Monitoring and Detecting Violation Services in QoS Networks

Ahmed Ali Ghanem* ,Khalid Hamid Bilal**

Abstract— At the present time, all the companies and governments have been achieved work by electronic ways through computer networks. With the extensive spread of the networks must be protected from intruder for protecting the rights of customers. This paper proposed new anomaly intrusion detection technique for monitoring the traffic and to identify the customer consumed the resources and effect on the other customers on the network. This technique based on the service level agreement specification parameters, delay, packet-loss and throughput. This agreement achieved between service provider and customers. The main goal was to detect intrusion or attack on the data forwarding process by monitoring service level agreement, our objects is distinguished the genuine customer from illegal customer who violate the terms of internet service. This paper used the network simulator NS2.35 to simulate the proposed network. This paper simulate that, two customers send traffic from a four nodes. In this papers detected the customers (intrusions) consume the resources.

Index Terms—SLA, violation, QoS parameters, detection, attack, NS2

1 INTRODUCTION

In security domain there are multi-level to prevent the networks. Antivirus treatment with the files and application on the devices wanted to examine, but unable to block unwanted network traffic. Firewalls able to block any protocols or IP address go to or from the networks. But if the destination protocol or IP address is legitimate the firewall can't detect this type of traffic such as spamming and worms. Firewall can't examine the content of the legitimate traffic. Intrusion detection able to detect and examine the content of the traffic flow and allows or denies this traffic passed through the network [1-3]. So, most the researchers attracted to study the intrusion detection on introduce a lot of approach to detect intrusion such as statistics-based, data-mining based, machine-learning based, and knowledge-based, each approach has a multiple sub-approach [4-8].

Along with spread and growth for using the internet, the attacks continue to grow. From "one hostile action a week" in 20 years ago, today internet hostel challenge billions of intrusion attempts every day [9, 10]. From the previous, there was a need for modern studies to overcome these challenges.

A lot of modern studies on several field of the intrusion detection, some of these studies indicate to the service level agreement to detect service violation [9, 11, 12]. SLA is an electronic signature between the service provider and the customer, in this signature the service provider guarantee to give the customer services with specification properties and the customer payment fees in order to get these services. Without protection the networks from the service provider the intruder (QoS attacks) will be exploited the vulnerabilities and cause depletion on the memory, CPU and network resources. The aims of QoS attack is consume of the network resources (e.g. throughput) or degradation of the services noticed by users [13].

The main objects of this paper introduce an edge-to-edge approach to detect intrusion and service violation in DiffServ networks based on SLA provisioning. It introduces and effective approach to remove the malicious traffic without penetrating to legitimate traffic. It focuses on detecting the user (attacker) cause this violation and detects his traffic in DiffServ domain. In this paper collect the QoS parameters such as delay, loss and throughput from ingress edges to egress edges and send reports to the service level management (SLM) to compare and take decision if this attacker or his

traffic normal or suspicion. Collect one-way-delay, packet-loss and throughput at all edges using active and passive measurement. One-way-delay and packet-loss used for monitoring network. Throughput used to ensure no user or attacker consuming excessive bandwidth.

OWD estimate for each user by using active measurement by take the time stamp for the packet sending from ingress edge to egress edge and return to the ingress edges as indicate at [14], in order to avoided the synchronization between the ingress and egress edges. Packet-loss estimate for users exceed the SLA violation for OWD by using the passive measurement. Throughput estimated for the suspicious attacker by passive measurement ategress edge to detect the users effect on the domain, and at ingress edge to detect the source of the attack because it near of the customers.

2 LITERATURE REVIEW

Petcu, D. and C. Craciun., [15] displayed the tools used for SLA management that dealing only with performance parameters and the tools available for the cloud monitoring. This paper studied only on the cloud environment.

Moustafa, S., [16] illustrate the architecture of the SLA management (SLAM) using multi tools. He uses the Zabbix tools, OpenStack, amazon EC2, and database server with MySQL to build the SLAM monitor on the cloud environment. This applied on the cloud environment, and this depends on the SNMP protocol.

Habib, A., et al., [17] proposed a core-assisted scheme approach to calculate the loss, in this approach the core router transmit the source and destination IP address with the packet drop information to the SLM. It's difficult to use and deploy it because of need to high overhead monitoring, and this consumes the core router resources, added to uncertainty in determining the threshold loss.

