An Integrated Victim-based Approach against IP Packet Flooding Denial of Service

Ruth M. Mutebi[7],
Department of Networks,
Faculty of Computing and IT, Makerere University

Idris .A.Rai
Department of Networks
Faculty of Computing and IT, Makerere University

Abstract:

In this work, we designed a detection technique from a combination of three existing anomaly detection algorithms to detect attacks at the victim machine. The technique is a combination the cumulative sum algorithm (CUSUM), the source IP monitoring algorithm (SIM), and the adaptive threshold algorithm. It is made up of parallel and sequential steps where by the CUSUM and SIM algorithms are designed to work in parallel terms, while the adaptive threshold algorithm is run in case the results from the two (i.e., CUSUM and SIM) are conflicting. We used simulations to evaluate the performance of the proposed technique under various attack scenarios. The results show that the proposed integrated approach is capable of detecting a much wider range of attacks and even flash crowds, compared to the individual algorithms in isolation.

Keywords: Denial of service (DoS) attacks, Anomaly detection Algorithms, Internet Protocol (IP), Transmission control Protocol (TCP), Hypertext transfer protocol (HTTP).

IJCIR Reference Format:

Ruth M. Mutebi and Idris .A.Rai. An Integrated Victim-based Approach against IP Packet Flooding Denial of Service. International Journal of Computing and ICT Research, Special Issue Vol. 4, No. 1, pp. 70 - 80. http://www.ijcir.org/Special-Issuevolume4-number1/article8.pdf.

1. INTRODUCTION

Undoubtedly, DoS attacks are one of the greatest security threats facing the Internet today, especially, the flooding attacks [Carl, 2006]. These attacks are very easy to implement and yet difficult to prevent and protect against because they use legitimate TCP/IP protocols and the weakness in the Internet structure. In order to respond to an ongoing attack, it is important to accurately detect the malicious traffic and cut it off. There are currently many anomaly detection algorithms designed to detect flooding attacks. Though these algorithms have a low overhead, they have a high ratio of false alarms [Kim, 2004], and one algorithm cannot detect all the existing attacks [Kim, 2004]. There are also situations whereby some algorithms can be subverted or fail to differentiate between legitimate and illegitimate traffic [Carl, 2006].

In real life, a host is faced with many types of flooding attacks. We proposed a solution based on a combination of existing algorithms that use different methods for detection in order to build a more effective detection system [Takada, 2001]. There exists a number of similar solutions, however the

[7] Author's Address: Ruth M. Mutebi, Department of Networks, Faculty of Computing and IT, Makerere University, Uganda, rmbabazi@tech.mak.ac.ug; Idris .A.Rai, Department of Networks, Faculty of Computing and IT, Makerere University, Uganda, rai@cit.mak.ac.ug

International Journal of Computing and ICT Research, ISSN 1818-1139 (Print), ISSN 1996-1065 (Online), Special Issue, Vol.4, No.1, pp. 70-80, October 2010.

algorithms used are too resource intensive to be used in a victim machine. The proposed combined detection system consists of the adaptive threshold algorithm, cumulative sum algorithm and the source IP monitoring algorithm. These were chosen because they are not computationally intensive and they enabled us to monitor two different parameters (traffic volume and source IP addresses). The proposed technique enabled us to detect a wide range of attacks and to separate a DoS attack from a flash crowd.

Improved detection at the victim will ensure that the victim can defend itself [Lakshminarayanan, 2004]. Secondly, since detection is easier at the victim, accurate detection at the victim would provide the edge router of the victim network with accurate detection information which the router would use to defend against the attack using methods like push back and IP trace back. Thirdly, due to the lack of centralized administration of the Internet, leaving the DoS detection to be done in only the source - network or in the core network may prove to be unreliable. Detection at the victim will ensure that the attack is detected even if the routers failed to detect it. Much as there exists a number of combinations of anomaly detection algorithms, we aimed at selecting algorithms that are fast and are not computationally intensive and could thus be used in a victim of a DoS attack.

This paper is organized as follows: In section 2 we present the related work, and in section 3 we mention briefly the existing anomaly detection algorithms and explain why we selected the three algorithms. We explain the experimental sup clearly showing how the attacks were simulated in section 4 and explain how the algorithms were used to detect those attacks in section 5. The analysis of the performance of the algorithms is presented in section 6 and it leads to the proposal of the combined detection technique in section 7. The technique is discussed in section 8 and we finally conclude in section 9.

2. RELATED WORK

In this section we present related work from three groups of authors, Dainotti et al [2006], Luo et al [2005] and Peng et al [2003]. In all these works, anomaly detection algorithms were combined to detect different types of attacks.

Dainotti et al [2006] used a combination of adaptive threshold, cumulative sum and continuous wavelet transform to detect volume based attacks. They used the adaptive threshold and cumulative sum in the first part of their detection engine, which they called rough detection. Here an anomaly was detected and an alarm was sent to the fine detection engine which was based on the continuous wavelet transform (CWT). The CWT would ensure a reduction in the number of false alarms.

