Software Defined Networking based Intrusion Detection System

Payal Kapre¹, Riya Shreshthi², Madhuri Kalgane³, Kalyani Shekatkar⁴,Yogita Hande⁵
¹,²,³,⁴,⁵Dept. Of Comp. Engg, Sinhgad Institutes Of Technology Narhe, Pune.

Abstract: With the rapid expansion of computer networks during the past decade, security has become a crucial issue for computer systems. The goal of a security system is to protect the most valuable assets of an organization like data and information. This paper state the method of learning the Intrusion Detection, rules based on genetic algorithms. The implementation is experimented using data sets on intrusions, which has become the de facto standard for testing intrusion detection systems. The paper talks about using Genetic Algorithm (GA) in Network Security. Specially, it describes a technique of applying GA to network Intrusion Detection Systems (IDSs). GA is one of the commonly used approaches on data mining. It presents a brief overview of the Intrusion Detection System, GA, and related detection techniques. Our experiments detect different Denial of Service (DoS) attack & network scanning attacks such as Neptune attack etc.

Keywords: – Software Defined Network (SDN), OpenFlow, Genetic Algorithm.

I. INTRODUCTION
Increasing access to the networks leads to further knowledge traffic and these demands needs a lot of numbers of repose connected servers for multiprocessing. Security is that the main issue in networking wherever existing security mechanism are deployed in an exceedingly static manner. Managing static security configurations in giant networks is incredibly time intense. software package outlined Networking (SDN) is supposed to handle the matter of static networks. SDN is associate approach to the pc networking that permits network administrator to manage all the network services providing abstraction of low-level practicality. SDN decouples management plane from knowledge plane. on top of things plane, selections regarding wherever to send the traffic from underlying systems are taken and therefore the knowledge plane that is liable for forwarding the information traffic to the destination. SDN is dynamic, manageable, convertible and cost-efficient network. SDN has programmable and centrally managed infrastructure. because the transmission of information over the net will increase, the requirement to shield connected systems additionally will increase. Intrusion Detection Systems (IDSs) are the most recent technology used for this purpose. though the sphere of IDS continues to be developing, the systems that do exist are still not complete, within the sense that they're not capable to notice all sorts of intrusions. Some attacks that are detected by numerous tools obtainable these days can not be detected by different merchandise, looking on the kinds and ways that they're designed on. employing a Genetic algorithmic rule (GA) is one among the ways that IDSs use to notice intrusions. They incorporate the conception of Darwin’s theory and survival of the fittest to notice intrusions. Not a lot of analysis has been conducted during this space besides the Genetic algorithmic rule as another Tool for Security Audit Trails Analysis (GASSATA) tool; [16] [23] there are only a few IDSs that are fully developed from victimisation GAs. The genetic algorithmic rule is utilized to derive a group of classification rules from network audit knowledge, and therefore the support-confidence framework is used as fitness perform to guage the standard of every rule. The generated rules are then accustomed notice or classify network intrusions in an exceedingly time period setting. in contrast to most existing GA-based approaches, owing to the easy illustration of rules and therefore the effective fitness perform, the planned methodology is less complicated to implement whereas providing the flexibleness to
either usually notice network intrusions or exactly classify the kinds of attacks. Experimental results show the accomplishment of acceptable detection rates supported benchmark DARPA knowledge sets on intrusions, whereas no different complementary techniques or relevant heuristics are applied.

