American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-5, Issue-10, pp-175-180
www.ajer.org
Research Paper Open Access

ICS: An Optimized IDS Mechanism for DDoS Attacks Mitigation

Hamed Nasser Al-Busaidi[1], Mohamed Abbas[2], Kareemullah Sheik[3]
[1]*PG Student, Mazoon College, Muscat, Oman*
[2]*Head, Dept. of CS & IT, Mazoon College, Muscat, Oman*
[3]*Lecturer, Dept. of CS & IT, Mazoon College, Muscat, Oman*

ABSTRACT: *Today, Distributed Denial of Service (DDoS) become a global fear that threat a wide variety of enterprises. Unfortunately, most of small and medium sized enterprises around the world are not well prepared for such type of attacks. While DDoS Monsters grow up in tremendous manner, there are a new methods born in order to defeat against it. DDoS methods can be categorized based on attack type as Signature based, Anomaly and Hyper schema can be also adopted. The ultimate objective of our proposed schema is to detect unknown attack signatures and to be ready for the new generation of DDoS tools.*
Keywords: *Distributed Denial of Service; Filtering; Confidence; Correlation Pattern; ICS Score.*

I. INTRODUCTION

Distributed Denial of Service (DDoS) attack is a serious problem that affects thousands of companies around the world. The sad story begins dramatically when an attacker sends a lot of requests to victim's machine to establish multiple half open-connections in order to overload a service of existed resources, which prevent any new legitimate connection. Attackers can achieve this work by controlling several active machines remotely which called zombies or bots, using malicious tools. They can play them together as botnet-army, a group of cooperative zombies, in full-automatic mode, semi-automatic or manually at real-time of event.

While DDoS attacks become more challenging now days, many defense mech-anisms were proposed which can be catego-rized into two major branches: detection and prevention. These branches can be roughly categorized by deployment based as: 1. Source based, 2. Destination based, and 3. Network based as mentioned on [1]. The method proposed here is source-based. PacketScore [3] is a static-based schema which proposed for detecting anomaly DDoS attacks. It depends on Bayesian theory to calculate packet score and then compare it with its scorebook. PacketScore schema has high rate of detection accuracy and good overload control at high speed. However, it has low performance rate at high-intensity of attacks traffic due to score calculation complexity.

ALPi [4] proposed two schemas the LB and AV in order to enhance the PacketScore [2] method. These schemas have better performance rate than CLP [3] of PacketScore at high volume of DDoS attacks. But they are useless against any teardrops or ping-of-death attack due to the lack of attack intensity variance. CBF [5] is confidence-based filtering approach which count packet score by comparing resulted CBF Score with discarding threshold in order to accept or reject the captured packet. At attack-period, CBF can be considered the faster method among previous methods [3] [4]. On comparison to PacketScore [3], this schema has some degradation on TCP-SYN flood attack.

Today, all of our necessary and luxury needs can be achieved through the Internet, which can vary from online shopping to Mobile banking. However, hackers are ready to disrupt large business as well as individual customers from reaching the desired services. Our method objective is to improve the detection speed of illegitimate packets by reducing number of attributes involved in correlation patterns. The proposed schema will offer a better performance and minimize consumption of system resources at real time filtering.

This paper is organized as follows: in section 2, we will introduce our ICS, the Iceberg Confidence Schema approach, with key terms and some definitions regarding ICS basic concepts. In the next two sections, Section 3. and 4 we will explain in more details about our filtering approach from generating the nominal profile till selecting a suitable discarding strategy against illegitimate packets. In the last section, Section 5, ICS performance evaluation results are shown up with analysis.

II. AN OVERVIEW OF ICEBERG CONFIDENCE SCHEMA

1. Basic Concepts of ICS

In order to understand our proposed schema smoothly, we list the key terms with its description in Table 1.

Definition 1 (Correlation Pattern). Correlation Pattern is a key factor for packet flow filtering in order to validate legitimate packet from illegitimated ones.

The concept of ICS Confidence illustrates how much trust of arrived packets based on its correlation pattern.

