Journal of Cyber Security
DOI: 10.32604/jcs.2022.027524
Article

Tech Science Press

Adaptive Polling Rate for SNMP for Detecting Elusive DDOS

Yichiet Aun*, Yen-Min Jasmina Khaw, Ming-Lee Gan and Vasaki Ponnusamy

Faculty of Information Communication and Technology, Kampar, 31900, Malaysia
*Corresponding Author: Yichiet Aun. Email: aunyc@utar@edu.my
Received: 05 March 2022; Accepted: 08 April 2022

Abstract: Resilient network infrastructure is pivotal for business entities that are growing reliance on the Internet. Distributed Denial-of-Service (DDOS) is a common network threat that collectively overwhelms and exhausts network resources using coordinated botnets to interrupt access to network services, devices, and resources. IDS is typically deployed to detect DDOS based on Snort rules. Although being fairly accurate, IDS operates on a compute-intensive packet inspection technique and lacks rapid DDOS detection. Meanwhile, SNMP is a comparably lightweight countermeasure for fast detection. However, this SNMP trigger is often circumvented if the DDOS burst rate is coordinated to flood the network smaller than the SNMP polling rate. Besides, SNMP does not scale well if the poll rate is set extremely fine for improved detection accuracy. In this paper, a lightweight 3D SNMP scaling method is proposed to optimize the SNMP poll rate for DDOS mitigation automatically. The 3D-SNMP uses horizontal scaling to dynamically adjust the optimal poll rate through random packet inspection that is selective. Suppose a sign of DDOS is detected, 3D-SNMP scales down the poll rate for finer detection. As DDOS subsides, 3D-SNMP scales the poll rate up for faster DDOS detection. The equilibrium between scalability and accuracy is determined on the fly depending on the types of DDOS variants. 3D-SNMP also adds a vertical scaling to detect non-salient DDOS that falls below the detection threshold. The experimental results showed that 3D-SNMP achieved DDOS detection of 92% while remaining scalable to different DDOS variants and volumes.

Keywords: SNMP; DDOS; poll rate; network security; threat detection

1 Introduction

Distributed Denial-of-Service (DDOS) is becoming more prevalent and targeted to disrupt continued operation in a world in which cloud computing start to dominates. DDOS uses a collection of botnets to flood some target of interests to exhaust remaining available network resources and bandwidth [1]. A few DDOS variants depend on attack types, such as ICMP flooding, SYN flooding, and UDP flooding [2]. Botnets, infected or dedicated, systematically generate ICMP or TCP requests traits in large volume to overwhelm the target's network buffer or compute resources [3]. These traits made DDOS somewhat more deterministic and are easily detectable using existing security countermeasures. Despite that, DDOS remains essentially disruptive since countermeasures like IDS and Firewall, which operate on rules matching, lack rapid detection due to heavy computing needs [4]. The delay in detection (timeliness) presents a vulnerable point for service denial before detection and mitigation. Meanwhile, SNMP is a lightweight approach to DDOS detection that evaluates bandwidth and compute utilization behavior [5]. SNMP can be programmed to raise a flag when a certain pre-defined threshold of resources is over-utilized in a short time frame [6]. In Metasploitable DDOS framework allows changing the burst size to a value smaller than the SNMP polling rate. As a result, SNMP becomes leaky and is prone to high true-negative when DDOS is programmed to circumvent the pre-configured polling rate [7].

Behavioral analytics and event-based monitoring are comparably more popular in DDOS detection for their contextual intelligence, but not without compromises [8–10]. Intrusion Detection System (IDS), like **SNORT**, uses rules-based filtering to check packet header for possible UDP/SYN/ICMP flooding in TCP flags. However, IDS is compute-intensive and is less effective on encrypted traffic. Meanwhile, **Netflow** is built into some Cisco network devices to monitor traffic flows for DDOS alike threats. However, Netflow often struggles to handle large traffic influx and is less effective for real-time DDOS detection. Cisco also designs Syslog to capture malicious traffic, but it is somewhat limited to the device to device communications. In [10–12], multiple machine learning trained models using SVM and GAN are proposed for threat intelligence. However, ML models are trained on synthetic data, making them difficult to generalize to fit heterogeneous network contexts [9,13].

This paper is organized as follows. In Section 2, some prominent DDOS detection methods are compared. In Section 3, the architecture of the proposed 3D-SNMP is discussed. The experimental setup, results and findings are demonsrated in Sections 4 and 5. Lastly, we conclude the findings and highlight the novelty of 3D-SNMP in Section 6.

2 Related Works

2.1 Detecting DDOS with SNMP

The distributed denial of service (DDOS) attacks are illegitimate traffic flows generated to overflow target hosts or destination networks. DDOS is commonly performed using SYN/UDP/ICMP flooding through the Metaspoitable framework [2]. Many types of DDOS detection are designed for early DDOS detection, but not without their pros and cons [4]. In this section, we compare some of these methods to using SNMP for DDOs detection.