In their work, Luo et al [2005](2005) proposed a two-stage scheme to detect the pulse denial of service attacks (PDoS) on the victim's side. The methods of detection were designed based on two key observations. First, that the PDoS attack causes the rate of incoming traffic to fluctuate more severely than would normally be the case, and secondly, that the outgoing TCP acknowledgements (TCP ACKs) decline after an attack has been launched. The first stage in the detection process employed a discrete wavelet transform (DWT) to monitor the variability in the incoming traffic and in the outgoing TCP ACK traffic. The nonparametric CUSUM algorithm was used then to detect abrupt changes in the incoming traffic and in the ACK traffic.

The detection scheme that was proposed by Peng et al [2003] had two engines. The first one for detecting abnormal traffic volume in one IP flow and the other for noticing rises in the number of new IP addresses. Both detection engines were run at the same time and they needed a decision engine to confirm presence of attack. They were thus able to detect highly distributed denial of service (HDDoS) attacks while ensuring that they could also detect single source attacks.

All the above combinations are excellent proposals and they achieve better results than the individual algorithms. This research was therefore not carried out because of the weaknesses of these combinations, but to apply the same principle in order to design a combination that would detect flooding attacks at the victim.

Our work is different from Luo et al's work [2005], which was focused on detecting pulse DoS attacks, and Peng et al's [2003] work that was focused on HDDoS. Dainotti et al's [2006] work would have been suitable for detecting flooding attacks at the victim but according to Carl[2006], wavelet analysis is complex and memory intensive and thus would not be suitable for use at the victim's machine.

3. ANOMALY DETECTION ALGORITHMS

There exist a number of anomaly detection algorithms, examples of the most common include those which monitor traffic volume [Siris and Papaglou, 2005; Dainotti et al, 2006], those which monitor the number of new source IP address [Peng et al, 2003] and those which monitor the ratio of incoming to outgoing traffic [Abdelsayed ,2003; Gil, 2001; Mirkovic, 2005]. After reviewing the strengths and weakness of each of the algorithms, we selected three algorithms to use.

3.1 Selected Algorithms

One of the requirements of the selected algorithms was that they needed to have a low computational and memory requirement. This is crucial because during the attack, the victim's resources are already constrained. For this research we chose to use the CUSUM algorithm [Siris and Papaglou, 2005], adaptive threshold algorithm [Siris and Papaglou, 2005] and the source IP monitoring [Peng et al. 2003] algorithm. This selection was made after analyzing the strengths and weaknesses of the algorithms. The reasons for the choice are as follows;

- The (CUSUM) algorithm was selected because it has a low computational overhead and can detect both high and low intensity attacks.
- The adaptive threshold algorithm was selected because it is robust, has a low computational overhead and can effectively detect high intensity attacks.
- Source IP monitoring algorithm (SIM) was chosen because it can accurately detect HDDoS and it has the ability to differentiate between a flash event and a DoS attack, a feature that CUSUM lacks.
- Due to its complexity and memory requirements, wavelet analysis is not suitable for use at the victim's machine, therefore it was not chosen.
- Rate comparison would have been an excellent choice but however due to lack of statistical techniques that use this method, we decided not to choose it in this study.

To study the performance of the algorithms we simulated attacks and found out how the algorithms performed during the detection. In the next section we present the experimental setup, the traffic simulated, and the different attack types that we simulated.

4. EXPERIMENTAL SETUP

4.1 Topology

We used the Network Simulator (ns) [vint,2008], to simulate a wired IP network with one Web server (the victim), four routers, one egress routers and one ingress router. It had nine clients five of which were generating attack free traffic (legitimate Web clients) and the others were generating attack traffic (illegitimate). The WAN link had a speed of 64Mbps and a delay of 60ms while the LAN links had a speed of 100Mbps and delay of 20ms. Figure 1 shows the simulated topology. In Figure 1, nodes 3-6 are the legitimate Web clients, while 8 -11 are illegitimate.