Habib, A., S. Fahmy, and B. Bhargava, Habib, A., M. Hefeeda, and B.K. Bhargava., [18, 19] propose a simple approach to detecting service violation and bandwidth theft in edge to edge domain. This approach depends on delay firstly to detect service violation. It measured OWD by using timestamps recorded at both ends. The drawback in this approach is the non-synchronization between the two ends as mention on [14].

This paper used the probe packet by sending it form the source (ingress) to destination (egress) and return to the source. By this approach avoided the non-synchronization by take the time stamp for the probe packet at the source node when the packet sending and receiving it and divided it by 2.

This approach avoided the core-assistance by using the passive measurement each ingress and egress calculate the amount of packets pass through and send the report to the SLM per interval time. SLM calculate the loss and take decision depend on.

3 MATERIAL AND METHODS

This paper introduce an approach to monitor and detect intrusion breach the SLA violation.

3.1 SLA violation detection

SLA monitoring is needed to achieve supervision on QoS parameter degradation or violation. The service provider should achieve SLA monitoring to prove whether the existing service is matching the

QoS parameters specified in the SLA. SLA monitoring includes monitoring the performance station of the existing service and provider related information to the service level management system. In order for service level management system to verify whither the specified QoS parameters are not violated, this technique must gather performance data from the simulated network performance and examine this data with the guarantees SLA data[9, 20]. When an abuse of a QoS parameter is detected, SLA study and analyzes which cause the violation and how the violation is occurred and which QoS parameter has degraded.

In the beginning, this paper calculated one-way-delay using the active measurement technique as discussed in [14], by sending probe packets form the ingress to the egress. When the user delay exceed the service provider guaranteed delay, a SLA violation may happen; however, this is not sufficient. In state of one-way-delay (OWD) violation, it should measure packet-loss to approve if violation is SLA guarantees are detected. If the measured packet-loss ratios exceed the guaranteed SLA ratio for any user, SLA violations are occurs. it should determine who cause the SLA violation. Loss measurement is estimated by using the passive measurement technique to get exactly measured ration. Simultaneously, this paper measured packet-loss only for suspicious users, in order to keep up network performance scalable.

3.2 Identify user illegitimate

Suspicious users who are violated the OWD. Not necessarily that any suspicious users violation SLAs are illegitimate users, on other meaning not all illegitimate users who are source of intrusions. A suspicious user in probability is either victim or intruder. Both victim and intruder in practical by the simulation they caused high loss rate in state of network congestion by an attack. Therefore, loss parameter is not valuable in recognizing the illegitimate users; however, loss estimation is beneficial as an additional parameter of proof of SLA violation. Throughput is measured to recognize the illegitimate users. Hence, the packet-loss is first measured, and then throughput. Users overwhelming higher than their share of bandwidth prevent other users from using their data transfer rate. So, it is very significant to distinguish between the behavior of victim and intruder, by measuring the throughput. When this technique measures one-way-delay and packet-loss and get that the users exceed SLA guarantees it has large probability that user is a suspicious user, SLM calculates the QoS parameters for every user to show the effect of the users. Thus, users who exceed the bandwidth ratios guaranteed in the SLA are considered illegitimate users, though those within the bandwidth ratios guaranteed in the SLA are considered as legitimate users. This paper used passive measurement to calculate the packet-loss and bandwidth in order to sure that the users exceed the SLA violation and take decision that user is an illegitimate user. This paper is used a passive measurement tools to calculate the packet-loss and bandwidth because, a very effective and accurate and their field is focus on to all traffic user transfer on network [21, 22].

4 MODELING

QoS is a great interest problem in recent communication networks in latest years. Priority queuing becomes an important and popular scheduling mechanism due to its simplicity and high efficiency. One-way-delay and packet-loss are important parameters used to monitor in a DiffServ domain. Throughput measurement is used to detect whether any attacker is getting more than its share of resources, which causes other attacker to suffer. This paper introduces simple methods to calculate

this QoS metrics that used to monitor and detect the intrusion detection. This calculation is compare between the metrics for each user in the DiffServ domain and the SLA guarantees in this domain.