SNMP protocol is a monitoring protocol that works on the application layer. SNMP is used to monitor a device condition, change the parameters of a device, detect an event failure, generate alarms, and report for the administrator for troubleshooting [1]. There are three main components SNMP agent, SNMP server, and Management Information Base operating together to monitor the network. An SNMP agent referred to the program or software running on the SNMP-enabled network devices, including printers, routers, switches, and computers. They are in charge of collecting data such as bandwidth, CPU usage, or disk space and sending this information to the SNMP server when it received the SNMP server's request. An SNMP server is software deployed on a server and functions as a central collector to the SNMP agents. The SNMP manager collects information on the network devices by querying a request to the SNMP agent to reply with the data requested. The Management information base is a database that resides in the SNMP agents and has a collection of objects about a particular device. MIB stores the data in a tree-like structure hierarchy to eliminate network devices' burden to exchange data in a rigid format. The objects can be queried and controlled by the SNMP. A MIB [14] can have many objects inside, so each of the objects is assigned with OID's unique identifier.

The SNMP protocol uses several types of messages to communicate between network devices and the management system that referred to SNMP agent and SNMP manager. The main benefit of SNMP is that it can support and manage devices from different vendors. SNMP uses a non-proprietary protocol so that it is not limited to support only specific vendor devices [8]. Next, SNMP allows the network administrator to configure specific parameters on the network to be managed automatically. This can save time for constantly checking on the system since the SNMP can automatically generate an alarm when the parameters' thresholds are exceeded [5].

However, SNMP is vulnerable to 'bursty' DDOS variants designed to circumvent the fixed threshold configured as SNMP triggers. Attackers used burst attacks to get around SNMP-based detection systems; by reducing the attack length rather than the traffic levels or volumes. Consider a router connected to a 1 Gbps downstream internet connection. When the total ingress bandwidth exceeds 900 Mbps (as defined in the threshold), the SNMP detector will detect volumetric attack events based on a threshold (90 percent utilization). Now consider a single burst, part of a more powerful burst attack, of 10 s at the whole saturation level (100% utilization). Such attack burst will not be detected as a saturation level event since SNMP calculates the average utilization over a polling period (for example, the total bandwidth used over 30 s). A short but saturated burst will not add significantly to the average bandwidth use; thus, SNMP is blind to such burst attacks unless the total bursts cumulatively add to an average that triggers the alarm (exceed the threshold).

2.2 Other DDOS Detection Methods

An **intrusion detection system** is deployed to monitor the network traffic for malicious activities and generates alarms when a significant event has occurred. An IDS can collect information ranging from a single computer to a network. An IDS operates based on four stages of functions. The first function is data collection [8]. In this stage, data flows are captured into IDS as input and then analyzed. The second function is feature selection which the IDS will choose particular features from extensive data to be evaluated since not all features are needed for the analysis. Next, in the analysis stage, the IDS started to analyze the data to determine traffics' legitimacy. Classification of IDS can be divided into Network-based IDS, Host-based IDS, and Hybrid-based IDS [15,16]. Intruders trigger an alert if changes in files include file creation, deletion, and modification. During a DDoS attack, the connection table will be used quickly because a new connection will be opened in the connection table for each malicious packet. Once overflowed, the legitimate user will not establish new connections, thus further congesting the network [17]. Besides, an IDS is limited because they cannot process a packet that is encrypted. If attackers encrypt their packet before sending it into the network, it can easily bypass the IDS [18].

Netflow is a Cisco proprietary protocol that allows the network administrator to collect and record down IP analyzer. Netflow data would show anomalies if any changes occurred in the network behavior. However, sending Netflow data can add too much overhead to the router and switch, overloading the infrastructure, resulting in stopping engineers from enabling Netflow on their network. Besides, Netflow is limited to show routed traffic or packets. This is because flow data is captured as the packet pass through the network devices. Any packets inside the internal LAN and VLAN are not visible to Netflow.

Syslog is a protocol used by network administrators to monitor events in the network. Network devices do generate logs about the events and their status. Syslog cannot pollute devices to collect the information as the SNMP messages are sent only when a specific event is triggered. Compared to SNMP, Syslog logged messages using UDP transport protocol. This means Syslog does not guarantee the messages can be arrived at the receiver due to network congestion or packet loss. Finally, Syslog message exchange is not secure since there is no authentication on the messages. This means an attacker can masquerade a legitimate machine to send forged log events and run replay attacks. Tab. 1 below summarizes and compares some popular DDOS detection methods [15].

Table 1: Comparing some popular DDOS detection methods

DDOS detection methods	Advantages	Disadvantages
Intrusion detection system	1. Able to monitor specific packet content. 2. Able to detect an unknown attack.	1. Unable to monitor encrypted packet. 2. Generate huge number of false alarms.
CISCO IOS NetFlow	1. Able to detect attacks in a real-time environment.	1. Too much overhead. 2. Limited to monitor routed packet.
Syslog	1. Ability to recover a system previous state. 2. No direct performance impact on a monitoring system.	1. No authentication on log messages. 2. Unreliable transport of log messages.
Simple network management protocol	1. It uses a non-proprietary protocol. 2. Manage certain parameters network automatically	1. Limited network details required for troubleshooting

3 3D-SNMP Architecture

This section introduces the adaptive 3D-SNMP (see Fig. 1) that uses dynamic poll rate scaling architecture to combat bursty DDOS attacks. At the ingress, traffic flows (DDOS and standard) are classified into SYN flows, RST flows, ICMP flows, and expected flows using Netflow. These classified flows are then piped into two components: (a) traffic sampler and (b) SNMP-DDOS monitoring. In (a), traffic flows lasting 10-s are selectively sampled at every 60-s interval compared with DDOS trigger baseline (rule-based detection). In (b), all traffic flows are sent to the SNMP monitoring for DDOS detection based on bandwidth over-utilization.