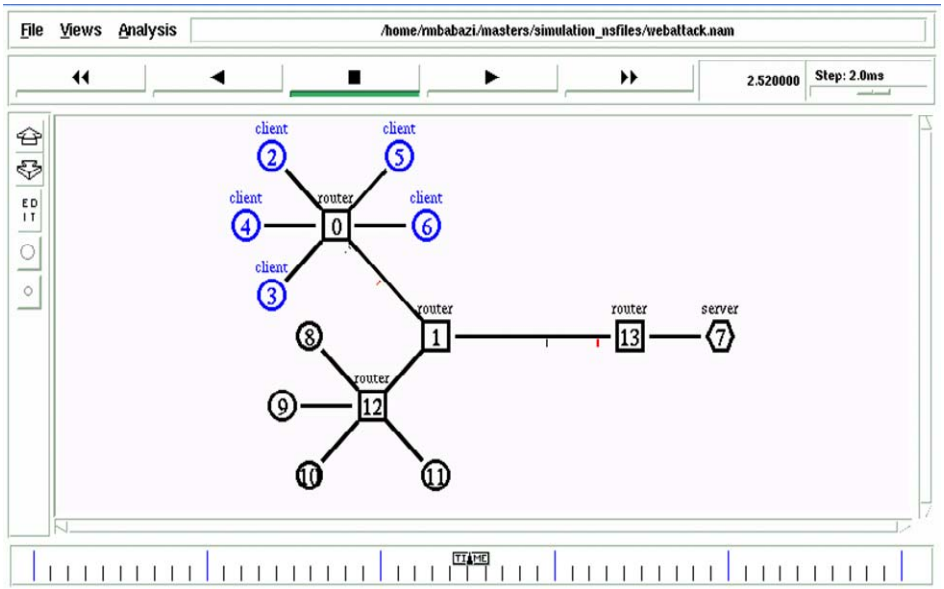

Figure 1: A setup of the simulated topology

4.2 The Traffic

According to a survey carried out by Moore [2001], most of the attacks on the Internet are directed to the TCP protocol and the HTTP (port 80) is among the most attacked ports. Therefore we decided to simulate legitimate HTTP traffic using the pagepool/webtraf application of ns2 and we superimposed on it the attack traffic using the same application.

In a real network, Web clients request the server for a certain number of pages per session and each page has a given number of objects. To access each object the client has to make a request. The pagepool/web-traff tool simulates this behavior by using values such as number of pages per session or page size. According to Feldmann et al (1999), legitimate use of the Web service can be modeled using various distributions for different parameters of the Web session. These parameters are defined as follows:

- Inter-Session time: Time between sessions from different users.
- Pages per session: Number of Web pages accessed within a session by the same user.
- Inter-page time: Time between consecutive pages downloaded by the same user.
- Page size: Number of objects within a Web page.
- Inter-object time: Time between requests to objects.
- Object size: Size of an object in KB (equals number of packets required to transfer an object).

Feldmann et al [1999] proposed the use of either pareto, exponential or constant probability distributions to generate any of the above parameters. The types of distributions used in the research were adopted from Xei et al [2005] and are shown in Table 1. For the exponential distributions the average is shown. For all the simulated traffic the inter-page time belonged to an exponential distribution with an average of 1, the object size belonged to a pareto distribution with a shape of 1.2 and an average of 12 and the inter-object time belonged to an exponential distribution with an average of 0.01.

Traffic Type	Sessions	Inter session Exponential	Pages	Page size constant
Legitimate	1000	1	15	10
Dos	1000	0.025	10	10
DDoS	1000	0.025	10	10
Pulse	40	0.025	10	5
Increasing attack	1000	0.5	10	10
Flash crowd	1000	0.025	10	10

Table 1: Showing the types of distributions and values used in the research

4.3 Simulated Attacks

We simulated a number of attacks and a flash crowd in order to find out how the algorithms behave in different scenarios. We simulated a DoS attack, DDoS (Distributed Denial of Service attack), slowly increasing attack, rapidly increasing attack and pulse attack. The verification for these attacks can be found in [Takada, 2001].

The attacks and background traffic were simulated using the varying parameters, as shown in Table 1. Throughout all the attacks, the background traffic was generated using the parameters for legitimate traffic shown in Table 1. The background traffic is simulated starting at 0 seconds and is generated throughout the simulation. The attack traffic is superimposed on top of the background traffic starting at 100 seconds from the start of the simulation (except for pulse attacks which start at 80 seconds and are repeated every 60 seconds).

