Analytical Study on Intrusion Detection In differentiated domain

Ahmed Ali Ghanem* Khalid Hamid Bilal**

Abstract— the network is a very famous thing in our life. Today most treatments achieve on the internet. So service provider should offer very good services so that win the confidence of the customers. Therefore service provider used multi-tools to save the customer resources from attack or steal or consume more than having; antivirus, firewall, intrusion detection. Intrusion detection systems (IDS) are systems attempt to detect attacks as they happen or after the attacks took a position. IDS can be rules-detection or anomaly detection based. This paper presents a study of IDS tools and presented architecture intrusion detection depends on the service level agreement parameters. This presented architecture detects any user attempt to consume the network resources or violation services. Service level management (SLM) collects the information (delay, packet loss, and throughput) from the ingress-to-egress service provider to verify the violation service and detect the customer causing of this.

ndex Terms— Architecture,IDS, SLM, violation service, QoS, DiffServ

1 INTRODUCTION

In the recent days, internet networks are a most important information source for the humans. By using the internet on the world wide to communicate people each other's and achieve treatments (e-commerce, band transaction, and most of alternative services) on the communication networks.

The Internet protocol was produced to support multi kind of level service that established on the priority. Quality of service (QoS) is the capability to determined different levels of assurance that its traffic and fulfilled the service requirement for network elements.

QoS does not produce bandwidth rather it manages the available bandwidth depend on the requirements of the applications. For a network service provider to be able to offer good quality of service, it should be offer some guarantees to the subscribers for their service. Service level agreement (SLA) concepts organize relationship between the service provider and the customer[1].

A SLA mostly aggregates the services on classes and supported the amount of traffic acceptable in every class. A SLA defines the performance of the service in packet networks by at least set of parameters that are measurable network indicators for most IP-based services [1-3]: throughput, packet-loss and delay. These metrics are network performance viewpoints the network services [4].

- *Sudan Academy of Science, Engineering Research & industrial technology council, Khartoum, Sudan E-mail:Al_hahmed@hotmail.com*
- *Science and technology university, Engineering Communication Department Khartoum, Sudan*

QoS networks providing different levels of service, the important reasons to steal bandwidth from the upper level. User might pay for a better service and another could try to steal some of that service. Thus, this feature has multi vulnerability, this vulnerable invitation the attacker to hack these networks. The QoS attack objects to steal network resources for example bandwidth or to degrade the service efficient the provider offers to the customer [5].

This kind of activities cause severe losses the target of networks attacked, in the order of billions of U.S. dollars. Consequently, it is actual significant to preventing and detection network for such attack at the real time, which is denoted as intrusion detection[6].

The main object of this paper introduced survey of the kind of intrusion detection. And introduce some concepts on the distributed DiffServ domain based on SLA violation monitoring and used it to detect the intrusion and proposed the architecture help to detect the intrusion detection in this field.

This paper present a general viewed on, Intrusion detection System (IDS) is a security system Their general purpose is to automate, monitor and analysis events on systems and networks and notify security administrators of an event that the sensor determines is worthy of alert. It's extensively used to detect Distributed Denial of Service (DDoS) [5] [7]. Intrusion detection systems are found on multi-forms software and/or hardware products. IDS are often classified to their primary technique, there are two main types: Signature-Based IDS (SIDS) and Anomaly-Based IDS (AIDS) [1].

In SIDS, also famous as misuse detection or rule detection, signatures of known attacks are stored and the events are matched against the stored signatures. The signature-based IDS would monitors packets on the network and match it against a database found or attributes from known, previously-established malicious threats, similarly to antivirus signature detection. The disadvantage with this technique is that it cannot detect zero-days attacks, because whose signatures are unknown, this means that misuse detection will only capture known attacks or attacks that are similar enough to a known attack to match its signature[1, 2]. So SIDS needs a huge database that contains information on every attack. It causes much system overhead to compare every packet with the signatures in the database. Therefore, these systems are not appropriate in a high-speed network [5].

AIDS known is a detection technique by behavior or profile. An intrusion can be detected by observing a variation from normal or expected behavior of the system or the users. AIDS build its profile from reference information collected by various means. After that, the IDS compares this profile with the current activity, if a change is noticing, an alarm is generated. In other meaning, any behavior that does not match to a previously learned behavior is considered intrusive [7, 8].

