Method of Construction of Fuzzy Tree of Solutions for Network Protection Against DoS-Attacks

Oleksandr Tymchenko[1], Bohdana Havrysh[2], Andrian Kobevko[2] and Orest Khamula[3]

[1.] *University of Warmia and Mazury Olsztyn, ul. Michała Oczapowskiego 2, Olsztyn,10-719, Poland*
[2.] *Lviv Polytechnic National University, Stepana Bandery Str, 12, Lviv 79013, Ukraine*
[3.] *Ukrainian Academy of Printing, Lviv, Pidholosko st., 19, 79020,, Ukraine*

Abstract

An Intrusion Detection System is a tool that can detect intrusions into a host, network, and application. DoS attack is one of the most common network attacks. During this time, the host sends a huge number of packages per machine and thus slows down the network and the host. There are a number of algorithms for detecting DoS attacks, and most of these solutions generate a high number of false alarms. The paper considers a new method of constructing a fuzzy solution tree for monitoring network flow in case of Smurf, Mail-Bomb and Ping-of-Death attacks. Intrusion Detection System (IDS) is a tool that can detect instances of intrusion into a host, network, and application. DDoS attack is one of the most common network attacks. During it, hosts send a huge number of packages per machine and thus slow down the network and host. There are several algorithms for detecting such attacks, and most of these solutions are based on mechanisms to generate a high number of false alarms. Most anti-attack solutions are monitoring and analyzing packages within the network instead of network traffic. The paper proposes a fuzzy decision tree that can detect four types of DDoS attacks by analyzing the network flow. The proposed architecture is the basis for the development and implementation of a protection system.

Keywords

Algorithms, DoS-attacks, fuzzy tree of solutions, network protection, mechanism

1. Introduction

Computing systems are used to solve a large number of problems in management and production. However, the performance and speed of a single physical server is in some cases insufficient, so cloud servers, or environments that combine the resources of many physical servers, are becoming popular. Such a powerful virtual system has a number of significant advantages when performing more tasks, but its complexity leads to greater vulnerability. Denial of Service (DoS) or Distributed Denial of Service (DDoS) are the main threats to access to virtual cloud servers, which can significantly reduce the performance of cloud services by damaging virtual servers. The rapid

CITRisk'2021: 2nd International Workshop on Computational & Information Technologies for Risk-Informed Systems, September 16–17, 2021, Kherson, Ukraine
EMAIL: olexandr.tymchenko@uwm.edu.pl (O.Tymchenko); dana.havrysh@gmail.com (B.Havrysh); email3@mail.com (A.Kobevko); khamula@gmail.com (O.Khamula)
ORCID: 0000-0001-6315-9375 (O.Tymchenko); 0000-0003-3213-9747 (B.Havrysh); XXXX-XXXX-XXXX-XXXX (A.Kobevko); 0000-0001-7596-0813 (O.Khamula)

increase in the number of DoS attacks on hosts, networks or applications encourages researchers to create an effective way to stop them. The obvious solution is to create a system that detects intrusions with the least error and quickly enough. The frequency of detection of erroneous results does not satisfy users, especially for detection systems based on the analysis of anomalies.

The purpose of the article. Identify and classify the main threats from DDoS attacks and protection mechanisms against them. Build a fuzzy tree of solutions to monitor network flow in the event of Smurf, Mail-Bomb and Ping-of-Death attacks.

2. Main part

The sharp increase in the number of users and ISPs leads to a decrease in network security, so service providers are always looking for solutions to monitor and verify packages coming from the client side to avoid any attacks.

The security mechanisms used in the network must prevent any attack. As it cannot completely prevent attacks, a new level of security is needed to detect and stop the attack as soon as possible [1, 2].