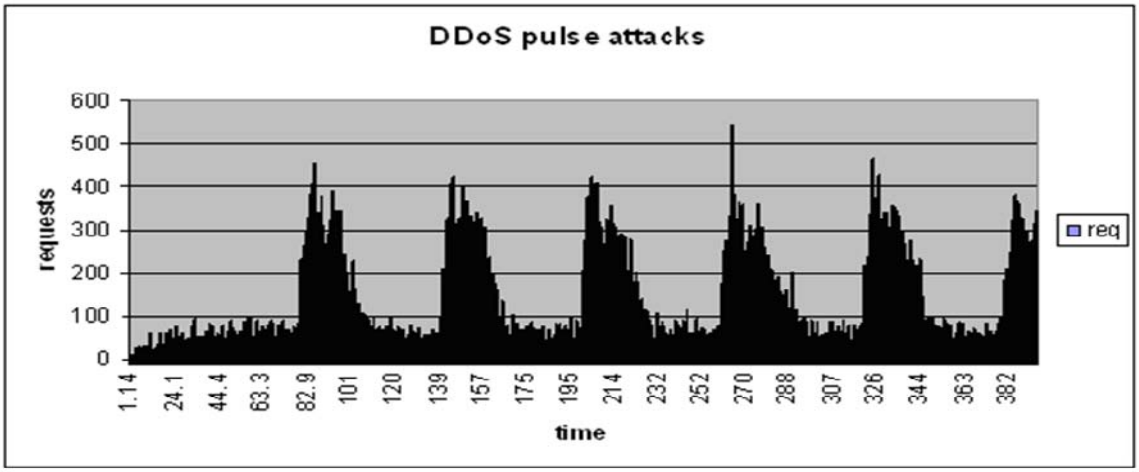

Figure 2: Five pulse attacks starting at 80 sec

During a pulsing DoS attack, short bursts of attack traffic are sent to the victim [Luo et al,2005]. In this work, we used a basic description of pulse attacks as being attacks in which the attack traffic oscillates between the maximum rate and zero [Takada, 2001]. Figure 2 shows an example of the simulated pulse attack using the traffic parameters and distributions shown in Table 1. Graphical presentation of other simulated types of attacks can be found in [Mbabazi, 2009].

In the next section, we show how the selected algorithms, namely CUMSUM, SIM, and adaptive threshold algorithm were used to detect the pulse attack shown in Figure 2.

5. DETECTION

In this section, we explain how the algorithms were used and we show the graphs for how the three algorithms detected the pulse attack.

5.1 CUSUM Algorithm

The total number of requests (number of synchronization packets) per second, x_n was got. The mean $\mu_n$was calculated every 5 seconds. Using these values $g_n$was calculated.

$$g_n = \left[g_{n-1} + \frac{\alpha\mu_{n-1}}{\sigma^2}\left(x_n - \mu_{n-1} - \frac{\alpha\mu_{n-1}}{2}\right)\right]^+$$

An attack was detected when $g_n \geq h$, where h is the attack threshold. The amplitude percentage parameter α was to 0.5. Instead of estimating the mean, the actual mean $\mu_n$was calculated. The value of h was varied to achieve accurate detection. Figure 3 shows detection of pulse attacks using CUSUM algorithm.

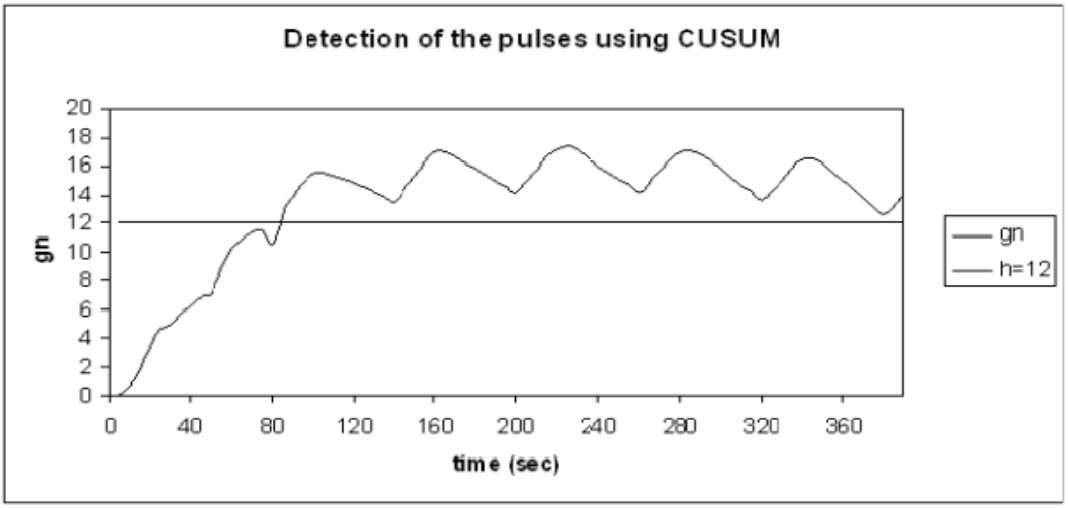

Figure 3: The detection of pulse attacks using CUSUM algorithm

A more detailed presentation of this algorithm can be found in [Siris and Papaglou, 2005].

5.2 Source IP Address Monitoring (SIM)

This was used to monitor the source IP addresses and an attack was detected when there were many new IP addresses. A database of trusted IP addresses against which to compare IP addresses was accumulated before any abnormal rise in IP addresses was detected. Since the simulated topology was small (only four attacking nodes), in most of the attacks there were only 4 new addresses. In order to have more realistic results the individual connections from the same node were considered as different. This means that instead of considering source addresses 2.1 and 2.2, as coming from the same node (node 2), they were considered as a separate sources.

An attack was detected when the decision function, $d_N = 1$. The threshold parameter N = 800 was used. A more detailed presentation of this algorithm can be found in [Peng et al. 2003]. Figure 4 shows how the pulses were detected.