4.1 One-Way-Delay estimation

Packet delay is the time spends to transport packet form the ingress to egress target and back. One-way-delay can calculate either by using delay of real user traffic (using time stamp for the ingress and the egress) or divided round trip time by tow, if link is symmetric [17]. This paper supposes that, the link is symmetric because it uses the simulation environment. The first way has an important drawback effect the correct of the value, this drawback is synchronization between the two ends ingress and egress. This paper proposed a probe packets to calculate a Round Trip Time, probe packets was a process created the packet had 64bytes at the ingress edges, when send this packet, take the timestamp for the sender node and take the time for the same node after return [23].

The inspection unit calculates the one-way-delay for every probe packet and sends that to SLM units.

$$OWD_j^i = \frac{RTT^i}{2} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$$

RTT: Round Trip Time

OWD: One-Way-Delay.

i: Packets.

At the SLM, it calculates the average delay packet i for user j traffic. Large time simulated to collect the large amount of traffic to get the correct and accurate points. It displayed that, the user j do not misbehave things, if the delay was not exceed its delay guarantee.

4.2 Packet-loss measurement

Packet-loss rate is defined as a ratio between of the number of lost packet (get it from the subtract the receive packets from the sent packets) and the total number of transfer packets (sent packets) [24]. It calculated only for the suspicious users. This paper used edge to edge methods for loss measurement between the ingress and egress provider edges. Ingress edge router (y) send report to the SLM contains the total number of packets sent to the egress edge router for the every users $sent_{sx}^{y}$ at interval time Δt. The egress edges router (z) sent a report to the SLM contains the number of packet received from the same suspicious user sx, $recv_{sx}^{z}$ at the interval time. SLM collect and aggregate all packets sent or received for the same user get form a lot of one edges router. After that, it calculate the average loss ratio for user sx using this equation.

$$avrg\_usrpktloss_{sx} = \frac{avrg_{sent\ sx} - avrg_{rcvd\ sx}}{avrg_{sent\ sx}} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots \quad (2)$$

$avrg_{sent\ sx}$: Average number of packets sent by user sx from any ingress edges

$avrg_{rcvd\ sx}$: Average number of packets received by user sx from any egress edges.

SLA violations are occurred if the average packet loss exceeds the loss ratio guarantee in the SLA.

4.3 Network throughput measurement

Bandwidth is the rate which bits or packets are transmitted [25]. Packet transamination rate (PTR) or throughput measured by the number of packet received successfully at the destination nodes [26]. Throughput is a service level agreement parameters measured to ensure that all users are getting their target share resources [27]. Throughput is an important factor which effect on the network performance[28]. The network performance is an important parameter used to detect the fault in the network. When the traffic contain the attack, it consumed the large amount of bandwidth greater than the amount it should use [29]. The main objective of calculate the throughput is to confirm that no user is overwhelming excessive bandwidth and starving the other resources. This architecture collects the amount of throughput of every user [21]. It collects the throughput per ingress and egress edge and sends it to the SLM. The SLM computes the throughput for each user as the sum of the throughput send and receive by the user at all ingress and egress edges. So, if the throughput rate exceeds the SLA bandwidth guarantees then emphasis that the violation is occurred. This paper calculates the bandwidth violation on the ingress and egress edges, in order to detectthe users effect on the domain and the source the attack. At egress edges measured to detect attack effect on the domain while ingress edges measured to detect the source of the attack.

It computes the throughput at ingress and egress edges using

$$avrg\_throughput_{sx} = pktSize * 8 * avrg_{sent\ sx}/\Delta t \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

$$avrg\_throughput_{sx} = pktSize * 8 * avrg_{recv\ sx}/\Delta t \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$avrg_{sent\ sx}$ is the average number packets sent by user sx at the time interval Δt

$avrg_{recv\ sx}$ is the average number packets received by user sx at the time interval Δt

$pktSize$ is the size of the packet sent it adjust by the simulation, it measure by byte.

5 Algorithm Works

This technique suggests this algorithm to summarize what did in this project. As illustrated in figure (1).j all users in the networks, but sx suspicious $users$ it breach the SLA violation with OWD.

6 Simulation Setup

The network simulator NS-2.35 was used [30-33]. In general, the network topology for the simulation comprised 6 edge routers where the traffic is marked according to parameters that will be specified. The edge gateway connected to 1 core routers as illustrated in Figure (2). The bottleneck is placed between core and egress gateways, and through egress gateway to the destination. This model used DiffServ environment domains to simulate the suggested topology. In the edge and core gateway queues used MRED to control the drop policy. This experiment suggests simulated 5 users and each user generates TCP New Reno was used with a congestion window of 2000 packets. Some user used multiple hosts to send multiple flows through one or more ingress edges along the topology paths. The maximum packet size is 592 bytes. Link from the source nodes to corresponding edge gateway have delays of$10\mu s$ and $6Mbps$ bandwidth. Bottleneck is the link between the core and the egress gatewayhas delays of $1\mathrm{m}s$ and $10Mbps$ bandwidth.