The main detection module is as illustrated in the 'SNMP-DDoS component. SNMP-DDoS employs statistical SNMP-MIB that are useful for DDOS detection from 4 MIB groups, like {*'icmpOutMsgs', 'icmpInMsgs', 'icmpOutDestUnreachs', 'icmpInDestUnreachs', 'icmpOutEchos', 'icmpInEchos', 'tcp', 'udp', 'interface', 'ip', 'tcpIn-Errs', 'udpNoPorts'*} etc. The SNMP detector is set to periodic flow polling of one minute (cold start; $time\ t = 0;\ pollrate = 5\,s$). Using rule-based trigger, the SNMP detector compares flow characteristics derived from SNMP-MIB with triggerDB to filter SYN/RST types of flooding. SNMP-detector also detects volumetric attack events based on a threshold, Th (we set Th to <90% bandwidth utilization). There are two sliders in SNMP-DDoS, that is (1) horizontal scaler and (2) vertical scaler. The horizontal scaler corresponds to the polling rate, which is the frequency of traffic being sampled for DDOS detection. The vertical scaler corresponds to the optimal threshold, which is adaptively scaled to detect low-impact DDoS hogging bandwidth but not significant enough to trigger any red flags.

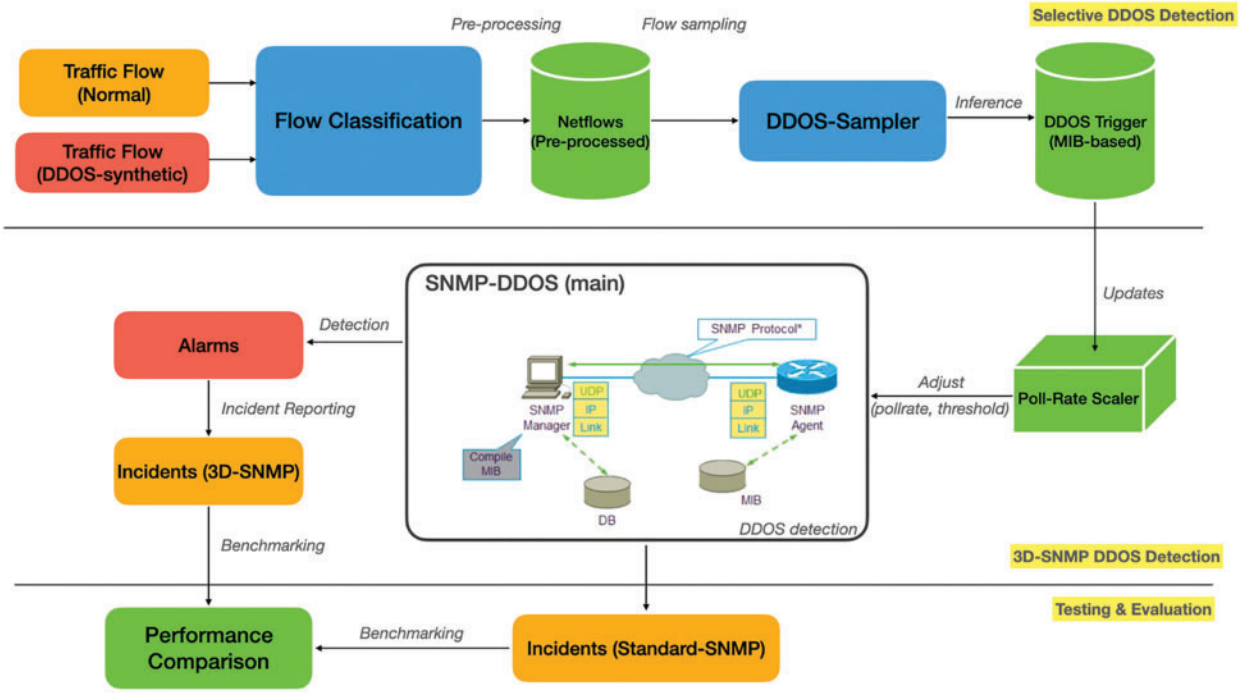

Figure 1: The 3D-SNMP architecture

Meanwhile, the '***sampler'*** component periodically checks traffic flows at a fixed 60 s interval to check for any indicative DDOS signs. The ***sampler*** is a rule-based method like any traditional SNMP method. The ***sampler*** is lightweight and only checks for a subset of traffic flows; it is not a replacement for SNMP-DDoS. The goal of ***the sampler*** is to regulate the poll rate of SNMP-DDoS (main detection) through the '***poll-rate scaler.'*** The intuition is that any bursty DDOS threats that DDOS-SNMP misses due to overly high poll rate can be flagged by a backup detection that will later inform the main engine to adjust the poll rate accommodatively. This means the ***sampler*** detect DDOS attack independently from DDOS-SNMP; and if detected, it raises a flag to reduce the polling rate of SNMP-DDoS to a smaller conversative value. After some period of non-detection, the ***sampler*** sends an update to SNMP-DDoS to scale up the poll rate to minimize compute through the ***poll-rate scaler***. The poll-rate scaler is a configurator that sets the poll rate interval in a .json file for adaptive polling-rate adjustment.