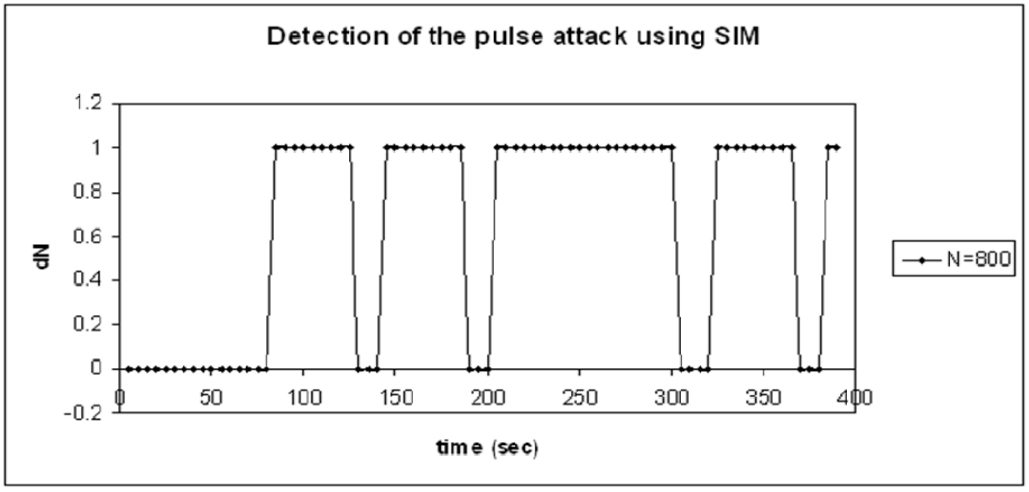

Figure 4: Detection of pulse attacks using the SIM algorithm.

5.3 Adaptive Threshold

This algorithm as presented in [Siris and Papaglou, 2005] was used to detect an attack by comparing the total number of requests x_n at time, t, to the estimated previous mean multiplied by a factor. In order to reduce false alarms, the alarm was signaled when the number of times that the requests are greater than the

mean is greater than a value, k . However in this work, we needed to use the adaptive threshold algorithm to analyze traffic from each source. Therefore instead of using x_n as the total number of requests at time, t, we used $x_n$as the number of requests from each source. We used this algorithm as shown in Equation 2.

$$x_n \geq (\alpha + 1)x_{n-1}$$

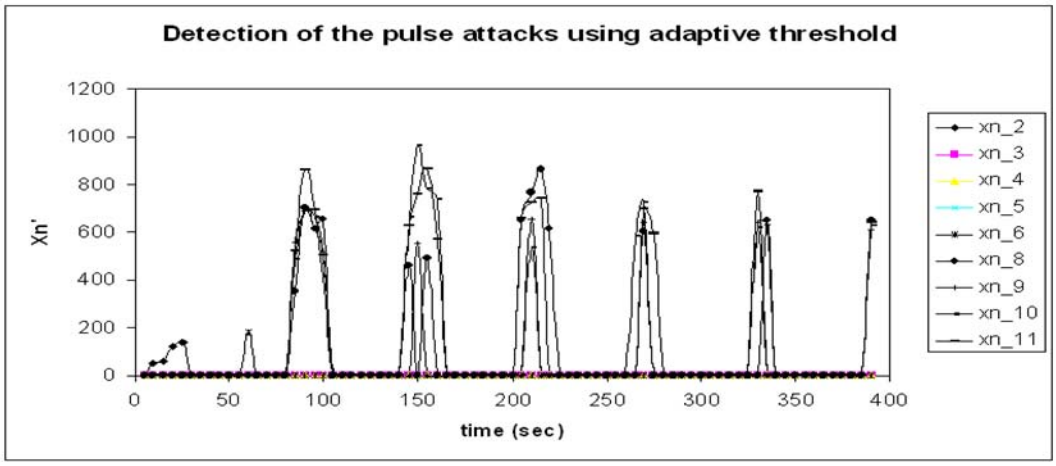

Figure 5 : Showings how the pulse attack was detected using the adaptive threshold algorithm.

A more detailed presentation of this algorithm can be found in [Siris and Papaglou, 2005].

6. SIMULATION RESULTS

From literature the metrics used to measure performance DoS and DDoS detection algorithms vary depending on the aim of the work. Due to the similarity in research aims, we used metrics that had been used by [Siris and Papaglou, 2005] and and [Peng et al, 2003]. These are:

- Detection delay: The time in seconds from when the attack started to when it was detected.
- Probability of detection: This is whether or not the algorithm detects the attack.
- False detection rate: This is a measure of the accuracy of the algorithm.

In this section, we discuss simulation results, showing the performance of each algorithm independent of the others. Based on the results presented in this section, we proposed a new detection technique.