Definition 2 (Confidence). Confidence is the frequency of legitimated packet flow percent which counted as the total number of appearance for a set of selected attribute pairs.

The confidence percent of legitimate packets will be calculated while generating the NP dataset which called Legitimate Confidence, LegConf.

The confidence of packet can be represented on the form of Iceberg Style profile, called as Iceberg Confidence, *IceConf*. That *IceConf* percent of attribute pairs can be calculated as in Formula (1).

$$IceConf(A_i) = \left(\frac{M(I_a)+P_a}{2} \right) \quad (1)$$

where i =1, 2, 3, …, n. Which identify current attribute pairs.

Table 1: Key Terms Of Ics

Terms	Description
P	A captured packet by ICS method
A	The selected attribute pairs which involved in ICS
P(a)	An attribute pair values in captured packet P.
I(a)	Iceberg percent of legitimate packet for a set of single attribute pairs p(a)
M(I(a))	The Max value of iceberg score for selected attribute pairs in the Nominal Profile
N	The total number of selected attributes in ICS
S	The total Sum of Attribute score

Definition 3 (ICS Score). ICS Score is the total average of sum of all IceConf scores can be calculated in Formula (2):

$$S(p) = \left(\frac{\sum_n^d IceConf\ (A_n))}{N} \right) \quad (2)$$

In Formula 2, d is the number of attributes involved in ICS Score calculation for single packet (p) in the packet flow, where n is the identification number of specified attribute.

To understand the above formula variables clearly, please refer to the Table 1.

Definition 4 (Legitimate Packet). The packet is considered as legitimate if its ICS Score is above the discarding threshold, DT.

Therefore, the DT mechanism is playing the decision maker role on behalf of human. The main function of this mechanism is to distinguish between legitimate packets from attacker ones.

2. Iceberg Confidence Filtering

The entire overall process of ICS method will work in two different modes according to the attack status, attack or non-attack period. The ICS process can be outlined as shown in Fig.1 and ICS Algorithm is also shown as in Fig. 2 to understand the ICS mechanism more easily. The process details will be discussed in the following sections.

In the non-attack period, the Nominal Profile, NP, dataset will be generated by executing two main tasks. The first task will extract attribute pairs in readable format from raw packet. The other task will handle following process of generating the Legitimate Confidence values, LegConf, as pre-request for the ICS Score calculation part.

While non-attack period is conducted under a quiet environment. However, at the attack-period, a lot of illegitimate packets are disturbing our network where ICS must show up to carry them out. Therefore, the ICS will stop updating the nominal profile and begin its filtering process. The ICS Score of packet, S(p), is calculated as in Def. 3. If S is above the DT value then it will be accepted, otherwise rejected.

III. GENERATING THE NP DATASET

1. The general structure

As illustrated on Figure 1, The Nominal Profile, NP, is the core component of ICS filtering approach. First of all, let us prepare ICS attributes which will be involved on NP construction.

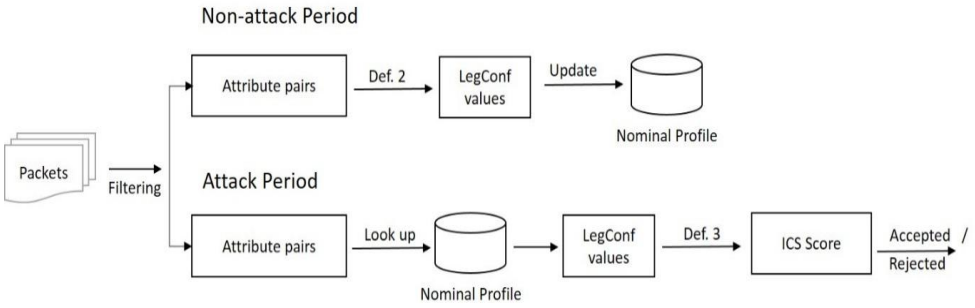

Figure 1: Outline of ICS Filtering

ICS method has only five single attributes as described on Table 2.