4 Experiment Setup

In this section, we shows the experimental setup to demonstrate the resillence of 3D-SNMP. Fig. 2 shows the DDOS attack architecture. We use Metaspoilt Framework (MSF) on Kali and hping to flood the target system (victim_x and victim_y). The proposed 3D-SNMP is configured on victim_x; while standard SNMP is configured on victim_y. All other DDOS preventives like Snort/IDS and Firewall are turned off. We set <90% bandwitdh utilisation to trigger *SNMP over-util* red flag and >10% spike on SYN/RST/UDP traffic compared to the baseline based on [7] (see Fig. 3).

We run *msfconsole* on Docker that spans across 40 machines for scalability reasons. These machines are equiped with 1 GBps interface running on a 1 GBps in/egress bandwitdh to commodity Internet. Prior to that, some network properties of ddos flows are transformed like replacing the original MAC and IP with a randomly generated pairs to bypass blacklisting mechanism at the endpoint or ISP level. Specifically, we use '*msf > use auxiliary/dos/tcp/synflood*' for SYN flooding, '*hping3–udp–flood*', '*hping3–icmp–flood*' to generate DDOS packets.

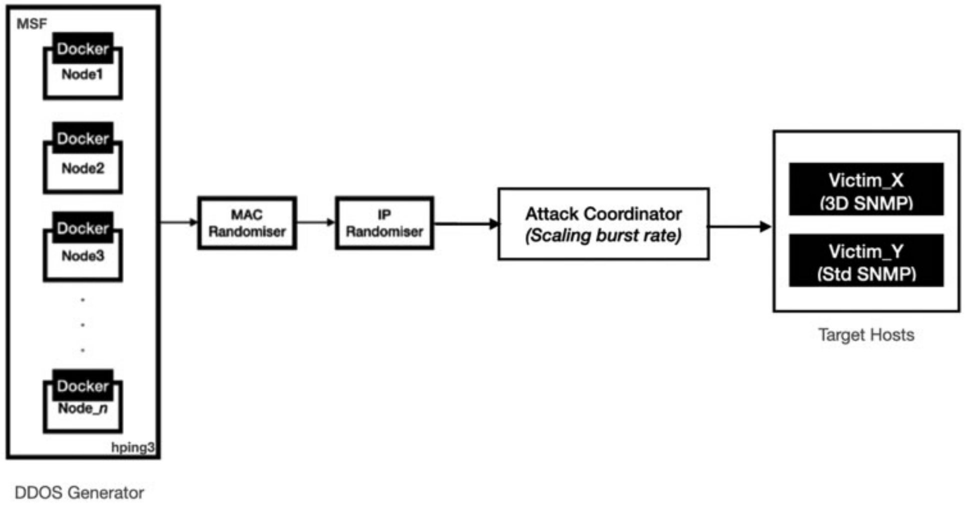

Figure 2: Attack architecture for generating DDOS

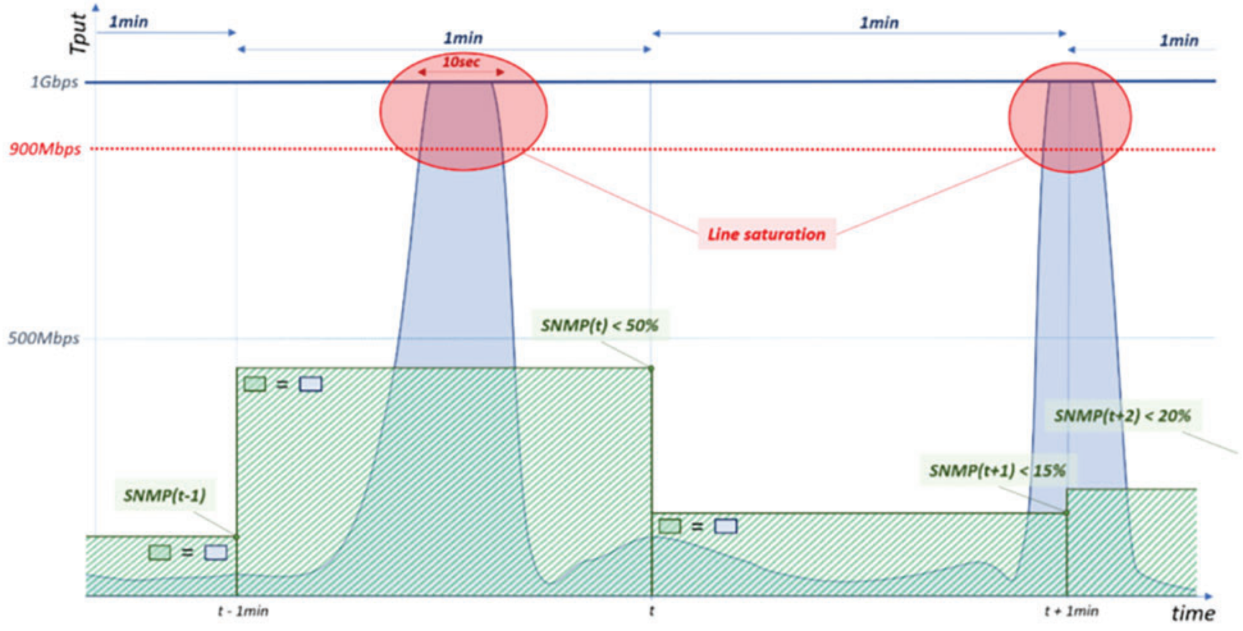

Figure 3: Missed classification of DDOS threats due to under-sampling in SNMP

We simulate two variants of DDOS attack patterns; which is systematically launched. In *experiment I*, we measure the accuracy of DDOS detection using different **sensitivity** level. We flood the victim machine using different DDOS rate to simulate variants of DDOS burstiness. We starts with a consistent periodic flooding with a sudden burst at fixed interval of 10 s (Fig. 4–Type A) to evade large SNMP poll rate. Then, we repeat the experiment with flooding burst at 30 s interval (Fig. 4–Type B).

Lastly, we repeat the experiment with inconsistent burst at random interval to test SNMP resilience in detecting DDOS (Fig. 4–Type C). In experiment II, we measure the accuracy of DDOS detection using different **alertness** level. We flood the victim host using scale-down DDOS that aims to hog the target network without exceeding the 90%_util threshold. Then, we compare the true positives and false positives of using 3D-SNMP (victim_x) and standard SNMP (victim_y) for DDOS detection.

