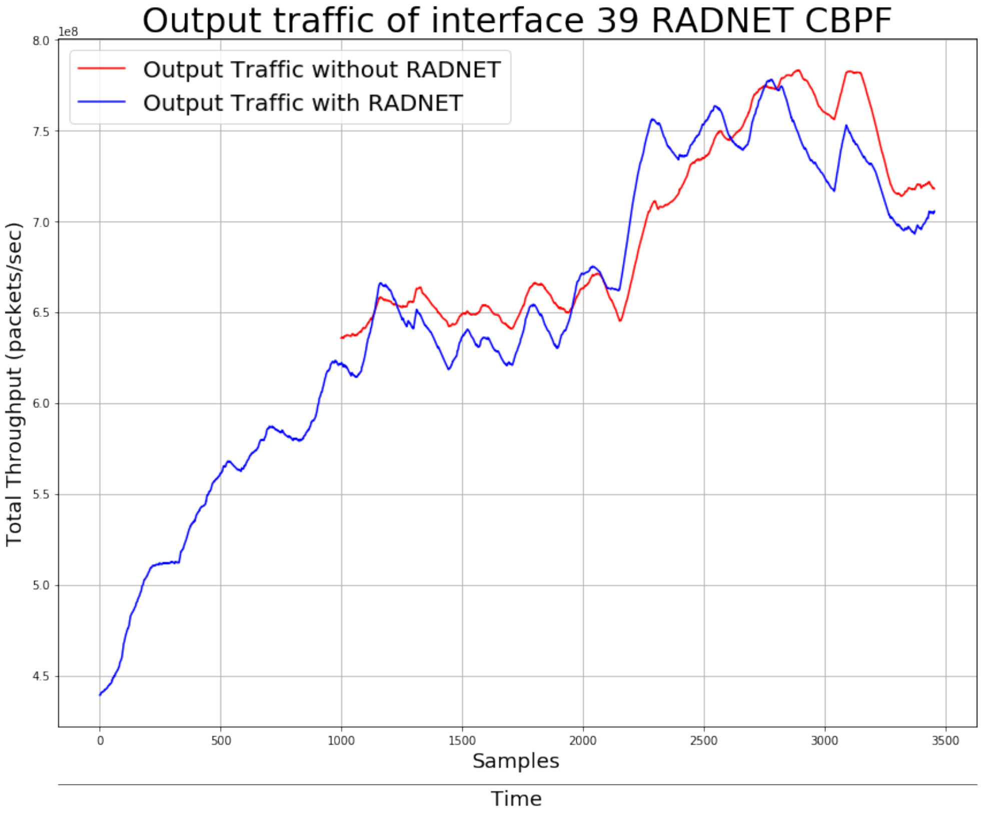


Figure 9: General results of Radnet protocol: Traffic without any impact due Radnet protocol

of traffic and its components. Different colors indicates the amplitude range, so as more intense in terms of impact (or traffic intensity) are close to red, otherwise lower impact are close to blue.

For this work, we adopted the Python library called PyWavelet [Lee et al. 2019] which makes it easy to construct the scalogram of any time series. Once we set window variance to consider the fundamental frequencies range, each component's impact can be determined. Figure 12 shows the scalogram of Radnet 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

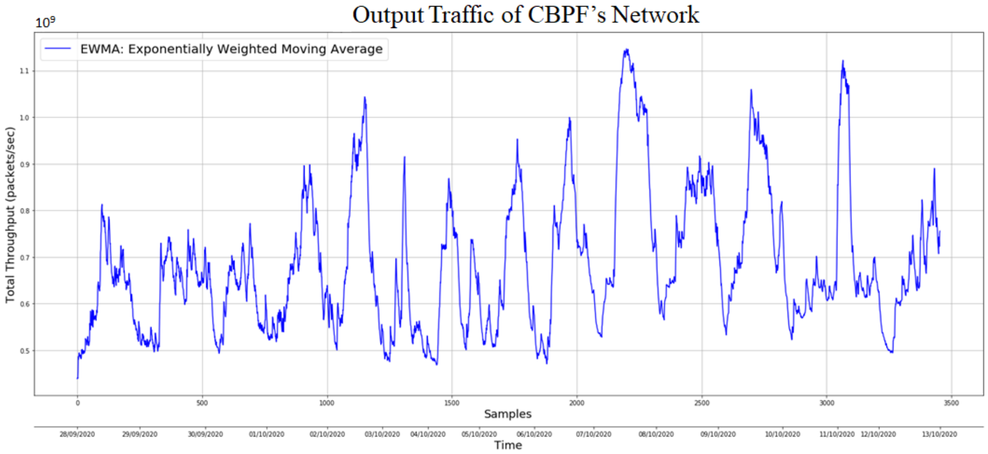


Figure 10: Sample traffic of CBPF network: sample of all local services during a normal day traffic. This graph shows the profile of utilization tagged as normal for further analysis