6.1 Probability of Detection

The probability of detection shows whether or not the algorithm detected the attack. A probability of 1 means that the algorithm detected the attack (or noticed an abnormality),while a probability of 0 means that nothing was detected. Table 2 shows the probability of detection for each algorithm, for each of the attacks.

Attack	CUSUM	SIM	Adaptive
Dos	1	0	1
DDoS	1	1	1
Pulse	1	1	1
Slowly increasing	1	1	1
Rapidly increasing	1	1	1
Flash	1	0	1

Table 2: Showing the probability of detection of the algorithms

For all the algorithms, probability of detection was high except for the source IP monitoring algorithm that failed to detect the DoS attack. The results for the CUSUM algorithm and the adaptive threshold algorithm are the same. This is not surprising since they both use traffic volume to detect attacks.

6.2 Detection Delay

Detection delay is the time in seconds from when the attack started to when it was detected. By subtracting the start time from the detection time, the detection delay of each algorithm for each attack was got. The values are presented in Table 3.

Attack	CUSUM	SIM	Adaptive
Dos	10	-	5
DDoS	10	5	0
Pulse	5	5	8.5
Slowly increasing	10	5	23.5
Rapidly increasing	5	5	7.5
Flash	5	-	5

Table 3: Showing the detection delay of the algorithms in seconds

6.3 False Detection Rate (FDR)

This metric was used to measure the accuracy of the algorithms by monitoring the false detections (mistakes) made by the algorithms. A false detection occurs either when an algorithm detects an attack when there is none or when an algorithm does not detect an attack when there is one. We took the FDR to be the total number of false detections. Table 4 below shows the false detection rates of the algorithms.

Attack	CUSUM	SIM	Adaptive
Dos	0	1	0
DDoS	0	0	0
Pulse	0	0	2
Slowly increasing	0	0	0
Rapidly increasing	0	0	0
Flash	1	0	1

Table 4: Showing the number of false detections made by the algorithms.

It is clear from Table 4 that the adaptive threshold algorithm was the worst performing, with 3 false detections while CUSUM and SIM performed equally well, each with one false detection. By analyzing only the columns for CUSUM and SIM, the results are the same for most of the attacks except for DoS and flash crowd, where the two algorithms contradict each other.

7. PROPOSED COMBINED ALGORITHM

From the results of the performance of the algorithms as presented in Tables 2, 3, and 4, the following points were noted;

- Apart from the detection of DoS attack and flash crowd where CUSUM and SIM disagree, they both detected the rest of the attacks.
- In situations where both SIM and CUSUM detected an attack, SIM was the first one to detect.
- The results for the adaptive threshold algorithm and CUSUM were similar for all situations but the performance of adaptive threshold in terms of detection delay and number of false detections was worse.

Based on the three issues raised above, we concluded the following:

i. Since SIM had the shortest detection time, its overall performance was better than that of CUSUM.
ii. Since adaptive threshold had the longest detection delays and most false detections, it was the worst performing of the three algorithms.
iii. Despite its poor performance, adaptive threshold algorithm could be used in DoS and flash crowd situations to identify the sources of the attack. During a DoS attack, there is only one source of abnormal traffic. However in a flash crowd, they are more than one and the sources of the abnormal traffic are old (previously existing) IP addresses.

We therefore propose a detection technique as shown in Figure 6. The proposed detection technique is made up of two steps, one parallel and the other sequential. The first step is made up of the CUSUM algorithm and SIM algorithm running in parallel. The second step is made of the adaptive threshold

algorithm. Since CUSUM and SIM are superior to the adaptive threshold algorithm, they would be run together and their results are fed to the decision engine. The result from the decision engine determines whether there is an attack or not and whether to run adaptive threshold algorithm. The adaptive threshold is run in case the results from CUSUM and SIM are conflicting. While CUSUM and SIM analyze incoming traffic in real time, the adaptive depends on the data collector to supply it with the necessary traffic information (that is, number of requests from each source IP address and the new and old IP addresses from the SIM algorithm).