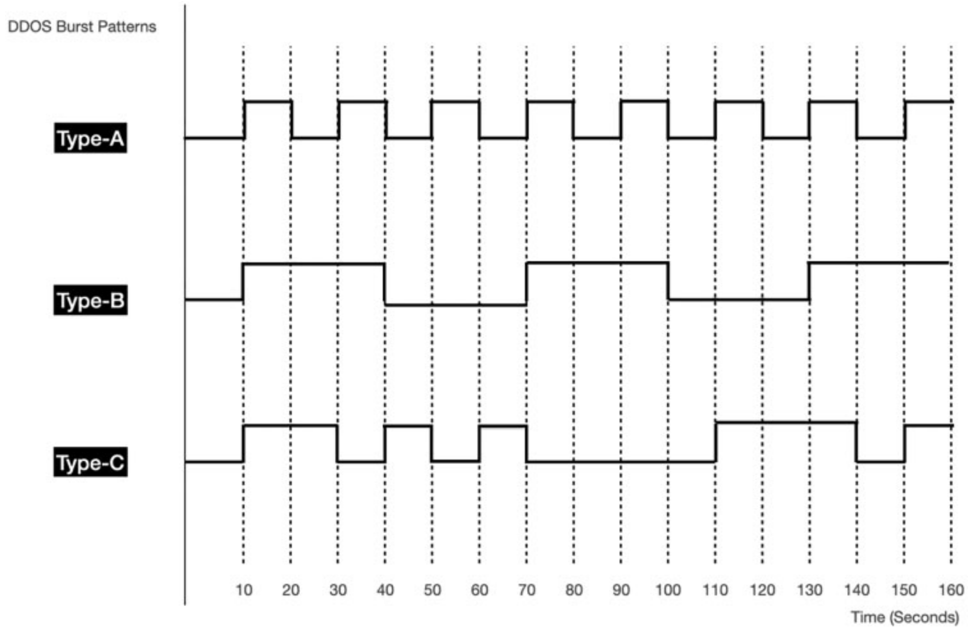

Figure 4: Three types of DDOS variants–Type A (short and bursty); Type B (long and consistent), Type C (random intervals)

5 Performance Evaluation & Findings

We measure SNMP's accuracy in DDOS detection using *True Positive Rate (TPr)* and *False Positive Rate (FPr)*. TPr and FPr is defined in the equations below.

$$TPr = TP/TP + FN \tag{1}$$

$$FPr = FP/FP + TN \tag{2}$$

where

$TP =$ *flow count of correctly identified DDOS traffic*

$FP =$ *flow count of normal traffic flows identified as DDOS*

$TN =$ *flow count of normal traffic flows identified as normal traffic*

$FN =$ *flow count of DDOS flows identified as normal traffic*

For context, we consider flows originated from SYN flooding, UDP flooding, and ICMP flooding as DDOS attacks. We measure TP as the number of identified {SYN flood/UDP flood/ICMP flood} flows over total {SYN flood/UDP flood/ICMP flood} flows. We choose to benchmark with TPr and FPr to measure the sensitivity and accuracy of SNMP detection. High TPr indicates accurate DDOS detection (*actual DDOS being detected as DDOS*). Meanwhile, low FPr indicates fewer false alarms (*non-DDOS traffic detected as DDOS*). A high TPr and low FPr is an indicator of resilient DDOS detection.

In experiment I, we evaluate the SNMP's DDOS detection accuracy using different sensitivity levels. Sensitivity is derived from SNMP's polling rate; for example, SNMP set to poll every 10 s has higher sensitivity than SNMP set to poll every 60 s. We compare five custom poll rates to the proposed automatically scaled poll rate in 3D-SNMP. The three types of DDOS attacks pattern is as described in Section 4. We added 50% off regular traffic (based on flow counts) as 'white noise. SNMP threshold is fixed at >90% of bandwidth utilization for all iterations. Tab. 2 shows the experimental results in terms of detection accuracy.