SLA guarantees were equally established for every user. OWD pre-defined ratios were guaranteed based on links delay. Edge-to-edge OWD was $7ms$, Packet-loss was 0.08, and the bandwidth was approximate $2.5\ Mbps$. The simulation was run for $1000s$. The objectives to detect the mutual attacks were simulated as malicious users. Malicious users generate Pareto traffic and trigger it to the U3 and U5 at time from 400-600 sec. this simulated two malicious users injected the traffic on multi nodes.

users$j$ sends probe packets to destination and return to source RTT_j^i (source and destination gateways).

Calculate the $OWD_j^i = RTT_j^i/2$

$$if OWD_j^i < SLA_j^{OWD}$$

Normal traffic

else

Calculate the average packet loss for each user violate on OWD by interval time

$$if avrg\_usrpktloss_{sx} > SLA_{sx}^{pktloss}$$

Calculate the average throughput for each user per second

$$if avrg\_throughput_{sx}^i > SLA_{sx}^{throug\ hput}$$

The user is illegitimate user

The traffic is illegitimate traffic

else

victum user

normal traffic

else

normal user

normal traffic

Figure (1) algorithm to detect the victim and suspicious user

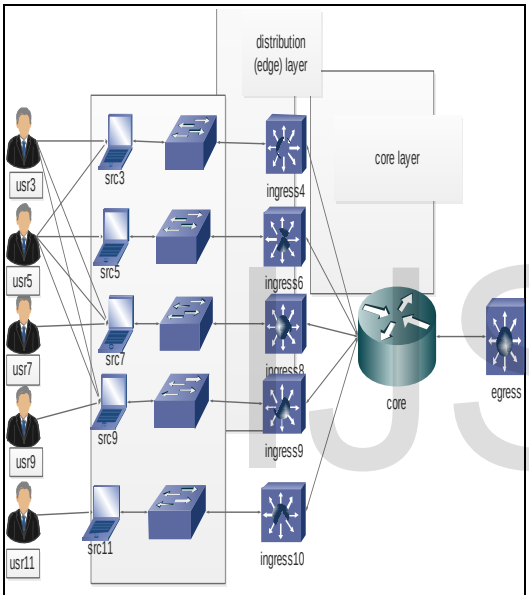

Figure (2) model topology simulated

7. RESULT AND DISCUSSION

This model illustrates the manner of the proposed technique for detecting attack under the networks' provisioning. The one parameter considers is the one-way-delay that estimates by measuring the probe packets delay. By active measuring probe packet take timestamp for the source node to the destination node and return to the source nodes (edge to edge); and divided it by 2.

This technique supposed that two parallel attacks send traffic at the same time at 400-600 sec. These attacks (users) used multiple nodes to send multiple flows through one or more ingress edges along the topology paths. This scenario used to measure the power of the OWD to detect the simultaneously attack.

Detection the suspicious user first step

From figure (3) it can notice that the average OWD measurement for U11 did not exceed the predefine OWD ration of 7ms throughout the simulation time. Whereas the average rate of U3, U5, U7, and U9 were normal before 400 sec and after 600 sec, but breach their SLA by exceeding OWD

guarantees to rise approximately 10ms in between this period. The initial result from the analysis of the aforementioned of OWD is U11 is a normal user, while the U3, U5, U7, U9 it can classified as suspicious users based on the OWD estimation. Also, the small values appear on the diagram for the OWD indicate that QoS applied on this network smallest the value time delay. From the previous, the monitor indicates that high delay point to abnormal behavior in DiffServ domain. and users U3, U5, U7, and U9 make SLA violation at the interval 400-600s.

