Intrusion detection system for Slowloris Attack

Abstract— **The usage of web services has increased rapidly amongst the people as it leads to the increment in the productivity, especially in areas such as e-business (on-line transactions). Web application attacks are growing rapidly and are becoming difficult to detect despite the availability of ingenious intrusion detection methods. The need for defense mechanisms against these threats led to the introduction of Intrusion detection systems (IDS). We introduce a novel method of intrusion detection for SlowDoS attacks using Ontology-based model with the intent to create linked data of the flat data, get better accuracy as well as to trace the attacks by knowledge acquisition.**

I. INTRODUCTION

There are many different types of SlowDoS attacks that are currently affecting big companies as they work in an insidious manner eventually leading to the denial of service. The SlowDoS attacks are increasing at a very heavy rate and are also difficult to detect as compared to other DoS attacks. Hence, not many intrusion detection systems have been constructed.

In order to detect the SlowDoS attacks we proposed a model where we try to detect the SlowDoS attack using one of the subsections of artificial intelligence called as the ontology. We try to use the concept of ontology for creating the intrusion detection systems.

Section 2 and 3 describes the different types of intrusion detection systems and the SlowDoS attacks. The next section talks about the researches done in the Ontology based intrusion detection systems and other systems that have been proposed until now for SlowDoS attacks. Section 5 talks about the proposed system and section 6 discusses the methodology of the proposed system in detail. Section 7 discusses the results followed by conclusion and future plans.

II. INTRUSION DETECTION SYSTEMS

With the emergence of Web 2.0, increased information sharing through social networking and increasing business adoption of the Web as a means of doing business and delivering service, websites are often attacked directly. An Intrusion Detection System(IDS) is a Network Security technology originally built for detecting vulnerability exploits against target application or computer.

A. Types of IDS

1) Based on Application::

a) : **Host Intrusion Detection System(HIDS)**: Host intrusion detection systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected.

b) : **Network Intrusion Detection System (NIDS)** Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

c) : **Distributed Intrusion Detection System (DIDS)** A distributed IDS (DIDS) consists of multiple Intrusion Detection Systems (IDS) over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data.

2) Based on Methodology:

a) : **Signature Based IDS**: Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware.

b) : **Anomaly Based IDS**: An anomaly-based intrusion detection system, is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.

III. SLOW DENIAL OF SERVICE(DOS) ATTACKS

The goal of a Denial of Service (DoS) attack is to make a particular network resource unavailable to its users by temporarily or indefinitely disrupting services of the host providing the network resource.

The general consensus about commencing a DoS attack is that one must deploy massive resources to generate massive traffic. However, there are a particuler set of DoS attacks known as Slow Denial of Service (Slow DoS) that do not need much resources but do achieve the objective. They do this by a small stream of very slow traffic. They target thread-based servers with an aim to tying every thread to a slow request in order to deny any service to genuine users. The slow requests are such that they ensure that the data pertaining to requests are sent slowly, but fast enough to prevent any connection timeout.

These class of attacks appear legitimate as per protocol and network rules, thus bypassing any standard form of security checks that are used to detect DoS attacks. These attacks require real time awareness of the resources consumed by the servers and the nature of connection and requests coming to them over time.

Slowloris is one of the SlowDos attacks that rely on HTTP protocol. The attack uses the fact that a server can accept

HTTP requests containing incomplete headers, thus waiting for the entire header content, keeping the connection open. Slowloris achieves DoS by slowly sending just incomplete HTTP header contents. The headers are sent at intervals short enough to prevent a connection timeout. The two most common tools used to commence a Slowloris attack are slowhttptest and slowloris.

IV. Literature Survey

Junhan Par et al [1] analyzed Slow Read Dos Attack with Countermeasures on web servers They analysed HTTP Slow Read Dos attacks on normal systems. Further experiments on systems reinforced with ModSecurity showed that single attacker system based on HTTP Slow Read Dos were being detected.

Imran Sharafaldin et al [2] generated a new intrusion detection dataset along with traffic characterization as per different attack tools used for the same. They have also used Machine learning techniques to extract important features for each class of attacks characterized.

Hossein Hadian Jazi et al [3] proposed detecting HTTP based attacks using sampling which is a novel method for novel detection approach for application layer DoS attacks based on nonparametric CUSUM algorithm.

Danny Velasco Silva et al [5] conducted a review and analyzed the principle issues, challenges and extent of progress related to distinct ontologies built for specific requirements in network security.