In 2009, the US National Institute of Standards and Technology (NIST) defined cloud computing as a "model for providing convenient on-demand network access to a shared environment of configured computing resources that can be quickly provided and released with minimal management or service provider interoperability." Payment for usage, virtualization, access to demand, flexibility and reduced costs for equipment and maintenance - factors that contribute to the popularization of cloud computing. An Infrastructure as a Service (IaaS) is a service model that allows users to deploy and run arbitrary software, which may include operating systems and applications. Virtualization plays a major role in cloud computing through the efficient and systematic use of existing equipment. Virtualization is used at various stages, including network, processor, memory, storage, and so on. This reduces cost and allows you to create an affordable and flexible system.

DDoS attack is the main threat to availability. An attacker could significantly degrade or completely destroy a user's network connection. To perform an attack, an attacker first creates many agents or hosts, and then uses these agents to launch an attack, loading the target network. The main purpose of a DDoS attack is to prevent the victim from using their resources. In most cases, the targets are web servers, processor, storage, and other network resources. In a cloud environment, DDoS can also significantly reduce the performance of cloud services by damaging virtual servers.

The Intrusion Detection System (IDS) dynamically monitors actions performed in a given environment, such as hosts and networks. It decides whether these actions are symptoms of an attack or whether they constitute lawful use of the environment. The two most common detection methods that can be used in IDS are signature-based detection and anomaly-based detection.

The signature-based detection technique in IDS looks for the characteristics of known attacks, and tries to find similarities between the previous behavior of the system or network with the characteristics of the known attack in the signature database. However, this technique cannot detect new attacks.

The anomaly detection technique takes the normal state of network traffic or host behavior as anomaly criteria. This approach can detect unknown attacks. This approach creates an error rate due to difficulties in determining the normal state of network traffic [2].

To detect intrusion, a number of researchers use artificial intelligence, data exchange and fuzzy clustering methods. Recently, fuzzy intrusion detection systems have proven noise resistance, self-learning ability, and the ability to build ground rules without the need for a priori knowledge.

Although there are various approaches to detecting DoS attacks. The practice of detection requires higher accuracy and efficiency. Therefore, there is an urgent task to improve the mechanism of detection of DoS-attacks by different algorithms.

Although there are various approaches to detecting DoS attacks, the practice of detection requires higher accuracy and efficiency. Therefore, there is an urgent task to improve the mechanism of detection of DoS-attacks by different algorithms.

2.1. DDoS attacks

DDoS attacks are initiated by a network of remotely controlled, well-structured and widely dispersed hosts - "zombies". They are also called secondary victims. In 2019, the victims of DDoS attacks were: Chinese websites, Wikipedia, Telegram, FBI, etc. Most of these attacks were distributed, ie they occurred simultaneously from a large number of IP addresses.