In this paper, a base-line (profile) of normal data is being set by using SLA to determine a normal behavior. If the incoming string or data deviates from its base-line of normal, the traffic will be considered as anomaly[9]. No intrusion detection technique achieve complete things to protect the system depend on it as an ideal system which capture and analysis all attacks types, each technique is technically suited to detect a separation of security violation[10].

2 PAPER RIEVIEW

2.1 Existing IDS systems

There are a number of kind's intrusion-detection systems. The detection method describes the features of the analyzer [8]. The most important are Statistical-anomaly based detection, Data-mining based detection, Knowledge based detection, and Machine-learning based detection. Anomaly based technique uses behavior matching mechanism, i.e., normal and abnormal behavior. If the incoming string or data deviates from its base-line of normal, the traffic will be considered as anomaly[9]. The most popular and widely spread open source software packages NIDS are Snort and Bro. They detect the attacks by using a group of rules written to examine the network traffic, to inspect the known attacks [11-13].

Snort: Snort is a signature-based NIDS, it capture packets and uses a combination of rules and pre-processors in order to analyze traffic. If the packets captures don't match any hacking patterns, they are allowed to be transmitted to their destination otherwise; packet captures are dropped [14]. Snort spends most running time searching for particular malicious traffic patterns inside the packets [15].

Bro: bro is behavior-based network traffic analyzer. It focuses on monitoring and inspecting all traffic on a link in order to detect of suspicious activity [16]. It used to monitor all entering and outgoing traffic. It detect intrusions by first describing network traffic to display is application-level indications and then runs event-oriented analyzers that compared the activity with patterns created to match normal behavior with it, otherwise it's malicious traffic [17] [18].

2.2 Literature survey

Mahadik, V.A., X. Wu, and D.S. Reeves [19], described method of detection denial QoS attack on DiffServ networks, on real time, using EWMA control chat test and using SRI'S statistical. But this paper doesn't use the profile to detect of the violation, it doesn't collect delay, loss and throughput of every user, it only calculates the throughput for the network. So it doesn't detect the user cause the attack.

Habib, A., M. Hefeeda, and B.K. Bhargava [20], uses SLA parameters define the features of service level behavior. It uses the core-based monitoring. It suggest to statistics method come from randomly selected packet headers saved by a core router. From that saved packet header, ingress routers from special packets known as probe packets that are sent to egress routers, which compute the network delay. Core routers compute the other SLA parameters in similar fashion. The significant drawback in this solution is the amount of overhead required to generate accurate statistics. The author introduces distributed monitoring, under the technique for SLA statistics computation: edge-based monitoring, this method similar to core routing except in the way it measures the packet loss. The author based on the delay to detect service violation. One-way delay detect by using the timestamps recorded at ingress and egress edges. This approach requires the synchronization between ingress and egress edges.

Lu, W.-Z., W.-X. Gu, and S.-Z. Yu [21], propose an approach to measure one-way queuing delay and its application on detection DDoS attack. This approach avoid synchronization problem between source and destination nodes; it isn't take timestamp at both ends. But sends dual probe packets and measured the time interval between two packets. The drawback for this technique is any probe send contain two packets; this probes increase the overhead on the networks.

3 METHODOLOGY

The QoS parameters used one-way-delay (OWD), packet-loss, and network throughput at all sensors (edges) using active for measuring RTT and OWD from RTT. Packet-loss and network throughput used passive measuring. Estimate the delay either by using the timestamps of probe packets from source to destination and round to the source called RTT by dividing the RTT by two[22]. The synchronization is the main problem in measurement one-way-delay. One other meaning, source and destination gateway and the network path must use the same time clock when measuring one-way-delay. There are two main approaches to accomplish synchronization. One is using some network protocols such as network time protocol (NTP) and the other is using GPS. The use of GPS devices in the monitoring system can increase the cost of the network and need to line-of-sight between the equipment and the GPS satellites. Then again, two critical concerns arise if the hosts at both ends of the network path determine their time utilizing a network synchronization protocol such as NTP: first, the accuracy of NTP depends in part on the properties (especially delay) of the Internet paths utilized by the NTP peers, and these may be exactly the properties that used to measure, so it would be unsound to use NTP to align such measurements.
Second, NTP focuses on clock accuracy, which can come at the expense of short-term clock skew and drift [21, 23, 24]. The measurement of round-trip-time has two specific features: first, ease of deployment. Unlike one-way-delay measurement, so should measure RTT by utilizing the time at the same host. So there is solving the synchronization problem in RTT measurements. Second, ease of interpretation.