Table 2: The Selected Attributes Of Ics

Attribute	Description
Total Length	The total size of a packet including the IP header part, TCP header length, and payload data length.
Header Length	The total length of TCP Header of the packet.
Source Port	The source port number of the packet.
Destination Port	The destination port number of the packet.
TCP Flags	These flags are indicators of current connection status in between sender and receiver

In order to enhance the strength of ICS power against DDoS attacks, ICS combined that five candidates into three attribute pairs based on unique set of correlation patterns of legitimated packet follow. These attribute pairs are 1) source port and destination port, 2) packet size with TCP flags, and 3) TCP header length with TCP flags. That TCP flags are syn, ack, fin, rst, and push.

2. Construction of the NP

The construction of the NP dataset can be divided into two main tasks. The first task is to prepare the normalized dataset of selected attribute pairs which can be accomplished by extracting attribute pairs values from raw packet. The output of this task is become as input for the second task where we can count the Legitimate Confidence, LegConf, values for each set of attribute pairs.

To calculate the LegConf accurately, ICS method count total number of appearance of single attribute pair values like the example shown in Table 3. Then, it calculates the total appearance-percent for each unique attribute pair and update final results to the NP dataset. At the end of updating the NP with LegConf values, ICS store the max, MaxLC, and min, MinLC, percent's of entire dataset of NP profile for each attribute pairs. Due to process complexity and time constraint, all tasks of constructing the NP take place at non-attack period only.

Table 3: Example Of The Np Attributes Pairs

#	Packet Size	TCP Flags*(syn,ack,rst,fin)	LegConf%
1	108	0, 1, 0, 0	0.0888
2	233	0, 1, 0, 0	0.0161
3	228	0, 1, 0, 0	0.0242
4	60	0, 1, 0, 1	2.2448
5	66	0, 1, 0, 0	4.2555

3. The NP Storage Strategy

Our method use two-Diminsional,2D array concept to store each attribute pairs LegConf values separately, 2-D array for each one. Also, store MaxLC, MinLC of all attribute pairs in 2-D array. At real time, all attribute pairs of captured packet will be stored in Microsoft Access Database file for any further analysis of false positive, false negative of ICS performance.

IV. PROPOSED MECHANISM

1. Calculating ICS Score

As the NP dataset has been constructed previously, we become ready and well prepared to push our method to face real time DDoS Attack. At attack-period, game rules changed dramatically, here fast response is required to deal with high volume of enemy traffic as well as receiving legitimated packets without any interrupts effectively. To win this game, the ICS Score agent is our hero for this battle.

Figure 2 illustrates how ICS Algorithm should run step by step in order to obtain a packet score. The internal mechanism of calculating ICS Score start by searching in the NP dataset for related LegConf values. Then we use Formula 1 to find score for each attribute pairs and Formula 2 to sum the average of all scores together, the total IceConf Score of packet p.

For example, if LegConf scores of packet p are: (0.00018, 0.00013, and 4.2555) for A1, A2, A3 respectively and that packet p has attribute values as follows: 22.16570, 22.16570, 22.16570. Then let us calculate the IceConf.

$$IceConf(A_1) = \left(\frac{(22.16570 + 0.00018)}{2} \right)$$

$$IceConf(A_2) = \left(\frac{(30.9674 + 4.2555)}{2} \right)$$

$$IceConf(A_3) = \left(\frac{(4.2878 + 10.0161)}{2} \right)$$

$$S(P_1) = \left(\frac{(11.08294) + (17.61145) + (7.15195)}{3} \right) = 11.94878$$

Most of captured packets will have repeated appearance of attribute value pairs which can be found easily. But, some packets can have a new attribute pairs value which is definitely not shown in the NP. To carry out such situation, we use the MinLC instead of LegConf value.

The process of calculating the ICS Score for incoming packets is fast enough even if attack speed is high because of reducing involved attribute pairs to be three only and using short calculation formulas. Therefore, ICS resource usage is optimized efficiently.

2. Discarding Mechanism

After completing ICS score calculation for a single packet, a discarding mechanism is required to take final decision to accept this packet, otherwise rejected.