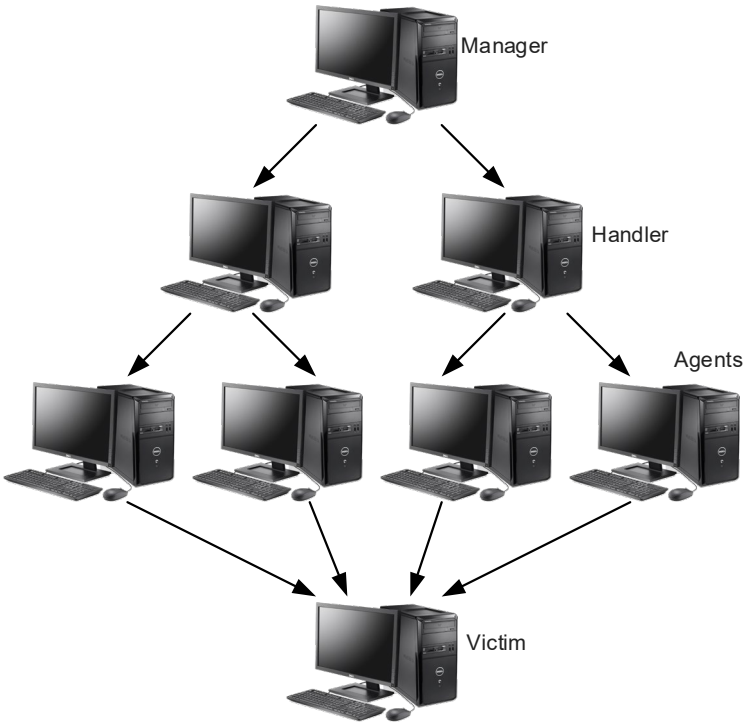

Figure 1: DDoS attack structure

2.2. DDoS attack structure

Internet bots are widely used to carry out DDoS attacks, ie client-server technology is used to launch a large number of "zombie" hosts. In general, a DDoS attack consists of a manager, handler,

agents, and victim (Figure 1). Zombies (agents or bots) are used by the leader to form internet bots. The strength of the attack depends on their number. The manager communicates with agents through handlers. Handlers, for example, can be programs installed on the affected devices (network servers) with which attackers communicate to send commands. An attacker sends a command and manages his agents through handlers. Bots - devices that are run by handlers, actually attack the victim's system [4-6].

Attackers use various scanning methods to find a vulnerable machine. The simplest strategy is to randomly scan for IP addresses because the virus does not know where the vulnerable host is. The method is only effective for IPv4 because the IPv6 address space is too large. When scanning the list, the attacker has a list of infected IP addresses.

When it makes another machine a host, part of the initial list of requests will be sent to it. Route-based scanning reduces search addresses using Border Gateway Protocol (BGP) prefixes. They reduce the amount of information in which the search takes place. With this technique, scanning is performed by different hosts in different parts of the address space, and thus saves resources. Other strategies are sometimes used, such as permutation scanning, local preference scanning, and topological scanning. Once a vulnerable host is detected, they find its vulnerability and gain control over it.

2.3. Classification

The variety of DDoS attacks is growing. The most common are attacks based on bandwidth and resources. These types consume all the bandwidth and resources of the network being operated. The results of the analysis of types of attacks are presented in figure 2. Depending on the vulnerability used, attacks can be divided into different types.

2.3.1. Bandwidth damage:

This type of attack consumes the bandwidth of the victim or the target system, loading unwanted traffic to prevent legitimate traffic from entering the victim's network [3]. Tools such as Trinoo are commonly used to carry out these attacks. Bandwidth attacks are further classified as:

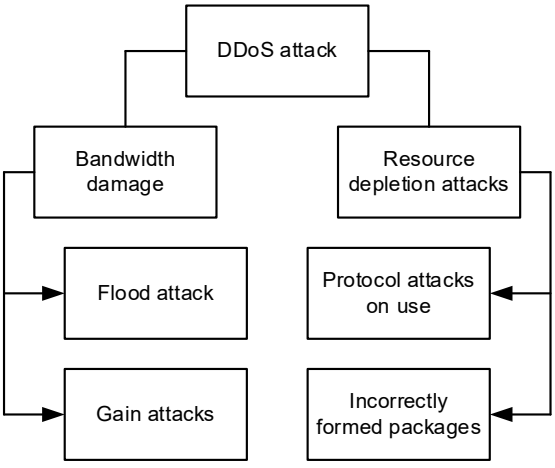

Figure 2: Classification of DDoS attacks

Flood attack:

The attacker sends a huge amount of traffic to the victim with the help of zombies, and thus overloads the network. The victim's system slows down quickly, preventing legitimate traffic from accessing the network. This is due to the UDP (User Datagram Protocol) and ICMP (Internet Control Protocol) packages [7, 8]. The UDP-flood attack consists of the following steps:

1. An attacker sends a large number of UDP packages to random or specified ports on the victim's system via zombies.
2. Upon receiving packages, the victim system looks for destination ports to identify programs waiting on the port.
3. It does not find the required programs and generates an ICMP package with the message "destination not available".
4. Return packages from the victim are sent to a fake address.