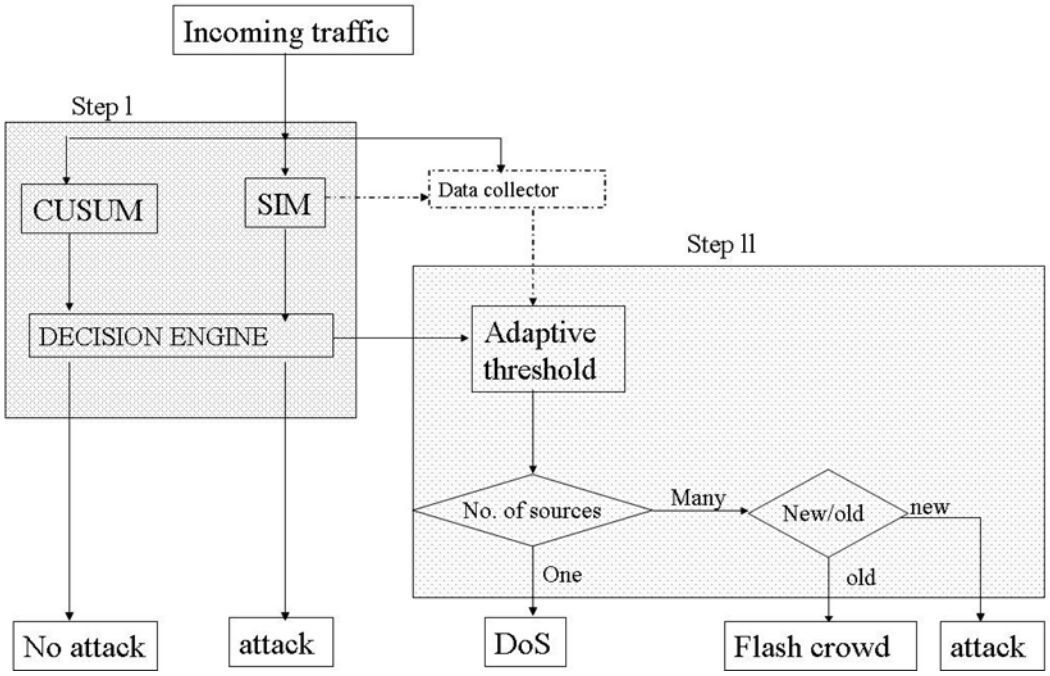

Figure 6: A flow diagram showing the operation of the combined detection technique

7.1 The Decision Making Process

Table 5 shows the decisions taken by the decision engine in the proposed algorithm depending on the outcomes of the CUSUM and SIM algorithms.

Outcome	CUSUM	SIM	Decision	Reason
I	Yes	Yes	Attack	Both algorithms have detected
Ii	No	Yes	Attack	SIM is superior
iii	Yes	No	Run Adaptive	May be Dos attack or flash crowd
Iv	No	No	No Attack	Both have not detected

Table 5 : Showing the decisions taken by the decision engine.

The reasons for the decisions taken are as follows:

i. Outcome i: Since both algorithms have detected an attack, then there is obviously an attack going on.
ii. Outcome ii: The results of the SIM algorithm show that it can never detect an attack when there is none. This implies that if the CUSUM algorithm failed to detect an attack yet SIM has detected one, it is mostly just starting.
iii. Outcome iii: In situations where the CUSUM algorithm detects an attack and SIM does not, then the adaptive threshold algorithm can identify whether the source of high traffic is one or they are many.
iv. Outcome iv: Since both algorithms have not detected an attack, then there is obviously no attack going on.

7.2 The Second Step of the Technique

In situations where the CUSUM algorithm detects an attack and SIM does not, the adaptive threshold algorithm can identify how many sources of high traffic there are. If it is only one, this shows that it is a DoS attack. If they are many, then a decision is made as to whether the IP addresses of attack sources are part of the legitimate IP addresses (old IP addresses), or if they are new IP addresses. If they are new, then this shows that that there is an attack. Whereas if they are old, then it's an indication that it is a flash crowd.

8. DISCUSSION

The successful performance of our technique largely depends on the accuracy of the SIM algorithm. This algorithm has been proved to be an accurate algorithm [Peng et al, 2003; Takada, 2001]. Working parallel with the SIM algorithm is the CUSUM algorithm. From the work of [Siris and Papaglou, 2005], the CUSUM algorithm is also very accurate and robust. Thus the results of the two algorithms, if similar are real proof of the presence of an attack. . When SIM detects and CUSUM does not, it implies there is an attack.

However in situations where CUSUM detects and SIM does not, the result of CUSUM cannot be relied upon. Thus the individual sources of traffic are analyzed by adaptive threshold algorithm. However there are issues that our work raises that we address in the sequent subsections.

8.1 Why three Algorithms?

Since we made it clear that our technique largely depends on the SIM algorithm, one wonders why we did not limit ourselves to use only SIM and CUSUM or to SIM and adaptive threshold. The reason we used three algorithms is to have accurate results. Had we used only SIM and CUSUM, then we would not be able to differentiate between a DoS attack and a flash crowd.

8.2 Reasons for False Detection

The outcomes of the proposed technique as shown in Table 5, are based on our findings and from previous work [Siris and Papaglou, 2005; Peng et al, 2003]. However these outcomes are not exhaustive. For example, what would happen if an attacker spoofed trusted IP addresses? In such a situation, SIM would not detect the attack but CUSUM would. Further investigation by the adaptive threshold algorithm would show that there are many old sources of attack traffic. This would imply that they are trusted sources and it is thus a flash crowd.

8.3 Performance of the Adaptive Threshold Algorithm

The use of this algorithm to analyze traffic from each source may not be realistic in real life. The number of sources would be so many that analyzing each would further reduce performance of the victim. However since the SIM algorithm uses a database of IP addresses, new and old, sampling may be used to select which addresses to analyze. The sampling may vary depending on the number of IP addresses. In case there is only one source of attack, there would be no need for sampling. The method of sampling to be used is an area for further research.