The proposed discarding mechanism is playing similar roles as in [3], [4], and [5] discarding threshold, DT, which judge a packet confidence based on packet score. As defined in Def. 4, ICS will allow any packet scores above the DT. For example, if DT value is set to be 00.07 and we take a packet p as example which S(p)=0.04. As a result, this packet is not legitimate, so, it will be discarded.

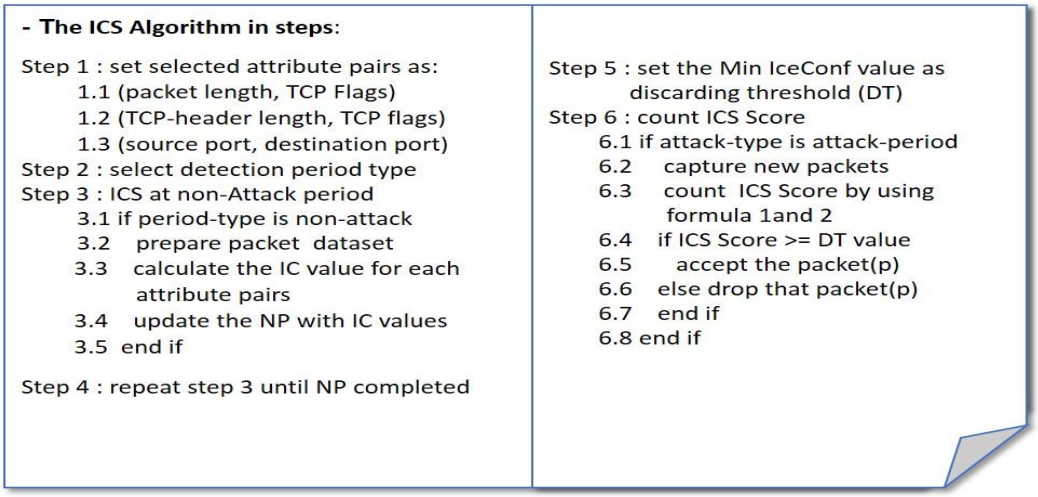

Figure 2: The ICS Algorithm

The static strategy is a fixed discarding mechanism that can be executed immediately form Step. 5 of ICS Algorithm as shown in Figure 2. Therefore, it can be implemented without further knowledge of victim environment setting. Due to short time execution is required, it can start DDoS filtering shortly and effectively.

On the other hand, dynamic strategy rely more on deployment setting of victim machine in order to build its own dataset of the NP as well as updating its DT value dynamically. Although this strategy performance is slower than its competitor, it has better filtering accuracy by having more false positive with less false negative rates.

Both strategies, static and dynamic can be adopted fairly according to complexity level of desired work environment. Dynamic schema can be preferred especially for Cloud Security while static can still shine up in small network of individual machines.

V. PERFORMANCE EVALUATION

1. Testing Preparation

In order to conduct the performance testing of ICS, we developed a C# program for real time packet filtering against different DDoS attacks. We use a real time of NP dataset which had been created based on current setting of testing environment. Our NP dataset has been generated based on 12384 packets from TCP protocol.

During the performance testing, ICS will use three attribute pairs which are {source port, destination port}, {packet size, TCP flags}, and {TCP header length, TCP flags}. For packet filtering through this test, the discarding threshold is set to be 0.0004.

This test will be conducted against simulated DDoS attacks which are: SYN Flood, ACK Flood, SYN-ACK, and Mixed Attack.

2. Evaluation Results

As shown in Figure 3, the legitimate distribution of packet flow which has been filtered under the SYN Flooding attack. However, illegitimate packets are discarded. To avoid long decimal points, ICS scores are multiplied with 100 to have a neat graph.

ICS performance can be evaluated more deeply by using the concept of false positive, FP, and false negative, FN, rates. Table 4 show the FP and FN rates under different types of DDoS attacks.

Table 3: The Fp And Fn Rates Underdifferent Attacks

AttackType	False PositiveRate (%)	False NegativeRate (%)
SYN Flood	05.44	08.16
ACK Flood	05.80	17.97
SYN-ACK Flood	04.78	11.39
Mixed	04.50	07.77

At SYN Flood attack ICS has better performance than CBF [4] in FP rates, 5.4 and 7.7 respectively. Therefore, ICS can guarantee more resources for legitimate flow. However, CBF has better performance results based on FN rates, 7.7 comparing with 8.1 of ICS. Even so, 8.1 percent can be accepted practically for DDoS mitigation.