Amina Souag et al [4] conducted and exhaoustive survey of 50 ontological models developed for network security and analysed their use for requirements definition.

Jeffery Undercoffer et al [6] proposed a novel modeling technique for computer attacks that use Ontology for Intrusion Detection. Undercoffer also talked about why and how Ontology can be well integrated with IDS. However, his proposed idea was more inclined towards DDOS attacks than normal DOS attacks. We try to build up on his ideas and try use it with Slow DOS attacks.

Sumit More et al [7] presented a situation-aware intrusion detection model that integrates these heterogeneous data sources and build a semantically rich knowledge-base to detect cyber threats/vulnerabilities.

Abdul Razzaq et al [8] proposed Semantic security against web application attacks system using Ontology that successfully detects web application attacks whilst generating few false positives. He developed a methodology using which we can find the accuracy rates of the attacks and has compared it to the existing IDS.

Abdul Razzaq et al [9] in his later paper proposed a hybrid system with Ontology base and Bayesian Filter for effective defenses against the application level attacks.

Sherif Saad et al [10]proposed a semantically aware attack scenario reconstruction method that uses common ontology for knowledge sharing of different alerts being reported by systems and for deriving inferences about correlation between multiple alerts. It makes use of Ontology for tracing the attacks by using the alert methodology.

V. Proposed system

In order to detect the slowloris attack we propose the following model.

A. Packet sniffing

We created our own dataset by setting up the attack using two virtual machines. We collected the TCP dump and got the required information about the packets which we needed to analyze further.

B. Feature extraction

With the packet information that we had gathered we needed to extract the required features from the entire information available. Here we observed patterns and extracted the required features based on the analysis of the slowloris attack.

C. Ontology

After the main features were selected we constructed an Ontology for the intrusion detection systems with proper relations.

D. Semantic rules

Based on the features and the patterns observed we constructed semantic rules for the ontology in order to detect the malicious packets.

E. Detection

In the detection part we passed a dataset into the ontology for checking if the malicious packets were being detected or not.

VI. Methodology

A. Ontology

a) : **Knowledge Representation:** The subset of Artificial Intelligence whose main purpose is to capture the semantics of properties, concepts, individuals and relationships of specific knowledge domains is called as Knowledge Representation.

b) : **Description Logics** DAML+OIL, RDFS, and OWL support a family of knowledge representation languages called description logics (DL). These are the knowledge representations that are used in Protege to represent the Ontology and the individuals.

c) : **OWL** For representing the knowledge based Web ontology language is the one currently used. The Web Ontology language is used to represent everything in form of RDF Triples.

d) : **Knowledge Base** A description logic knowledge base is the equivalent of a theory in first-order logic or an ontology in OWL. Definition (Knowledge Base). A DL knowledge base K is a triple T, A, R where

1) T is a set of terminological axioms (TBox)
2) A is a set of assertional axioms (ABox)
3) R is a role box (RBox)

e) : **Definition of Ontology** Ontology is a conceptualization that describes mapping between computer representation of symbols and the human vocabulary, which consists of individuals and the relations between them in a hierarchical form. It provides a particular abstraction of the world and notation for that abstraction. In AI, an ontology is a specification of the meanings of the symbols in an information system. The primary purpose of an ontology is to document what the symbols mean the mapping between symbols (in a computer) and concepts (in someones head). Given a symbol, a person is able to use the ontology to determine what it means. When someone has a concept to be represented, the ontology is used to find the appropriate symbol or to determine that the concept does not exist in the ontology. The secondary purpose, achieved by the use of axioms, is to allow inference or to determine that some combination of values is inconsistent.

B. *Technologies for Ontology based IDS System*

a) : In order to build an Ontological model, using existing tools was required. All the tools which were used as a part of this project are Open source Tools and their entire code is available on Github pages.

b) : **Protege** : Developed by Stanford to build Ontologies. It offers support for turtle and OWL formats in order to represent the Semantic Data.

c) : **Google Refine** : Currently known as Openrefine, we made the use of Google refine v2.5 as it offers support for converting flat data into RDF triples format.

d) : **Apache Jena** : We used the Apache JENA API with Protege in order to Query the Ontology with instances fed in it to obtain results. We used SPARQL Queries for getting the required results.

e) : **Wireshark** : In order to capture the data for the Slow DoS Attacks, Wireshark is used for packet capturing after the set of two networks.

f) : **5. CICFlowmeter** : Designed by researchers working on IDS, we pass packets through wireshark and we obtain 83 features related to the packets we have passed in order to obtain a proper labelled dataset with features.