We demonstrate the efficiency of the wavelet method to detect possible attacks of LDoS by adding a synthetic low-rate attack in CBPF network. We monitor and collect all traffic of the interest network interface. Figure 11 shows the synthetic signal and its respective scalogram. The effect of this attack on the CBPF normal traffic can be visualized in Figure 12. The attack components and the impact in throughput over all the infrastructure are noticeable, while the average attack traffic is relatively low, which can lead conventional detection methods to miss such an attack.

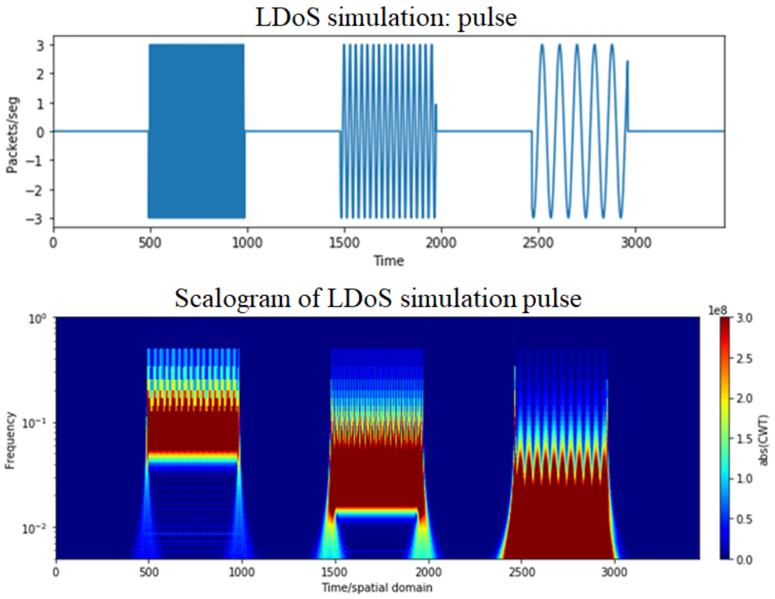


Figure 11: Synthetic attack using LDoS method: in this case, three different frequencies were used to simulate a real LDoS attack, which pattern is variants low frequencies and low average intensity

5 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 can 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 the critical service to be protected. We showed through wavelet analysis that Radnet does not impact the network's performance with any overload or overhead in the broadcast flood. Moreover, we also presented how wavelets can be applied to efficiently identify LDoS attacks.

As future works, we propose to expand Radnet to other critical components such as DNS servers and AAA/DHCP services to analyze the behavior of the protocol 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

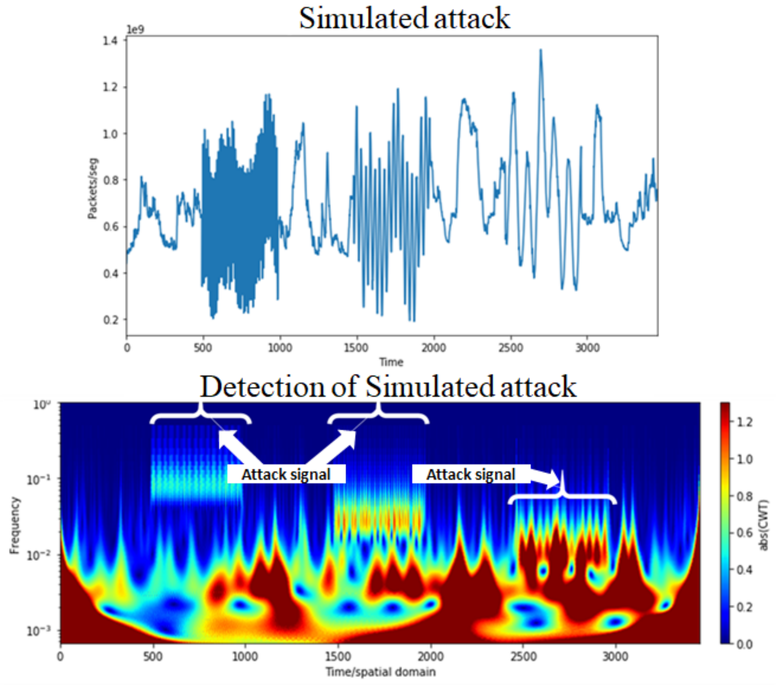


Figure 12: Attack result and detection using CWT according to the described method. The pattern of attacking traffic is clearly differentiated from normal service traffic with expected and known behavior

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

[Almaini et al. 2020] Almaini, A., Al-Dubai, A., Romdhani, I., Schramm, M., and Alsarhan, A. (2020). Lightweight edge authentication for software defined networks. *Computing*, pages 1–21.