The FN and FP rates of ICS can be reduced gradually by updating the NP dataset periodically with new LegConf as well as re-generating the MaxLC and MinLC values. To achieve better performance, hash function should be used to reduce consumed time while lookup for LegConf values.

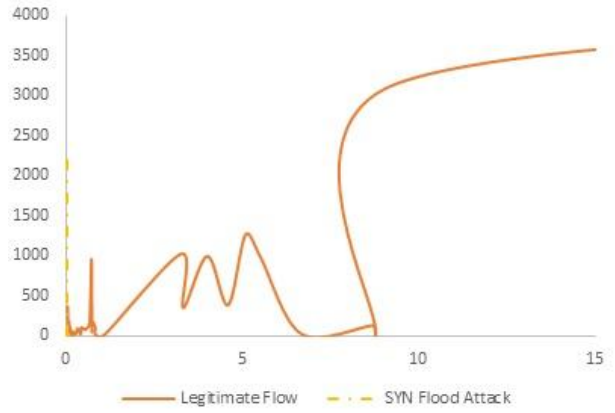

Figure 3: ICS Score Distribution at SYN FloodAttack

VI. CONCLUSION AND FUTURE WORK

The key concept of ICS method is utilizing the similar properties of correlation-pattern within legitimate packet flow. These correlation patterns had been used as a unique set of legitimate packet flow in order to generate the LegConf from the NP dataset. The ICS Score can be calculated as described in Def.2, Def.3. If that score is below the DT value, then that packet will be discarded. Therefore, the higher ICS score is obtained, more legitimate flow is granted. The final results of performance test, show an accepted level of

filtering accuracy with a good response time in DDoS mitigation even with high speed. So, the ICS can be integrated with IDS as an effective solution against DDoS.

In future, the processing time of finding related LegConf of attribute pairs can be optimized by using faster hash function which can improve ICS performance as well as adopting paralleled design for Score calculation. In order to gain the best possible value of ICS in real time, we should improve our discarding mechanism, so it can be integrated easily with IDS and IPS.

ACKNOWLEDGEMENTS

Foremost, I would like to express my sincere gratitude to whom words give up before giving them anything back, to my great parent, thank you very much for supporting my research from first letter until last dot. Also, I am very grateful for my advisor Dr. Abbas for the continuous support of my M. Tech study and research, for his patience, motivation, and trust. Last but not least, my sincere thanks to Dr. Juma Saleh Al-Ghailani, Managing Director and Dr. Jamal Dawood Salman, Dean, Mazoon College for having provided the opportunity to carry out this article.

We deem it a great privilege to offer our sincere thanks to the Research and Development Center, Mazoon College, Muscat for their constant encouragement and support.

REFERENCES

[1]. Asosheh A., Ramezani N., A Comprehensive Taxonomy of DDoS Attacks and Defense Mechanism Applying in a Smart Classification. *WSEAS Transactions on Computers*, (7), 2008, 281–290

[2]. S. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks."*IEEE*, 2013.

[3]. Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial of Service Attacks," *IEEE Trans. Dependable and Secure Computing*, 3(2), pp.141-155, 2006.

[4]. P.E. Ayres, H. Sun, H. J. Chao, and W. C. Lau, "ALPi: A DDoS Defense System for High Speed Networks," *in IEEE J. Selected Areas Comm*., 24 (10), 2006, pp.1864-1876.

[5]. Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu, "CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment", in *Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing*, 978-0-7695-4612-4/11, 2011.

[6]. Sadhu, A.K.K.Vijaya, K.Seth, Md.T. Riasat, M.Hasan and O.Abuzaghleh ,IA Study on Various Defense Mechanisms Against DDoS Attacks , *International Journal of Scientific & Engineering*.

[7]. Candid Wueest, "*The Continued Rise of DDoS Attacks," Security Response by Symantec version 1.0 – Oct 21, 2014.*