II. LITERATURE SURVEY
To reduce false positives and improve the standard of the forwarding rule set increasingly. In coincidence, Its answer claims to instantly send attack traffic that might cause Associate in Nursing overload of the on-the-scene network to a cloud security supplier that's able to deal with this quantity of traffic, having in mind privacy issues of the buyer. Incoming traffic reaches Associate in Nursing OpenFlow enabled switch (OF-switch). This switch is supplied with a base rule set within the forwarding tables. This base rule set acts as a light-weight IDS that maintains a history of continual events together with concerned IP addresses yet as info from external sources. These sources embrace public obtainable black-lists, white-lists, geolocation knowledge and their severities, supported this info of events, lists and former determined incidents, forwarding rules within the OF-switch area unit changed to adapt the practicality of the general observation and detection method. SDN controller maintains a rule set per shopper that features basic information concerning the capabilities on the buyer website to sight security connected behavior (e.g. IDS) and most popular DDoS laundry MACHINES. Advantage is redirects the attack traffic to a cloud security supplier. Limitations is Trustworthy half is untouched.[1] Snort could be a light-weight intrusion detection system capable of performing arts real time traffic analysis and packet work on IP networks. it's not resource intensive and therefore the ASCII text file is little. Snort is best used on tiny to medium sized networks, single hosts, or on segments of an oversized network. Snort uses the quality libpcap library and tcpdump as a packet work backend. Snort is Associate in Nursing IDS designed to be comprehensive and correct in with success work malicious network activity and notifying directors once potential breaches occur.[2] Using SDN with IDS for web security by generating sensible or dangerous packets and therefore the user are going to be able to see the dangerous packets yet because the different packets that area unit being captured by IDS and may be able to analyze them through the packet instrument wire shark. The projected system is largely designed for Intrusion detection system in field networks employing a new construct referred to as SDN (Software outlined Networking). the power to detach networks supported code outlined networking (SDN) has up in quality. Intrusion detection is one in every of the most challenges of web security these days. If in real time the field system gets intruded then what helps is that the SDN.SDN can solve this drawback through the employment of Openflow. Blessings is Operational savings, Flexibility, higher management, Panning, Infrastructure savings. Limitations is It doesn't support multiple IDS virtual machines running within the same network.[3] Rule-based systems use a group of “if-then” implication rules to characterize pc attacks. The rule-based skilled system is that the most generally used approach to misuse detection. The patterns of legendary attacks area unit nominative as rule sets, and a forward-chaining skilled system is sometimes accustomed hunt for signs of intrusions. However at the first stage of intrusion detection era, rule primarily based languages delineated one in every of the regular strategies for describing the expert’s information that's collected concerning various attacks and vulnerabilities. Here we have a tendency to discuss 2 rule-based skilled systems A) Rule-based sequence analysis language (RUSSEL) B) Production-based skilled system tool set (P-BEST). Disadvantages is it's a low-level language Associate in Nursing  Specifying an attack pattern is analogous to writing a program, though it provides a general condition trigger framework and is declarative in nature. The feature that rules will share world variables introduces the chance of bugs together with the convenience of sharing info among completely different rules.[4]
III. PROPOSED SYSTEM

In this project, we tend to gift a GA-based approach to network misuse detection. GA is chosen attributable to a number of its nice properties, e.g., strong to noise, no gradient info is needed to seek out a worldwide optimum or sub-optimal resolution, self-learning capabilities, etc. during this work, we tend to implement software system supported the bestowed approach. Employing a Genetic formula (GA) is one amongst the ways that IDSs use to find intrusions. They incorporate the conception of Darwin’s theory and activity to find intrusions.

What is Genetic Algorithm: Genetic algorithms (GAs) are pc programs that mimic the processes of biological evolution so as to unravel issues and to model biological process systems. Genetic Algorithms (GAs) are adaptive heuristic search formula supported the biological process concepts of activity and biology. The essential techniques of the GAs are designed to simulate processes in natural systems necessary for evolution; particularly those follow the principles 1st set down by Darwin of "survival of the fittest.” GAs simulates the survival of the fittest among people over consecutive generation for determination a problem’s.

IDS with genetic algorithm: Intrusion Detection is an important mechanism to shield pc systems from several attacks. New attack forms are regularly being discovered. Current IDS systems have restricted capabilities for sleuthing attacks that disagree considerably from antecedent best-known attacks precisely those attacks that systems are most susceptible to. Because the use knowledge of knowledge of information) over the web will increase the necessity to shield these data additionally will increase. Sometimes unwanted intrusions occur once the particular software system systems are running over the web. In-depth study of Intrusion Detection System, genetic formula and connected detection techniques was bestowed during this thesis report. Genetic rule (GA) could also be a programming technique that mimics biological evolution as a problem-solving strategy. It's supported Darwinian’s principle of evolution and survival of fittest to optimize a population of candidate solutions towards a predefined fitness

![System Architecture](image)

**Figure 1: System Architecture**

GA uses associate evolution and survival of the natural process action that uses a chromosome-like system and evolve the chromosomes exploitation selection, recombination and mutation operators, the method sometimes begins with arbitrarily generated population of chromosomes, that represent all attainable resolution of a haul that area unit thought-about candidate solutions. From everybody completely different positions area unit encoded as bits, characters or numbers. Several network features have higher possibilities to be involved in network intrusions. In our approach, seven of those features are selected from the network audit data to compose a classification rule. The feature names are given in the first column, while the second and third columns indicate how each of the
network features is encoded in a chromosome. The second column represents the feature format and the third column shows the number of genes used for the corresponding feature.

IV. IMPLEMENTATION

The Operation of Genetic Algorithm:

Figure 2 illustrates the operation of a general genetic algorithm. The operation starts from an initial population of randomly generated individuals. Then the population is evolved for a number of generations and the qualities of the individuals are gradually improved. During each generation, three basic genetic operators are sequentially applied to each individual with certain probabilities, i.e., selection, crossover, and mutation. First, a number of best-fit individuals are selected based on a user-defined fitness function. The remaining individuals are discarded. Next, a number of individuals are selected and paired with each other. Each individual pair produces one offspring by partially exchanging their genes around one or more randomly selected crossing points. At the end, a certain number of individuals are selected and the mutation operations are applied, i.e., a randomly selected gene of an individual abruptly changes its value.