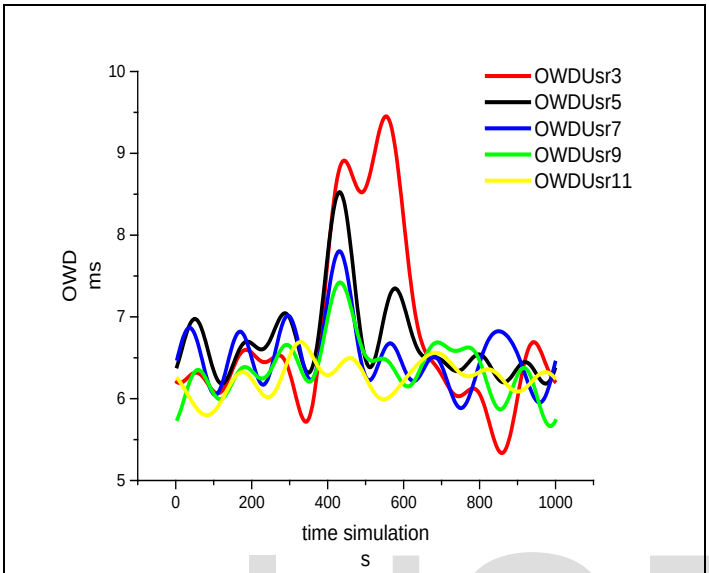

Figure (3): OWD for each users

Detection the suspicious user second step

As previously discussed in OWD; estimation the OWD alone is not accurate; then, to verify SLA violation, the loss rates of suspicious users were measured at the provider edges at ingress and egress gateways using the passive technique measurement.

Passive measurement used to collect the average loss rate for suspicious users on the provider edges. From figure (4) noticed that, the average bit loss rate of U3, U5, U7, and U9 are normal before 400 sec and after 600 sec, but breach their SLA by exceeding packet loss guarantees to rise approximately 0.1 percent between this period.

This attack sends traffic from U3 and U5 on nodes (3, 5, 7, and 9) in simulation period 400-600 sec.

In this approach the users U3, U5, U7, and U9 exceed the SLA violation of OWD and packet loss. Therefore, these users U3, U5, U7, and U9 considered as suspicious users. The main reason for increasing the loss is the congestion link.

Detection the suspicious user third step

At egress gateway:

As mention previously, some users were classified as suspicious users who violated the OWD and packet loss SLA guarantee. The suspicious users are a summation of malicious users who perform an illegal acts of the bandwidth abuse, victim users whose shares of bandwidth were stolen by the malicious ones and normal users who experienced a normal in case of experience on all the detection steps, they didn't effect by the OWD or packet-loss or bandwidth-stolen.

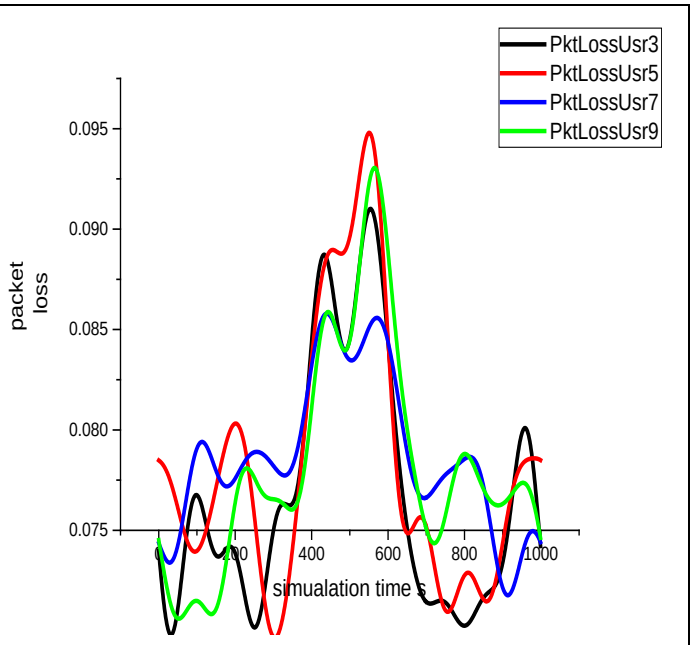

Figure (4) packet loss for suspicious user

This technique detects malicious users by distinguishing between the criminal users from the victim and normal users. For this purpose, users throughput of those performs at illegal acts the SLA violations was passively measured in gateways in ingress and egress gateway.