Table 2: DDOS detection accuracy (TPr, FPr) using different SNMP poll rates (tested on 3 DDOS variants)

DDOS variants	Sensitivity [Poll rate (s)]|Trigger: >90% BW usage									
	PR = 10 s		PR = 15 s		PR = 30 s		PR = 60 s		3D-SNMP	
	TPr	FPr	TPr	FPr	TPr	FPr	TPr	FPr	TPr	FPr
Type A	0.92	0.27	0.71	0.22	0.47	0.24	0.35	0.21	0.88	0.12
Type B	0.91	0.25	0.92	0.22	0.87	0.23	0.51	0.18	0.89	0.13
Type C	0.91	0.36	0.79	0.37	0.55	0.33	0.39	0.28	0.87	0.11

We observed declining TPr as the poll rate increases, noting that the magnitude depends on the DDOS types. Using the smallest poll rate (*pr = 10 s*), detection accuracy is consistent and accurate at (+−) 0.91 TPr. Meanwhile, detection accuracy with the largest poll rate (*pr = 60 s*) is at a mere (+−) 0.30 TPr range. Looking at the poll rate (*pr = 15 s*), SNMP scored merely 0.71 TPr in the Type-A attack, but the score improved to 0.92 TPr in the Type-B attack. Type-A burst at 10 s interval while Type-B burst at the 30 s; consequently, SNMP (pr = 15 s) missed some of the attacks for Type-A attack but detected most Type-B variants. The results confirmed the hypothesis of 'DDOS with burst rate lower than poll rate' can circumvent SNMP detection. Meanwhile, there are no overt TPr changes when the DDOS burst rate is randomized (Type-C). We imply that the lowest poll rate is highly effective in detecting DDOS at the cost of computing. Implicatively, this poses the question of '*how much smaller should the SNMP poll rate be set at'* for DDOS detection to work? It is a cat-mice race; the attacker can adjust DDOS to burst at a rate lower than the SNMP poll rate until the high poll rate becomes too demanding.

It is also apparent that FPr somewhat decreases with the increasing poll rate. Lower FPR is essential to prevent accidental filtering of legit traffic or risk a high amount of TCP retransmissions. This is true to Pareto principles; since SNMP with higher poll rate checks less often, there is a lower chance for SNMP to misclassify, thus lowering the FPr rate. Currently, the FPr is in the range of 0.2–0.3 that translates to 3 out of 10 legit packets being wrongly flagged. Despite being ideal, we attribute the shortcomings to SNMP MIB mechanisms like throughput/bandwidth utilization that hardly distinguish between legitimate bulk data transfer from traffic flooding. The increases in TPr and FPr over reduced polling rate are visualized in Fig. 5. Ideally, higher TPr is a good sign (most DDOS are detected), but the higher FPr (most normal traffic are tagged as DDOS) indicates increased false alarms.