As a result of the attack, the available bandwidth of the system is exhausted and cannot be used by the victim. This affects internet connections and systems located near the victim. Varieties of this attack are: fragmentation, DNS flood attack, VoIP flood attack, media data flood, etc.

The ICMP flood attack consists of the following steps*:*

1. An attacker sends a large number of ping requests to the victim system using zombies.
2. The victim sends answers to the received inquiries.
3. The network is now jammed with traffic sent by the victim. Responses to requests can be sent to the fake IP address specified in the ICMP package.

As a result, the bandwidth of network connections is quickly depleted and cannot be used by the user. Also types of ICMP attack are: fragmentation, DNS flood and Ping-flood [9-11].

Gain attack

An attacker sends a large number of packages to a broadcast IP address. The router transmits these responses to requests to the victim's IP address, which results in a complete system lock. This type of attack uses the broadcast addresses of most devices that have access to the Internet, such as routers. This type of DDoS attack can be launched directly by an attacker, or with the help of zombies. The most famous attacks of this type were Smurf and Fraggle.

The Smurf attack consisted of the following steps:

1. An attacker sends packages to a network device with a broadcast address. The answer will be sent either to a fictitious address or to the victim's address.
2. ICMP_ECHO_RESPONSE packages are sent by the network amplifier to all broadcast IP address systems. This package assumes that the receiver will respond to ICMP_ECHO_REPLY.
3. The message ICMP_ECHO_REPLY from all systems in the range reaches the victim.

The Fraggle attack is similar to Smurf, but during which UDP is sent to ports that support character generation. It consists of the following steps:

1. An attacker sends UDP packages to a port that supports character generation. The return address in these packages can be the address of the victim's seventh port, which will generate characters and thus create an infinite loop.
2. The attack targets the ports of all systems to which the broadcast address refers.
3. All these systems in the range are repeated back to the port of the victim symbol generator.
4. This process is repeated because UDP packages are used.

Such an attack is more dangerous than Smurf. Its variety is a reflex attack that uses "reflectors" (intermediary hosts or devices) to perform a task. The peculiarity of the reflector is that it constantly responds to the packages it sends and receives [10]. Therefore, attackers use this method for attacks to which responses are required. The return address for the victim's response will be forged.

2.3.2. Resource depletion attacks

The resource depletion attack aims to deplete the resources of the victim system to make it impossible to serve users. There are the following types of resource depletion attacks:

Protocol attacks on use: the purpose of these attacks is the consumption of excess resources of the victim, using the peculiarity of the protocol established in the system. The most common attacks of this type are TCP SYN attacks, PUSH + ACK, authentication server attack and CGI requests [11, 13].

Improperly generated packages are processed with malicious information. The attacker sends these packages to the victim to hack her system. This can be done in two ways:

IP Address Attack: The package consists of the same source and destination IP address, creating chaos in the victim's operating system. Thus, the attack slows down and breaks the system [12].

IP Package Settings Attack: Each of the IP packages consists of additional fields to transmit additional information. The attack uses these fields to form a package. They are populated by setting all the quality bits to one. Therefore, the victim spends extra time processing this package. This attack is more vulnerable when attacked by more than one "zombie".

2.4. Protection mechanisms

There are various measures to prevent DDoS attacks. The initiator of DDOS-attacks is an attacker who tries to gain unauthorized access to the system / network of victims. Protective mechanisms are shown in figure 3.

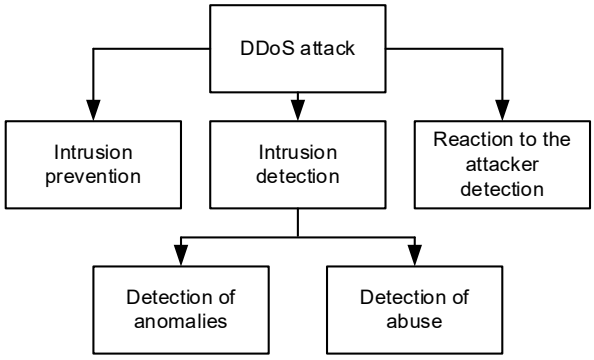

Figure 3: Mechanisms of protection against DDoS-attacks

Methods of prevention

The best strategy against any attack is to prevent it from occurring. One of the following techniques is the use of filters:

- Inbound filtering - this process stops incoming packages with an invalid source address. Routers are used for this purpose. This technique stops DDoS attacks caused by fake IP addresses.
- Output filtering - this technique uses an output filter. This technique allows packages that have a valid IP address in the specified network range to leave the network.
- Route-based package allocation - the filter uses route information to capture or filter fake packages. It is also used to track an IP address. But this requires global information about the network topology.
- Enhanced connection security is a distributed feature architecture that assumes that an incoming package is valid if it is from legitimate servers. Other packages are blocked. The client must log in to the network by re-accessing SOAP.

You can also prevent attacks by disabling unused services, applying security patches, changing your IP address, disabling IP broadcasts, and balancing downloads and traps. Attack prevention methods do not guarantee complete protection against DDoS attacks, but increase security [14, 15].

Detection methods

The intrusion detection system helps the victim to avoid the spread of DDoS attacks and prevents the system from shutting down. Among the following methods:

1. Detection of anomalies: This method detects attacks by recognizing abnormalities in the system. This is done by comparing the current values with the previously detected normal operating characteristics of the system. This method determines erroneous values in system behavior. The most common methods of detecting anomalies are:

- NOMAD – a network monitoring system that detects network anomalies by analyzing IP package header information.
- Package's selection and filtering technique packages with congestion. A statistical analysis was performed on a subset of dropped packages, and as soon as an anomaly is detected, a signal is sent to the router to filter out malicious packages.
- D-WARD – detects a DDoS attack in the first victim. This prevents the attack from spreading to other network users. D-WARD is installed on the router to detect incoming and outgoing network traffic.
- MULTOPS- MULTOPS – is a data structure designed to detect DDoS attacks. It detects attacking or attacked systems, operating in an attack-oriented mode and its victim, respectively. This is a multi-level structure that determines the speed of packages at different levels of aggregation. But this requires a router configuration and additional memory management schemes.

2. Detection of overuse: This method detects DDoS attacks by supporting a database of addresses or exploit templates. When such a pattern is detected, the system reports DDoS attacks.

Response to detection

If a DDoS attack is detected, it should be blocked and the identity of the attacker identified. This can be done, for example, using the Access Control List (ACL) or automatically [16-18].

Some methods used to track and identify the attacker are given in table. 1. Note that there are many methods to stop DDoS attacks, but not all attacks can be detected and prevented, in reality you can only reduce the impact of the attack.

Table 1
Methods for tracking DDoS attacks

Method	Description
ICMP tracking	The mechanism involves forwarding packages with a low probability to each router, as well as sending an ICMP feedback message to the destination. If the bulk of ICMP messages used to identify an attacker face issues such as additional traffic, verifying these packages and identifying overhead information from the route map is difficult
IP- tracking	This method tracks the attacker's path to find the origin of the attack. In this technique, the attacker's path is traced back to find its source. But this becomes a difficult task if the reporting of sources in the TCP / IP protocol is disabled
Reverse link testing sequence	This mechanism checks each of the incoming links to determine if it is an attack. To do this, a large flow of traffic is created and the presence of violations in the network is monitored. To use this mechanism, you need a system that can generate a large flow of traffic, as well as information about the location and connection of network computers
Probabilistic marking of packages	This technique overcomes the disadvantages of feedback testing because it does not require prior knowledge of network topology, traffic size, etc. This advantage also imposes additional costs on the system, but there are many methods to avoid additional costs

2.5. Problem solving methodology

The process of solving this problem is divided into stages of design and analysis. After defining the goals, previous research and methods used by different researchers are studied. A system based on these studies is then developed to improve protection. The second stage, called analysis, determines the effect of design and its impact on system improvement.