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

[Chaum 1981] Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–90.

[Di Bella et al. 2007] Di Bella, A., Fortuna, L., Graziani, S., Napoli, G., and Xibilia, M. G. (2007). A comparative analysis of the influence of methods for outliers detection on the performance of data driven models. In *2007*

IEEE Instrumentation Measurement Technology Conference IMTC 2007, pages 1–5.

[Dutra et al. 2012] Dutra, R. C., Moraes, H. F., and Amorim, C. L. (2012). Interest-centric mobile ad hoc networks. In *2012 IEEE 11th International Symposium on Network Computing and Applications*, pages 130–138.

[Fernandes et al. 2019] Fernandes, G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., and Proença, M. L. (2019). A comprehensive survey on network anomaly detection. *Telecommun. Syst.*, 70(3):447–489.

[Houmansadr et al. 2013] Houmansadr, A., Brubaker, C., and Shmatikov, V. (2013). The parrot is dead: Observing unobservable network communications. In *2013 IEEE Symposium on Security and Privacy*, pages 65–79.

[Jafarian et al. 2012] Jafarian, J. H., Al-Shaer, E., and Duan, Q. (2012). 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, page 127–132, New York, NY, USA. Association for Computing Machinery.

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

[Lee et al. 2019] Lee, G. R., Gommers, R., Wasilewski, F., Wohlfahrt, K., and O'Leary, A. (2019). Pywavelets/pywt: Pywavelets v1.0.3.

[Lee et al. 2018] Lee, S., Kim, S., Lee, S., Choi, J., Yoon, H., Lee, D., and Lee, J. (2018). Largen: Automatic signature generation for malwares using latent dirichlet allocation. *IEEE Transactions on Dependable and Secure Computing*, 15(5):771–783.

[Lima et al. 2018] Lima, L., Filho, P. C., Dutra, D. L. C., Amorim, C. L., Macedo, E. L. C., Silva, R. S., Coutinho, M. A., and de Moraes, L. F. M. (2018). 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.

[Major et al. 2020] Major, W., Buchanan, W. J., and Ahmad, J. (2020). An authentication protocol based on chaos and zero knowledge proof. *Nonlinear Dynamics*, pages 1–23.

[Meisel et al. 2010] Meisel, M., Pappas, V., and Zhang, L. (2010). Ad hoc networking via named data. In *Proceedings of the fifth ACM international workshop on Mobility in the evolving internet architecture*, pages 3–8.

[Mekinda et al. 2018] Mekinda, L. et al. (2018). 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*, number 16 in International Conference on Accelerator and Large Experimental Control Systems, pages 1142–1148, Geneva, Switzerland. JACoW. https://doi.org/10.18429/JACoW-ICALEPCS2017-THBPA02.

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

[Park et al. 2017] Park, J., Noh, J., Kim, M., and Kang, B. B. (2017). Inviserver: Reducing the attack surfaces by making protected server invisible on networks. *Computers & Security*, 67:89–106.

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

[Stéphane 2009] Stéphane, M. (2009). Chapter 4 - time meets frequency. In Stéphane, M., editor, *A Wavelet Tour of Signal Processing (Third Edition)*, pages 89 – 153. Academic Press, Boston, third edition edition.

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

[Wu et al. 2018] Wu, X., Tang, D., Tang, L., Man, J., Zhan, S., and Liu, Q. (2018). A low-rate dos attack detection method based on hilbert spectrum and correlation. In *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pages 1358–1363.

[Yan et al. 2019] Yan, Y., Tang, D., Zhan, S., Dai, R., Chen, J., and Zhu, N. (2019). Low-rate dos attack detection based on improved logistic regression. In *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 468–476.

[Zhang et al. 2019a] Zhang, D., Tang, D., Tang, L., Dai, R., Chen, J., and Zhu, N. (2019a). Pca-svm-based approach of detecting low-rate dos attack. In *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 1163–1170.

[Zhang et al. 2019b] Zhang, D., Tang, D., Tang, L., Dai, R., Chen, J., and Zhu, N. (2019b). Pca-svm-based approach of detecting low-rate dos attack. In *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 1163–1170.

[Zhang et al. 2014] Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., claffy, k., Crowley, P., Papadopoulos, C., Wang, L., and Zhang, B. (2014). Named data networking. *SIGCOMM Comput. Commun. Rev.*, 44(3):66–73.