3.1 Active and Passive measurement

The types of network measurements are active and passive. Active measurement is a technique that creates and injects specific packets into the network under observation. Later, these packets are checked and metrics based on their behavior are calculated. In other meaning, active measurement uses to inspect the behavior the traffic in end-to-end network domain [25].
Passive measurements are a powerful tool used for modeling internet traffic. They used to observe actual traffic without injecting additional traffic into the network and produce a trace of the actual traffic on measured link at a certain time [23]. Passive measurement will be especially useful to support efforts toward internet QoS support [25]. The captured packets are kept in a trace file to analysis, and check of all captured packets produces an accurate analysis of the traffic situation.
Using either active or passive technique alone in whole stages are effects negatively on the accuracy of the measure or display a network performance [26]. Consequently, active technique used to measure probe packet to estimate RTT. This can be collected by sending packet from the source to specific destination and measuring the time. It takes the time of the source node when sending the packet and the time for the source when it receive replay and subtract the times [27]. This technique is clear and simple to get the RTT delays. This technique used RTT instead of one-way-delay because the RTT need not synchronization. RTT is also the metric used in most SLAs currently [23]. Also it uses passive technique to measures loss and bandwidth ratios.
The purpose for estimation measurement technique is that, active measurement is to draw conclusions regarding the general network behavior, while the passive measurement used to get a complete picture of traffic behavior on the network. Thus, an active technique is used as an indicator to SLA violations, whereas a passive technique verified or confirms violations and distinguishes violation source.

3.2 Architecture of the QoS intrudion detection

This technique divides the architecture into two main parts:
Part 1: this part is used to detect SLA violations. It includes an inspection unit, and verification unit.
An inspection unit monitors the abnormal activities in network traffic. Inspection unit collects packets delay from ingress to egress for each user and makes reporting transmit to the service level management. Inspection unit should be always run at to monitor change in the round-trip-time delay.
In verification unit performs functionality in passive loss measurement of users who breaches their SLA guarantees.
Part 2: Diagnosis unit is used to recognize the user penetrate the network and exceed in SLA violations. Diagnosis unit function is measuring the throughput rate of users whose packet loss guarantees are preach SLA violation. It measures at the ingress edges, and compare users' throughput with throughput guarantees, In order to recognize malicious users behind network resources abuse.
Service level management (SLM) is the main body of this technique, the SLM is a control and

management unit of the system; it collects the average loss packet and consumed bandwidth in egress and ingress gateway for each user based on data given by previous units. SLM is responsible of making the significant decisions which user break or exceed their services. Figure (1) displays the proposed architecture for new intrusion detection technique.

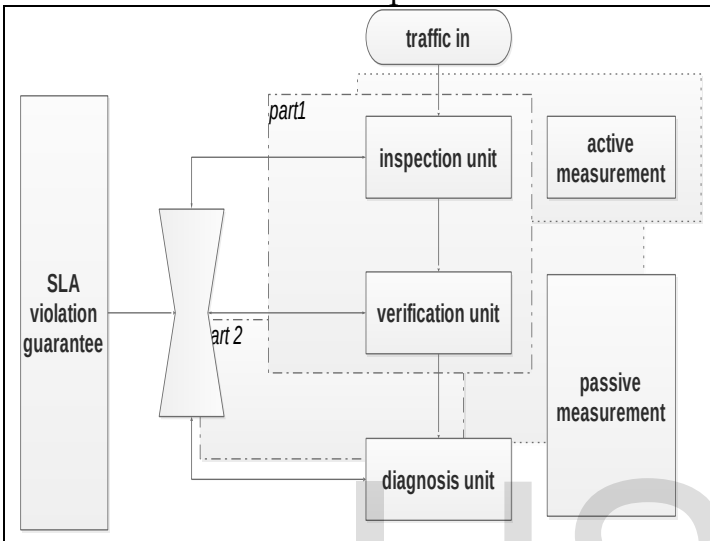

Figure (1) intrusion detection architecture

3.3 Intrusion detection detector

This technique proposed policy to detect Intrusion detection in network. This policy based on SLA violations, when the SLA was violation it probably that is an intrusion, and it should to identifying the user that causes the violation. In most state, the policy applied at the ingress routers, when traffic arrive to the ingress router it classified and policed to confirm that each user did not exceed the ration guarantee prepared by the SLA. After apply the policy attacker (users) cannot send a volume of traffic higher the SLA rates through a single ingress. However, the attacker could not be apple to send a higher volume from one ingress edge, but be apple by sending a volume lower than setup on the ingress edge over several ingress edges.