8.4 Choice of detection thresholds

For the CUSUM and SIM algorithms, for each attack, we tried a number of threshold values and chose the value that achieved detection in the shortest time. Since this study was not focused on analyzing how varying the threshold values affects performance of the algorithms, we deemed it unnecessary to focus on that issue. In addition, Siris and Papaglou [2005] carried out a similar study for the CUSUM algorithm.

8.5 Limited number of attacks of each type

We simulated only one attack of each type. This affected our results for example; our detection probability values were either "1" or "0". However, each of the attacks simulated had the characteristics of that attack. Therefore we are confident that if we had simulated more attacks of each type , the results would have been similar.

9. CONCLUSION

In this paper, we presented a novel DoS attacks detection technique based on a combined algorithm detection technique, and presented some simulation results under varying types of attacks. The selection of individual algorithms was based on prior studies and evaluation of their performances to identify their strengths and weaknesses. The proposed combined algorithm was derived based on the conclusion we derived on the performances of the individual algorithms.

The problem of DoS attack detection is a very wide one and we cannot say that we have designed the ultimate solution. However, this is part of the many steps that have been and are being made in the journey towards defeating DoS attacks. In particular, simulation results show that the proposed technique performs much better compared to the individual algorithms. Despite a few weaknesses and limitations of the proposed technique, we are confident that with further testing and improvement of the technique, it will achieve and perhaps exceed user expectations.

10. REFERENCES

ABDELSAYED, S., GLIMSHOLT, D., LECKIE, C., RYAN, S., and SHAMI, S. 2003. An efficient filter for denial of service bandwidth attacks, in IEEE Global Telecommunications Conference, vol. 3, pp.1353 – 1357.

ALJIFRI, H. 2003. IP trace back, a new denial of service deterrent?. IEEE SECURITY AND PRIVACY MAGAZINE, vol. 1, pp. 24–31.

CARL, G. KESIDIS, G., .BROOKS, R., R., and RAI, S. 2006. Denial of service attack detection techniques. IEEE Internet Computing, vol. 10, pp. 82–89.

DAINOTTI, A., PESCAPE, A., and VENTRE, G. 2006. Wavelet-based detection of DoS attacks. in IEEE Global Telecommunications Conference.

FELDMANN, A., C. GILBERT, A., C., HUANG, P., and WILLINGER, W. 1999. Dynamics of IP traffic: A study of the role of variability and the impact of control, in SIGCOM, Cambridge, Massachusetts.

GIL, M., AND POLETTO, M. 2001. Multops: data structure for bandwidth attack detection. in USENIX Security Symposium, Washington D.C.,

KIM, M., KANG, H., HONG, S., CHUNG, S., and HONG, J., W. 2004. A flow-based method for abnormal network traffic detection. In Network Operations and Management Symposium, vol. 1, pp. 599 –612.

LAKSHMINARAYANAN, K., ADKINS, D., PERRIG, A., and STOICA, I. 2004. Taming IP packet flood attacks," ACM SIGCOMM Computer Communication, vol. 34, pp. 45 –50.

LUO, X. and CHANG, R., K. 2005. On a new class of pulsing denial-of-service attacks and the defense," In Network and Distributed System Security Symposium, San Diego, CA.,

MBABAZI, R. and RAI, I. 2009. Victim-based defense against IP packet flooding denial of service attacks.

MIRKOVIC J. and REIHER, P. 2005. D-ward: A source-end defense against flooding denial of service attacks. IEEE Transactions on Dependable and Secure Computing, vol. 2, pp.216 – 232.

MOORE, D., VOELKER, G., V., and SAVAGE, S. 2001. Inferring internet denial-of-service activity. In Proceedings of the 10th conference on USENIX Security Symposium, vol. 10.

PENG, T., LECKIE, C., and RAMAMOHANARAO, K. 2003. Detecting distributed denial of service attacks using source IP address monitoring. Available:http://www.cs.mu.oz.au/

V. PROJECT. 2008. The network simulator ns-2 homepage. [Online]. Available: http://www.isi.edu/nsnam/ns.

SIRIS, V., A., and PAPAGLOU, F. 2004. Application of anomaly detection algorithms for detecting SYN flooding attacks. IEEEE Communications Society.

TAKADA. H., H., and HOFMANN, U. 2001. Application and analyses of cumulative sum to detect highly distributed denial of service attacks using different attack traffic patterns. Available: http://www.istintermon. org

XIE, L., SMITH, P., BANFIELD, M., LEOPOLD, H., STERBENZ, J. P., and HUTCHISON, D. 2005. Towards resilient networks using programmable networking technologies. in Seventh Annual International Working Conference on Active and Programmable Networks ,Sophia Antipolis, France.