The throughput was aggregated at the egress gateways router using equation (4), with $avrg_{recv\ sx}$ parameters. As

notice in figure (5), U3, and U5 consumed a share throughput for the other users at the period 400-600 sec. U3 and U5 consumed throughput and penetrate the SLA data rate guarantees by exceeding the bandwidth share to approximately 3Mbps. Other users starved to less than 2Mbps. it verified that U3 and U5 are criminal users, while the U7, and U9 is a victim starved by U3 and U5. From this the U3, U5 are the users effect on the DiffServ domain.

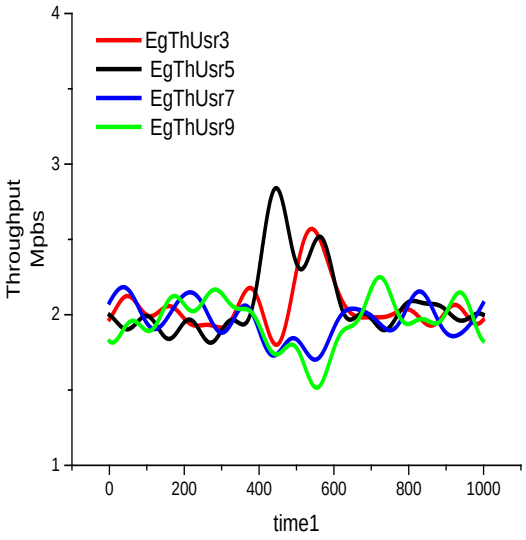

Figure (5) throughput for egress user

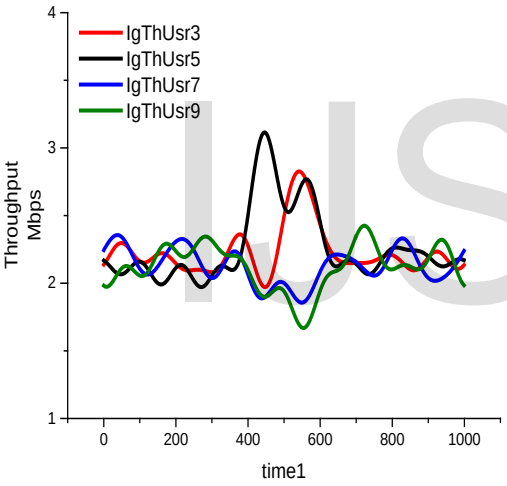

Figure (6) :throughput for ingress users
At ingress gateways

This technique computes the throughput rate for each user at ingress gateway in order to know the source of the intrusion. From Figure (6), it illustrate that measurement throughput of all users from 0 to 1000sec. U7, U9, U11 don't exceed the SLA guarantees throughput but the other users consumed some throughput at the period 400-600 sec. U3 and U5 didn't exceed the SLA violation before 400 second and after 600 second, but between this range the consumed a lot of throughput from other users and effected on. From the ingress measurement the source of the attack from the U3 and U5.

From the previous, the result of the experiments infer the behavior of the proposed technique on detecting the abnormal activity among the 5users, from 5 users this technique reduce the number of malicious users from 5 to 4 with OWD step and verify that at the packet loss percentage and to tow users with third stem with throughput. U3 and U5 are a malicious users but the others users is a victim uses. From the previous, the higher loss by the attack and the other users are a victim affected by the attack. Form the previous.

8.CONCLUSION

This technique can detect the SLA violations and identify their source. It can detect the DoS/DDoS on the service provider networks.

This technique is more accurate to detect a small change on the networks; it is an efficient and effective than other techniques that are used in networks.

This technique can work on the service provider domain; it needs the gateways to apply the policy.