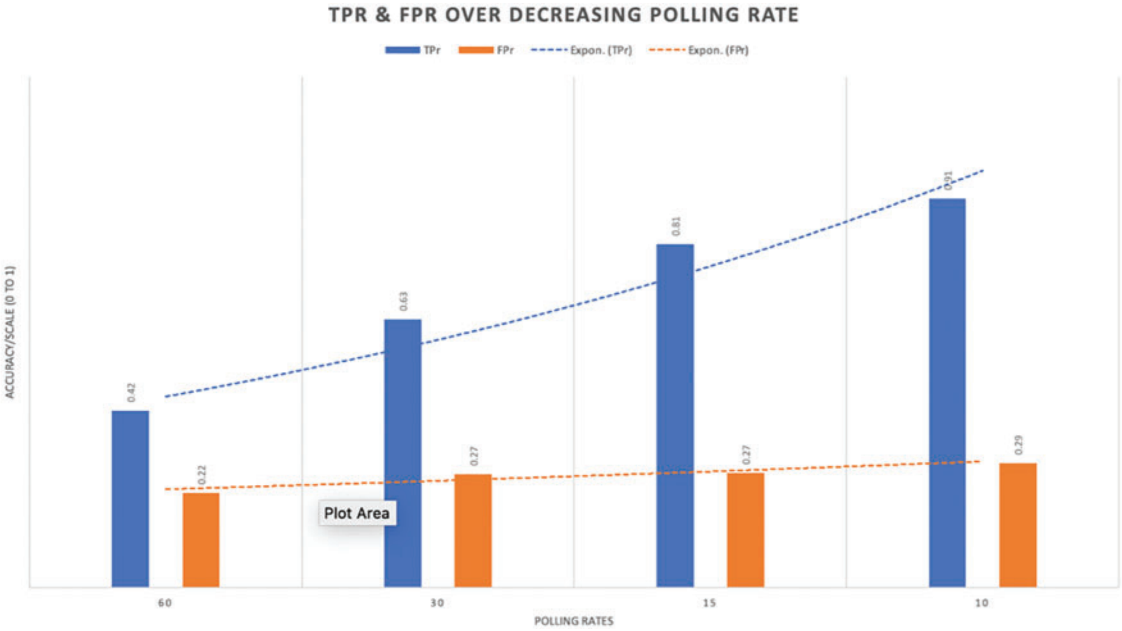

Figure 5: Scaling down SNMP poll rates for improved TPr

Comparing the TPr of SNMP with fixed poll rates to 3D-SNMP, we see the proposed 3D-SNMP outperforms all existing SNMP configurations except for the smallest poll rate (pr = 10 s). 3D-SNMP consistently scores +−0.88 TPr across three attack variants, which only marginally trails the most compute-intensive poll rate setting (pr = 10 s). The robustness is attributed to the adaptively scaled poll rate that only kicks in when DDOS are pre-emptively detected. In Type-A attack, 3D-SNMP uses the optimal poll rate (pr = 10 s) when flooding occurs at each of the interval's onset. In Type-B, the poll rate is scaled to 30 s to adequately detect DDOS that burst at 30 s/rate while slightly relaxing the SNMP checks' compute needs. In Type-C, 3D-SNMP hit 0.87 TPr, although it does scale more aggressively to react to burst rate randomness. We imply that using a **DDOS Sampler,** 3D-SNMP managed to minimize the detection loss during scaling transitions. As the DDOS Sampler is pre-emptive rather than predictive, the TPr is slightly less than SNMP at (PR = 10 s) due to the scaling delay between 3D-SNMP synchronize with DDOS sampler optimal poll rate. However, we ramify that the strength of 3D-SNMP is at adaptively changing the optimal poll rate to reduce detection loss and conserve compute. We hypothesize that the proposed 3D-SNMP is equally robust against a DDOS that burst at 5 s. This DDOS-variant would easily bypass SNMP set to poll at 10 s interval despite being the most aggressive setting here.

In experiment II, we evaluate SNMP's DDOS detection accuracy using different alertness levels. **Alertness** is derived from the threshold value set as the SNMP trigger. High alertness allows SNMP to detect low impact DDOS that is hogging network resources but not significant enough to trigger an SNMP TRAP. SNMP that can detect DDOS at various thresholds is comparably more artful than an SNMP with a fixed threshold. We set the SNMP threshold to >80%, >70%, >60%, and >50% of bandwidth utilization compared with the proposed 3D-SNMP that uses an optimally scaled threshold. Tab. 3 shows the TPr of DDOS detection at different threshold configurations.

Table 3: True positive rate for DDOS detection on low impact DDOS using 3D-SNMP

DDOS counts	Threshold (% of BW utilisation)				
	>50%	>60%	>70%	>80%	3D-SNMP
100 k/s	0.91	0.89	0.57	0.39	0.87
1000 k/s	0.88	0.82	0.78	0.72	0.89
10000 k/s	0.92	0.87	0.88	0.89	0.86

3D-SNMP also detects low-impact DDOS that is designed to 'operates' below the SNMP defined threshold. Such DDOS is less visible but is equally detrimental to network performance. We launched DDOS at three volumes, starting from 100, 1000, and 10000 k number of flows in one second. The experimental results showed that low impact DDOS (100 k) managed to circumvent SNMP-DDOS for most settings unless the threshold is set to >50%. SNMP's main challenge is the 100 K variants, while SNMP quickly detects other more aggressive DDOS. Although the 0.91 TPr gained with >50% threshold is promising, we inevitably raise the false favorable rates since most efficient networks generate more than 50% traffic in peak hours. Meanwhile, we observed 3D-SNMP is capable of detecting the 100 k variants at 0.87 TPr. In 3D-SNMP, the default threshold starts at 50% and continually scales up to 90% in regular operation. When DDOS is detected, the **DDOS Sampler** sends vertical scaling updates to the 3D-SNMP controller to reduce the threshold back to 50%. Then, 3D-SNMP monitors the flagged flows (UDP flood/SYN flood/ICMP flood). If these suspicious flows are confirmed as DDOS, the threshold rate stays at the default value. Meanwhile, if these flows are confirmed as legit flow, 3D-SNMP continues to scale the threshold up until any further alert from **DDOS Sampler**.

6 Conclusion

This paper proposed a novel 3D-SNMP method to detect irregular DDOS designed to circumvent standard SNMP MIB-based detection. Firstly, 3D-SNMP uses a lightweight DDOS Sampler to pre-emptively detect DDOS. 3D-SNMP then scales the SNMP polling rate up and down to accommodate DDOS with a burst rate lower than the pre-configured SNMP poll rate. Meanwhile, the vertical scaling enables 3D-SNMP to dynamically adjust the threshold for detecting low-impact DDOS that carefully avoid SNMP triggers. Using adaptive poll rate, 3D-SNMP successfully detect DDOS with 0.87 TPr for 3 DDOS variants, including (a) DDOS with a small burst, (b) standard DDOS, and (c) DDOS with irregular burst patterns. The proposed 3D-SNMP only trailed SNMP set to poll every 10 s, which we argue overly compute demanding and not scalable to future variants (like a DDOS that burst with 5 s duration). 3D-SNMP also detects low impact DDOS that is previously considered a blindspot when using SNMP for DDOS detection. By scaling the threshold vertically, SNMP can now detect resource-hogging flows like SYN/UDP/ICMP flood that carefully avoids hitting a fixed, predefined SNMP threshold. Although alternatives like behavioral analytics and event-based monitoring are more effective than SNMP, SNMP is somewhat preferred for its ease of configurations, and relatively low compute demand. The proposed 3D-SNMP further extends these advantages by adaptively setting an optimal poll rate. Rather than using the lowest polling rate possible, 3D-SNMP set an optimal rate discrete enough to accurately detect DDOS while not overly aggressive to relax the compute needs for continuous SNMP monitoring.