In the developed algorithm fuzzy logic processes the data received from a network stream to find the intrusion. The data for the study is the information accumulated after the detection of attacks. Basic and general information about IDS is collected, and then a conclusion is made about DDoS attacks and their behavior. These studies show two important problems in IDS - low speed and slow detection of DDoS attacks.

The proposed solution is to monitor the flow of the network using a fuzzy system to increase the speed and quality of detection of DDoS-attack.

Modeling

At this stage, related work is investigated and the mechanism of such systems is analyzed in detail to determine which mechanism should be used to detect DDoS attacks. Most DDoS attacks have their own signature, so the detection rate on this basis is higher.

The system is configured to achieve the goals that were set at the stage of identifying the problem, as well as to take into account the information collected. Note that the designed component must have the correct output from each module and the entire system (attack report).

Analysis

The system monitors network traffic and considers all packages in the stream. A fuzzy algorithm finds a suspicious package and stores these threads in an array. Finally, the fuzzy decision tree checks the headers of the suspicious thread and in the event of an attack, the system generates an error.

It is advisable to check the speed and efficiency of the developed system on a sample of traffic provided by the Agency for Progressive Defense Research Projects (DARPA) from the Lincoln Laboratory of the Massachusetts Institute of Technology (MIT). The result will be the development of a fuzzy algorithm to detect attacks.

System development

Consider in more details, what processes affect the performance and accuracy of the system. First, we describe the system architecture, then - fuzzy algorithm and network flows, the application of fuzzy algorithm and network flow on IDS, the speed of attack detection is analyzed.

Protection system architecture

In fig. In Fig. 4 shows the structure of the developed system. IDS collects all packages from the traffic sample and places them inside the streams to store in memory. A fuzzy selection algorithm collects any suspicious packages and assigns them to a suspicious stream. Each time a suspicious thread ends, a fuzzy algorithm will check it for an attack.

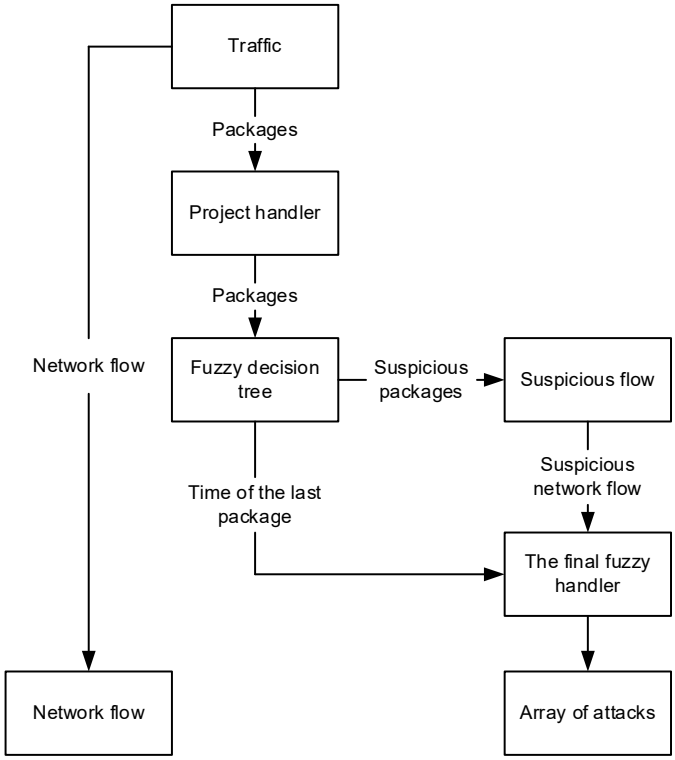

Figure 4: Block diagram of the system

Data for pre-processing

TCP and ICMP packages from the network are used where network flows are formed by the network handler. Stream identification for TCP packages is based on the number of packages from a single source, destination, source port, and destination port. The process starts with the SYN

package and ends when the FIN package arrives. On the other hand, for the ICMP protocol, two types of packages can be defined. The first package contains a request from one machine to another, and the second package is a response to the request. The network flow handler checks the network flows for any anomalies.