9. REFERENCES

1. Shiri, F.I., B. Shanmugam, and N.B. Idris. A parallel technique for improving the performance of signature-based network intrusion detection system. in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. 2011. IEEE.
2. Fowler, S., S. Zeadally, and N. Chilamkurti, Impact of denial of service solutions on network quality of service. Security and Communication Networks, 2011. 4(10): p. 1089-1103.
3. Fitzpatrick, D., Intrusion Detection and Security Assessment in a University Network. 2011, Dublin City University.
4. Herve Debar , M.D., Andreas Wespi, Towards a taxonomy of intrusion-detection systems. Computer Networks, 1999: p. 18.
5. Wang, Y., Statistical Techniques for Network Security: Modern Statistically-Based Intrusion Detection and Protection: Modern Statistically-Based Intrusion Detection and Protection. 2008: IGI Global.
6. Abhaya, K.K., R. Jha, and S. Afroz, Data Mining Techniques for Intrusion Detection: A Review. International Journal of Advanced Research in Computer and Communication Engineering, 2014. 3(6).
7. Soysal, M. and E.G. Schmidt, Machine learning algorithms for accurate flow-based network traffic classification: Evaluation and comparison. Performance Evaluation, 2010. 67(6): p. 451-467.
8. Berger, G., Knowledge Discovery in Databases for Intrusion Detection, Disease Classification and Beyond. 2001, New York University.
9. Ahmed, A.A., A. Jantan, and T.-C. Wan, SLA-based complementary approach for network intrusion detection. Computer Communications, 2011. 34(14): p. 1738-1749.
10. Polychronakis, M., K.G. Anagnostakis, and E.P. Markatos. Emulation-based detection of non-self-contained polymorphic shellcode. in International Workshop on Recent Advances in Intrusion Detection. 2007. Springer.
11. Ahmed, A.A., A. Jantan, and T.-C. Wan, Filtration model for the detection of malicious traffic in large-scale networks. Computer Communications, 2015.
12. Ahmed, A.A., A. Jantan, and G.A. Ali, A potent model for unwanted traffic detection in QoS network domain. JDCTA, 2010. 4: p. 122-130.
13. Lu, B., Quality of service (qos) security in mobile ad hoc networks. 2006, Texas A&M University.
14. Ahmed Ali Ghanem, K.H.B., Analytical Study on Intrusion Detection in Differentiated Domain. International Journal of Scientific & Engineering Research2017. 8(5): p. 6.
15. Petcu, D. and C. Craciun. Towards a Security SLA-based Cloud Monitoring Service. in CLOSER. 2014.
16. Moustafa, S., SLA Monitoring For Federated Cloud Services. 2015, Queen's UniversityKingston, Ontario, Canada School of Computing p. 97.
17. Habib, A., et al., On detecting service violations and bandwidth theft in QoS network domains. Computer Communications, 2003. 26(8): p. 861-871.
18. Habib, A., S. Fahmy, and B. Bhargava, On monitoring and controlling QoS network domains. 2003.
19. Habib, A., M. Hefeeda, and B.K. Bhargava. Detecting Service Violations and DoS Attacks. in NDSS. 2003.
20. Lee, H.-J., et al., QoS parameters to network performance metrics mapping for SLA monitoring. KNOM Review, 2002. 5(2): p. 42-53.
21. Hu, N. and P. Steenkiste, Estimating available bandwidth using packet pair probing. 2002, DTIC Document.
22. Hu, N. and P. Steenkiste, Evaluation and characterization of available bandwidth probing techniques. IEEE journal on Selected Areas in Communications, 2003. 21(6): p. 879-894.
23. Löf, A., Improving the Evaluation of Network Anomaly Detection Using a Data Fusion Approach. 2013, University of Waikato.
24. Lu, W.-Z., W.-X. Gu, and S.-Z. Yu, One-way queuing delay measurement and its application on detecting DDoS attack. Journal of Network and Computer Applications, 2009. 32(2): p. 367-376.
25. Dordal, P.L., An introduction to computer networks. 2015, Release.
26. Khan, Z.A., A Novel Patient Monitoring Framework and Routing Protocols for Energy & QoS Aware Communication in Body Area Networks. 2013.
27. Habib, A., M. Khan, and B. Bhargava, Edge-to-edge measurement-based distributed network monitoring. Computer Networks, 2004. 44(2): p. 211-233.
28. Reddy, T.B. and A. Ahammed, Performance comparison of active queue management techniques. Journal of Computer Science, 2008. 4(12): p. 1020.
29. Fall, K.R. and W.R. Stevens, TCP/IP illustrated, volume 1: The protocols. 2011: addison-Wesley.
30. Li, M., J. Li, and W. Zhao, Experimental study of DDOS attacking of flood type based on NS2. International Journal of Electronics and Computers, 2009. 1(2): p. 143-152.
31. http://www.isi.edu/nsnam/ns/. The Network Simulator (ns-2) home page. 2017 [cited 2017 11/5].

32. Altman, E. and T. Jimenez, NS Simulator for beginners. Synthesis Lectures on Communication Networks, 2012. 5(1): p. 1-184.
33. Issariyakul, T. and E. Hossain, Introduction to Network Simulator NS2. 2012, Springer New York Dordrecht Heidelberg London. 535.