We created our own data set and used the official dataset for studying the data and making rules in order to put constraint on the classes that we create on our Ontology.

The previous data set was ICSX, which contained DoS Attacks and also Slow DOS attacks along with it created by the researchers in University of New Brunswick. In year 2017, they created another data set which features all the types of Slow DOS attacks such as Slowloris, SlowHTTP etc.[1] We used this dataset to observe the behavior of Slowloris accordingly.

We observed a pattern according to which the detection of malicious packets depended on the Total Backward packets and the forwards packets

In order to construct an Ontology we used a tool by Stanford called as Protege. Fig 1. illustrates the Attack Ontology that we constructed for SlowDoS attacks. The diagram is displayed with the use of an API called as Ontograph.

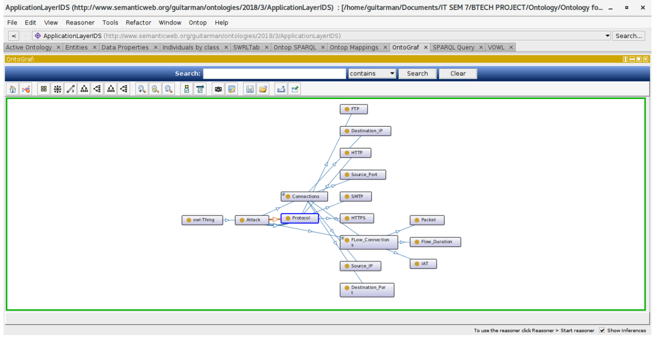
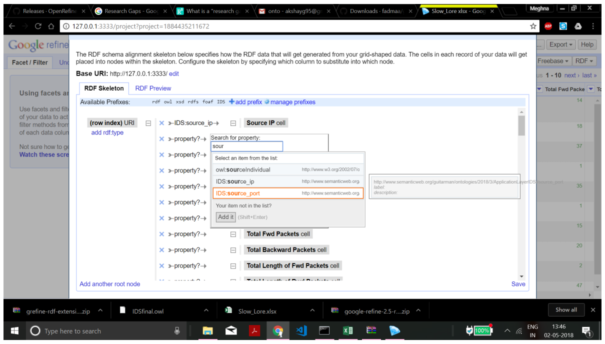


Fig. 1. Ontology using Ontograph



The RDF schema alignment skeleton below specifies how the RDF data that will get generated from your grid-shaped data. The cells in each record of your data will get placed into nodes within the skeleton. Configure the skeleton by specifying which column to substitute into which node.

Base URI: http://127.0.0.1:3333/ edit

RDF Skeleton | RDF Preview

Available Prefixes: rdf owl xsd rdfs foaf IDS +add prefix manage prefixes

(row index) URI — add rdf:type
- IDS:source_ip → Source IP cell
- property? → Search for property: sour
- property?
- property?
- property?
- property?
- property?
- property? → Total Fwd Packets cell
- property? → Total Backward Packets cell
- property? → Total Length of Fwd Packets cell

Select an item from the list:
- owl:sourceIndividual http://www.w3.org/2002/07/o
- IDS:source_ip http://www.semanticweb.org
- IDS:source_port http://www.semanticweb.org

http://www.semanticweb.org/guitarman/ontologies/2018/3/ApplicationLayerIDS/source_port
label:
description:

Your item not in the list? Add it (Shift+Enter)

Add another root node — Save

Fig. 2. Adding data using Google Refine

For adding Data to the Ontology we need to convert the flat excel sheet data set into an RDF format and create Linkages between the data. For this, we used Google Refine as displayed in Fig 2.

After we obtained the complete Ontology with instances fed properly into it, we query them with the RULES that we had created initially while selecting the features we selected for the Ontology construction. We worked on SPARQL queries for obtaining or fetching the required data from the RDF file.

Using the obtained count as shown in figure we try to construct a methodology by setting a specific threshold value to get the accuracy rates.

VII. Results

Now that we have the above results of Machine Learning, let us analyze the data of Slowloris with respect to it's semantic aspect.