The most common IDS problems are error detection error and attack skip error, detection speed, performance, and overall performance. By using a network stream for the input signal and using a fuzzy intrusion detection solution tree, the result can have fewer false-positive errors and a better detection rate.

Each attack is described below.

1. Land attack

If TCP is the protocol of the incoming package, and the source IP and the target IP are the same, the source port is equal to the destination port, there is a Land attack.

2. Mail Bomb attack

An attack occurs by establishing a single TCP connection between two computers. In this stream, the SMTP port is used to send e-mail, but the number of packages in one stream can be 10,000 packages and the size of each package is 1,000 bytes. Thus, the stream size will be approximately 10 MB.

3. Smurf attack

The attack takes place via an ICMP stream. The number of packages in one thread is small, but the size of each package is approximately 1000 bytes. However, the flow will be large because several computers send a large package to one computer. The package contains a response message, but the message request is not sent by the victim.

4.Ping packages attack

A large number of large IP packages are sent from one computer to another. Each package has about 1,000 bytes and the size of the attack stream is about 64,000 bytes. It uses the ICMP protocol, which causes the victim's machine to reboot, freeze, and crash.

Fuzzy sets usually consist of 0 and 1, so there can be only two possible answers. But in fuzzy logic, when combining several fuzzy sets, there may be several answers. Therefore, the fuzzy handler looks for suspicious packages to change the flow state from normal to suspicious for faster detection:

Rules are used for Land attacks

IF flowprtcl is equal to TCP
IF flowrc is equal to flowdest
Write to the Land Attack array

The following rule applies to Mail Bomb attacks:

IF flowprtc is equal to TCP
IF the flowdestPort is SMTP
IF streams> 10 MB
Write to the Mail Bomb attack array

The following rule applies to the Smurf attack:

IF flowprtc is equal to ICMP
IF the information contains an answer
FOR A last minute Package, follow this Package one by one
IF the information does not contain a Request from the same machine
Write to the Smurf attack array

To attack with ping packages, the rule is:

IF flowprtc is equal to IP
If the information contains ICMP
Write to the Ping of Death array

3. Conclusions

A fuzzy solution tree is proposed, which can detect four types of DDoS attacks by analyzing the network flow. The proposed architecture is the basis for the development and implementation of a protection system. The experiments were performed using the DARPA data set.

Previous IDS decisions were based on a detection method that used package data and resulted in erroneous errors. This study used IDS to solve the problem using a fuzzy decision tree as a preprocessor and inbound network flow analysis.

In the proposed system, all packages are processed, and then network flows are built. During this time, the fuzzy handler stores all suspicious packages in memory. When a thread header is generated, the suspicious thread will be checked again by a fuzzy handler and attacks will be detected.

References

[1] C.Marsala, M.Rifqi, Fuzzy decision tree and fuzzy gradual decision tree: Application to job satisfaction, 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2017, pp. 1-6, doi: 10.1109/FUZZ-IEEE.2017.8015740

[2] P.Su, T.Chen, H.Mao, J.Xie, Y.Zhao, J.Liu, On the Application of Preaggregation Functions to Fuzzy Pattern Tree, 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2019, pp. 1-6, doi: 10.1109/FUZZ-IEEE.2019.8858922

[3] P.Su, T.Chen, H.Mao, J.Xie, Y.Zhao, J.Liu, On the Application of Preaggregation Functions to Fuzzy Pattern Tree, 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2019, pp. 1-6, doi: 10.1109/FUZZ-IEEE.2019.8858922

[4] S.Sardari, E.Ahmadi, M.Taheri, M.Z.Jahromi, Weighted Fuzzy Decision Tree for Multi-Label Classification, 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), 2020, pp. 169-174, doi: 10.1109/ICCKE50421.2020.9303626