4 CONCLUSION

In this paper, we have presented an analytical study on the intrusion detection and presented an anomaly based intrusion detection by using quality of service parameters and service level agreement violation. The study shows that the presented intrusion detection architecture is able to monitor the SLA parameters and take the decision that user violates the SLA. In our subsequent work, we will examine how to implement a new algorithm to detect the attackers who consume the bandwidth on networks.

5 REFERENCE

1. Gyanchandani, M., J. Rana, and R. Yadav, *Taxonomy of anomaly based intrusion detection system: a review*. International Journal of Scientific and Research Publications, 2012. **2**(12): p. 1-13.
2. Ghorbani, A.A., W. Lu, and M. Tavallaee, *Network intrusion detection and prevention: concepts and techniques*. Vol. 47. 2010: Springer Science & Business Media.
3. sheldon's, t. *quality of service*. netowrking denfined and hyperlinked 2017.
4. Lee, H.-J., et al. *Mapping between QoS parameters and network performance metrics for SLA monitoring*. in *Proc. of*. 2002.
5. Kim, M.-S., et al. *A flow-based method for abnormal network traffic detection*. in *Network operations and management symposium, 2004. NOMS 2004. IEEE/IFIP*. 2004. IEEE.
6. Mulvenon, S.A.M.D.a.J., *Contested Commons: The Future of American Power in a Multipolar World*. January 2010.
7. Alaidaros, H., M. Mahmuddin, and A. Al Mazari. *An Overview of Flow-based and Packet-based Intrusion Detection Performance in High Speed Networks*. in *Proceedings of the International Arab Conference on Information Technology*. 2011.
8. Herve Debar , M.D., Andreas Wespi, *Towards a taxonomy of intrusion-detection systems*. Computer Networks, 1999: p. 18.
9. Beigh, B.M., *A New Classification Scheme for Intrusion Detection Systems*. International Journal of Computer Network and Information Security, 2014. **6**(8): p. 56.
10. Zaman, S., *A collaborative architecture for distributed intrusion detection system based on lightweight modules*. 2009.
11. Caswell, B., J. Beale, and A. Baker, *Snort Intrusion Detection and Prevention Toolkit*. 2007: Syngress.
12. Dreger, H., et al. *Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection*. in *Usenix Security*. 2006.
13. Paxson, V., *Bro: a system for detecting network intruders in real-time*. Computer networks, 1999. **31**(23): p. 2435-2463.
14. Othman, M. and M.N. Kermanian, *Reliable and security-based Myren network traffic management*

using open source tools. Journal of Information & Communication Technology, 2009. **3**(1): p. 1-10.

15. Brooks, R.R., *Introduction to Computer and Network Security: Navigating Shades of Gray*. 2013: CRC Press.
16. https://www.bro.org/. *BRO. intrusion detection* 2017.
17. Moya, M.A.C., *Analysis and evaluation of the snort and bro network intrusion detection systems*, in *Intrusion Detection System, .* 2008, Universidad Pontificia Comillas. p. 83.
18. Rødfoss, J.T., *Comparison of open source network intrusion detection systems*, in *department of informatics*. 2011, UNIVERSITY OF OSLO
19. Mahadik, V.A., X. Wu, and D.S. Reeves, *Detection of Denial-of-QoS Attacks Based on χ2 Statistic And EWMA Control Charts.* URL: http://argos. csc. ncsu. edu/papers. htm, 2002.
20. Habib, A., M. Hefeeda, and B.K. Bhargava. *Detecting Service Violations and DoS Attacks.* in *NDSS*. 2003.
21. 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.
22. Culverhouse, M., *User-Centric Quality of Service Provisioning in IP Networks*, in *School of Computing and Mathematics Faculty of Technology*. 2012: france.
23. Ta, X., *A Quality of service monitoring system for service level agreement verification*, in *SCHOOL OF ELECTRICAL AND INFORMATION ENGINEERING THE UNIVERSITY OF SYDNEY*. 2006.
24. de Santiago, J.R. and J.A. Rico, *Proactive measurement techniques for network monitoring in heterogeneous environments*. 2013, Ph. D. dissertation, Universidad Autónoma de Madrid.
25. Mochalski, K. and K. Irmscher. *On the use of passive network measurements for modeling the internet*. in *Kommunikation in Verteilten Systemen (KiVS)*. 2003. Springer.
26. 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.
27. Löf, A., *Improving the Evaluation of Network Anomaly Detection Using a Data Fusion Approach*. 2013, University of Waikato.