A. *Understanding Attack Behaviour*

1) Total Forward and Backward Packets: We want to detect whether a Slowloris attack is taking place or not. By observing how Slowloris functions, we know that it sends incomplete headers to the server to keep the connection open. This also means that it does not expect any response from the server (in the form of packets). So, the attack is done by making connections where the only response from server is for the handshaking and connection breakdown. This means

TABLE I

Query Results for a Particular Source IP

Source IP	Z is less than 0(A)	Z is greater than 0(B)	Z Total
172.16.0.1	5654	142	5796
192.168.10.15	5	3	8
192.168.10.25	15	1	16

that the total forward packets(TFP) would be greater or equal to the total backward packets(TBP). This is not the usual case in legitimate connections which contain HTTP GET requests

2) Analysis through Correct Ratio: So in order to identify if its a Slowloris attack, we need to check how many connections per set of Source and Destination IP have this condition satisfied. If it greater than a particular threshold those who do not, we assert that a Slowloris attack is in work.

3) Pertaining to Legit Connections: There might be legitimate connections that may satisfy the above condition. To eliminate that possibility we should to check only when the no of connections per set of IP (source and destination) is greater than 200 as through experiments done by us, Slowloris managed to bring down a server by creating just 200 connections.

B. *Query Results*

We appropriately Queried the linked data to obtain the count of connections which satisfy the condition on TFP and TBP for a given connection pair from our dataset known to be that of Slowloris. Note that we are checking the count for this condition only if the prototcol used is HTTP. As per this condition and the web server's network traffic stats we have considered for Slowloris from the dataset (ie 192.168.10.50), the query results are as given below. Here Z is the value of TBP - TFP

C. *Observing the Ratio*

Since we need to check further only those IP connections whose total is greater than 200, we only need to check further that of IP 172.16.0.1 with the web server. We use the results from the table above to define the following ratio.

$$R = \frac{A}{B} \tag{1}$$

If this R is beyond a given threshold we assert that the connections made with this IP are intended for commencing a Slowloris attack. We have kept the threshold as 10 which means that if there are 10 times more connections than those that have Z greater than zero, then it is a SlowLoris attack. With respect to our Slowloris dataset we analyzed, the value of R came out to be close to 40, which indicates there are 40 times more connections which are suspicious. The remaining benign connections failed to satisfy the threshold limit.

VIII. Conclusion

We built an Ontology to contain our dataset which provided semantic meaning to the data. We built rules based on this data which were based on behavioral observations and wrt our data set gained near 100 percent accuracy.

IX. Future Work

A. *Continuing the same methodology*

There exist three more types of Slow DOS attacks, We can extend the same methodology using Ontology, to create rules for other SlowDoS attacks existent out there. eg: slow POST, Slow Read.

B. *Other ideas*

From what we read and understood, Ontology seems more like a method that can be used to accelerate or make other existing methodologies work better.
There is still much left to explore in this field that we need to understand using which we can develop ideas as to how we can make use of it in better ways.

References are important to the reader; therefore, each citation must be complete and correct. If at all possible, references should be commonly available publications.

References

[1] H. T. Junhan Park, Keisuke Iwai and T. Kurokawa, Analysis of slow read dos attack and countermeasures on web servers, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(2): 339 353, 2015.

[2] A. G. Imran Sharafaldin, Arash Habibi, Towards generating a new intrusion detection dataset and intrusion traffic characterization, Canadian Institute of Cybersecurity(CIC), 2018.

[3] N. S. A. A. G. Hossein Hadian Jazi, Hugo Gonzalez, Detecting http based application layer dos attacks on web servers in the presence ofsampling, Faculty of Computer Science, University of New Brunswick, 2017.

[4] Amina Souag, Camille Salinesa, Isabelle Wattiau, ”Ontologies for Seurity Requirements: A literature survey and classification (long version)”, 2012

[5] D. V. Silva and G. R. Rafael, Ontologies for network security and future challenges, s University National of Chimborazo, Ecuador University National Mayor of San Marcos, 2015.

[6] J. U. A. Joshi and J. Pinkston, Modelling computer attacks : An ontology for intrusion detection, RAID, 2003.

[7] A. J. T. F. Sumit More, Mary Matthews, A knowledgebased approach to intrusion detection modeling, ., 2012.

[8] H. F. A. A. H. Z. A. P. C. B. Abdul Razzaq, Khalid Latif, Semantic security against web application attacks, Information Sciences Volume 254, 2014.

[9] F. A. N. H. Abdul Razzaq, Ali Hur, Ontology based application level intrusion detection system by using bayesian filter, IEEE, 2009.

[10] S. Saad and I. Traore, Semantic aware attack scenario reconstruction, Elsevier, 2013.