Acknowledgement: The authors expressed their utmost gratitude towards Centre of Internet and Big Data (CIoTBD) for endorsing the research works that leads to the finding published in this paper.

Funding Statement: This research is currently not directly funded by any institutions and research grants. The DDOS attack are simulated on attack boxes hosted on servers sponsored by Hilti.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Boyko, V. Varkentin and T. Polyakova, "Advantages and disadvantages of the data collection's method using SNMP," in *Int. Multi-Conf. on Industrial Engineering and Modern Technologies (FarEastCon)*, Vladivostok, Russia, 2019.

[2] J. Jiao, B. Ye, Y. Zhao and R. J. Stones, "Detecting TCP-based DDoS attacks in baidu cloud computing data centers," in *IEEE 36th Symp. on Reliable Distributed Systems (SRDS)*, Hong Kong, China, 2017.

[3] A. Mishra and A. Dixit, "Resolving threats in IoT: ID spoofing to DDoS," in *9th Int. Conf. on Computing, Communication and Networking Technologies (ICCCNT)*, Bengaluru, India, 2018.

[4] N. M. Prajapati, A. Mishra and P. Bhanodia, "Literature survey-IDS for DDoS attacks," in *Conf. on IT in Business, Industry and Government (CSIBIG)*, Indore, India, 2014.

[5] S. Brahanyaa and L. Jani Anbaras, "Classification of SNMP network dataset for DDoS attack prevention," in *IEEE Int. Conf. on Computational Intelligence and Computing Research (ICCIC)*, Madurai, India, 2018.

[6] J. Ren, Y. Liu, J. Wu, J. Li and K. Wang, "Smart NCAP supporting low-rate DDoS detection for IEEE 21451-1-5 internet of things," in *IEEE Int. Conf. on Industrial Cyber Physical Systems (ICPS)*, Taipei, Taiwan, 2019.

[7] P. Geenens, "Can SNMP (still) be used to detect DDoS attacks?," Radware, 2018. [Online]. Available: https://medium.com/@RadwareBlog/can-snmp-still-be-used-to-detect-ddos-attacks-2317b79a4037. [Accessed 30 May 2021].

[8] S. Shitharth and D. P. Winston, "A novel IDS technique to detect DDoS and sniffers in smart grid," in *World Conf. on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, Coimbatore, India, 2016.

[9] C. Y. Tseung, K. P. Chow and X. Zhang, "Extended abstract: Anti-DDoS technique using self-learning bloom filter," in *IEEE Int. Conf. on Intelligence and Security Informatics (ISI)*, Beijing, China, 2017.

[10] B. Zhang, T. Zhang and Z. Yu, "DDoS detection and prevention based on artificial intelligence techniques," in *3rd IEEE Int. Conf. on Computer and Communications (ICCC)*, Sichun, China, 2017.

[11] C. M. Bao, "Intrusion detection based on one-class SVM and SNMP MIB data," in *Fifth Int. Conf. on Information Assurance and Security*, Xi'an, China, 2009.

[12] R. Chauhan and S. Shah Heydari, "Polymorphic adversarial DDoS attack on IDS using GAN," in *Int. Symp. on Networks, Computers and Communications (ISNCC)*, Montreal, QC, Canada, 2020.

[13] S. K. Ajagekar and V. Jadhav, "Study on web DDOS attacks detection using multinomial classifier," in *IEEE Int. Conf. on Computational Intelligence and Computing Research (ICCIC)*, Chennai, India, 2016.

[14] W. Park, D. Seo and S. Sohn, "The study about detection of traffic congestion attacks using MIB traffic variables," in *The 6th Int. Conf. on Advanced Communication Technology*, Phoenix Park, Korea (South), 2004.

[15] B. Habib, F. Khurshid, A. H. Dar and Z. Shah, "DDoS mitigation in eucalyptus cloud platform using snort and packet filtering—IP-tables," in *4th Int. Conf. on Information Systems and Computer Networks (ISCON)*, Mathura, India, 2019.

[16] K. Hong, Y. Kim, H. Choi and J. Park, "SDN-assisted slow HTTP DDoS attack defense method," *IEEE Communications Letters*, vol. 22, no. 4, pp. 688–691. 2017.

[17] A. Di, S. Ruisheng, L. Lan and L. Yueming, "On the large-scale traffic DDoS threat of space backbone network," in *EEE 5th Intl Conf. on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conf. on High Performance and Smart Computing, (HPSC) and IEEE Intl Conf. on Intelligent Data and Security (IDS)*, Washington, DC, USA, vol. 22, no. 4, pp. 688–691, 2019.

[18] D. Fadhilah and M. I. Marzuki, "Performance analysis of IDS snort and IDS suricata with many-core processor in virtual machines against Dos/DDoS attacks," in *2nd Int. Conf. on Broadband Communications, Wireless Sensors and Powering (BCWSP)*, Yogyakarta, Indonesia, 2020.