[5] R.Tkachenko, I.Izonin, N.Kryvinska, V.Chopyak, N.Lotoshynska, D.Danylyuk, Piecewise-linear Approach for Medical Insurance Costs Prediction using SGTM Neural-Like Structure, CEUR-WS.org, vol. 2255, 2018, pp.170–179

[6] L.Fang, H.Jiang, S.Cui, An improved decision tree algorithm based on mutual information, 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), 2017, pp. 1615-1620, doi: 10.1109/FSKD.2017.8393008

[7] G.Zheng, X.Xu, J. Yan, SD-CRF: A DoS Attack Detection Method for SDN, 2020 IEEE 20th International Conference on Communication Technology (ICCT), 2020, pp. 1116-1120, doi: 10.1109/ICCT50939.2020.9295801.

[8] M.T.Kurniawan, S.Yazid, Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System, 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2020, pp. 1-5, doi: 10.1109/ICECCE49384.2020.9179255

[9] M.J.Anagha, R.Lepakshi, V.Goutham, V.Thavish, T.G.Keerthan Kumar, Package Injection and Dos Attack Controller Software(PDACS) Module to Handle Attacks in Software Defined

Network, 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 966-970, doi: 10.1109/ICCMC48092.2020.ICCMC-000179
[10] Y.Tsymbal, R.Tkachenko, A digital watermarking scheme based on autoassociative neural networks of the geometric transformations model, in: 2016 IEEE First International Conference on Data Stream Mining Processing (DSMP), 2016, pp. 231–234. ttps://doi.org/10.1109/DSMP.2016.7583547
[11] M.Nazarkevych, Y.Voznyi, V.Hrytsyk, I.Klyujnyk, B.Havrysh, N.Lotoshynska, Identification of Biometric Images by Machine Learning, 2021 IEEE 12th International Conference on Electronics and Information Technologies (ELIT), 2021, pp. 95-98, doi: 10.1109/ELIT53502.2021.9501064.
[12] O.Tymchenko, B.Havrysh, O.Khamula, S.Lysenko, K.Havrysh, Risks of Loss of Personal Data in the Process of Sending and Printing Documents, CITRisk (2020), CEUR Workshop Proceedings, 2805, 2020, pp. 373–384
[13] M.Elkano, M.Uriz, H.Bustince, M.Galar, On the Usage of the Probability Integral Transform to Reduce the Complexity of Multi-Way Fuzzy Decision Trees in Big Data Classification Problems, 2018 IEEE International Congress on Big Data (BigData Congress), 2018, pp. 25-32, doi: 10.1109/BigDataCongress.2018.00011
[14] J.Rabcan, P.Rusnak, Generation of structure function based on ambiguous and incompletely specified data using the fuzzy decision trees, 2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2017, pp. 1-7, doi: 10.1109/ICETA.2017.8102521
[15] H.Yang, D.Ye, Observer-Based Fixed-Time Secure Tracking Consensus for Networked High-Order Multiagent Systems Against DoS Attacks, in IEEE Transactions on Cybernetics, doi: 10.1109/TCYB.2020.3005354
[16] O.Tymchenko, O.O.Tymchenko, B.Havrysh, O.Khamula, O.Sosnovska, S.Vasiuta, Efficient Calculation Methods of Subtraction Signals Convolution, 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), 2019, pp. 1-4, doi: 10.1109/CADSM.2019.8779250
[17] E.Cambiaso, G.Papaleo, G.Chiola, M.Aiello, Mobile executions of Slow DoS Attacks, in Logic Journal of the IGPL, vol. 24, no. 1, 2016, pp. 54-67, doi: 10.1093/jigpal/jzv043
[18] W.Zhe, C.Wei, L.Chunlin, DoS attack detection model of smart grid based on machine learning method, 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS), 2020, pp. 735-738, doi: 10.1109/ICPICS50287.2020.9202401