![Figure 2: The Operation of Genetic Algorithm](image)

The following shows a rule example that classifies a network connection as the denial-of-service attacks neptune.

if (duration="0:0:1" and source_port=18982 and destination_port=79 and source_ip="9.9.9.9" and destination_ip="172.16.112.50")
then (attack_name="neptune")

The above rule expresses that if a network packet is originated from IP address 9.9.9.9 and port 18982, and sent to IP address 172.16.112.50 and port 79 using the protocol finger, and the connection duration is 1 second, then most likely it is a network attack of type neptune that may eventually cause the destination host out of service.
Algorithm:
1. Received Packets
2. Identify suspicious flow
   2.1 Apply Sampling Techniques
      2.1.1 Packet Counter Method
      2.1.2 Time Interval Method
3. Send suspicious flow to IDS
4. Identify Attacks
   4.1 Apply Genetic Algorithms to identify DoS Attacks
   4.2 Apply Genetic Algorithms to identify DDoS Attacks
5. Block Attack

III. RESULTS
In this system the results show the varied effective solutions compared with the present system. Expected results square measure as follows:

To observe noted attacks we've got elite 5 fields like affiliation length, protocol, supply port, destination port & attack name. Currently genetic algorithmic program is applied on same coaching information set, with same initial population & variety of generations. As same fitness operate is employed to pick the best-fit rules with threshold worth zero
5. Procedure of algorithmic program is same as explicit in implementation half. When finishing all steps with success we tend to get following classification rules. The experimental results show that the planned methodology yielded satisfactory detection rates once utilizing the generated rules to classify the testing information.

It may be potential to yield smart detection whereas testing the information: 1) have less variety of generations once coaching the system; or 2) use less variety of best-fit rules once classifying new network data.

Advantage of our approach is that crossover rules don't seem to be static for each execution totally different rules square measure generated that square measure useful to observe new kind attacks gift within the given network

IV. CONCLUSION AND FUTURE WORK
SDN will replace the existing traditional network with a lot of advanced features. However, it is facing with many security challenges. In our system, we propose a security mechanism to combat against DDoS flooding attack. However, other security challenges are yet to be addressed. SDN is currently being applied into cloud computing and networks.

In this paper, a method of applying genetic algorithms for network intrusion detection is presented. One of the major advantages of this technique is due to the fact that in the real world, the types of intrusions change and become complicated very rapidly. The proposed detection system can upload and update new rules to the systems as the new intrusions become known attack present in the given network. Therefore, it is cost effective and adaptive. A GA is used to derive a set of classification rules from network audit data. Initially seven network features including both categorical and quantitative data fields were used when encoding and deriving the rules. But proposed method yield less detection due to fix source & destination IP address. We selected five fields only & applied same procedure with simple but efficient and flexible fitness function, i.e. the support-confidence framework, is used to select the appropriate rules. Depending on the selection of fitness function weight values, the generated rules can be used to either generally detect network intrusions or
precisely classify the types of intrusions. This genetic algorithm can be modified depending on the traffic that is passing through the network. This increases the reliability of the algorithm. This will help in the prevention of attacks and provide security to sensitive data.

In the future, work include implementing same approach on large scale network. So that it helpful to identify known & detect unknown attack present in the given network.

REFERENCES
[1] Sebastian Seeber, Lars Stiemert, Gabi DreoRodosek, “Towards an SDN-Enabled IDS Environment”, Neubiberg, 85577, any, 978-1-4673-7876-5/15/ ©2015 IEEE 751
[2] Tiyani Xing, Deep Medhi, “SDNIPS: Enabling Software-Defined Networking Based Intrusion Prevention System in Clouds”, 10th CNSM and Workshop 2014 IFIP
[3] Martin Roesch – Stanford Telecommunications, “Snort-Lightweight Intrusion Detection for Networks”, November 1999- Seattle, WA
[4] PengNing, Sushil Jadodia, Intrusion Detection Techniques.
[5] L. Todd Heberlein, and Karl N. Levitt, Network Intrusion Detection Biswanath Mukherjee, IEEE Network MayiJune 1994
[6] Wenke Lee, Salvatore J. Stolfo, Combining Knowledge Discovery and Knowledge Engineering to Build IDSs.
[7] Detecting Computer and Network Misuse through the Production-Based Expert System Toolset (P-BEST). In Proceedings of the 1999 IEEE Symposium on Security and Privacy, Oakland, California, May 9–12, 1999.