Granger Causality in TCP Flooding Attack

Rup Kumar Deka[1], Dhruba Kumar Bhattacharyya[1], and Jugal Kumar Kalita[2]
(Corresponding author: Rup Kumar Deka)
Department of Computer Science and Engineering, School of Engineering, Tezpur University
Napaam, Tezpur, Assam, 784028, India[1]
(Email: rup.deka@gmail.com)
Department of Computer Science, College of Engineering and Applied Science, University of Colorado
1420 Austin Bluffs Parkway, Colorado Springs, CO 80933-7150, United States[2]
(Received Oct. 18, 2017; revised and accepted March 27, 2018)

Abstract

Malicious software events are usually stealthy and thus challenging to detect. A triggering relation can be assumed to be causal and to create a temporal relationship between the events. For example, in a spoofed TCP DDoS flooding attack, the attacker manipulates a three-way handshake procedure. During this attack, the number of spoofed IP addresses and the number of open ports used by the attacker follow a causal relationship. This paper demonstrates the effectiveness of Granger Causality in confirming TCP flooding attacks. We focus on discovering the presence of TCP-SYN flooding DDoS activity in network traffic by analyzing causal information in near real time.

Keywords: DDoS; Granger Causality; TCP Flooding

1 Introduction

Most DNS reflection attacks are currently caused by spoofing the source IP address to flood the Internet. SYN floods, for example, are spoofed TCP floods, in which the source of the IP packets appears to be different from their actual origin. Figure 1 shows that SYN and TCP attacks are predominant according to the Kaspersky DDoS Intelligence Report for the first quarter 2016 [25]. If the servers are compromised, they too can send spoofed packets to create a large attack. In the third quarter of 2016, there was a huge intensity TCP-SYN flood attack of approximately 60 giga bytes per second and 150 million packets per second, as rated by Verisign [43]. It was bigger than the previous biggest at 125 million packets per second during the fourth quarter of 2015.

In the recent past, a good number of efforts to provide real time detection or mitigation of DDoS attacks with adequate accuracy have been proposed [2, 7, 8, 10, 18, 39]. However, a report of the United States Computer Emergency Readiness Team (US-CERT), has recently observed that an effective DDoS defense solution that can handle DDoS attacks of all types well, is still lacking [42]. In addition, with the evolution of botnet technology, it has become even more difficult to provide real time defense.

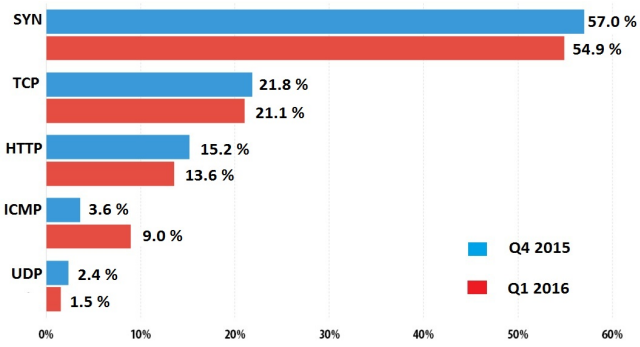

Figure 1: Recent DDoS attack statistics

To investigate into causal or correlational behavior in the network traffic during a SYN flood attack, we have to analyze the traffic if the intrusion detection systems (IDS) system generates any alarm about an abnormal situation. It is often a challenge to effectively deal with the large number of alerts generated by intrusion detection systems. Alert correlation is necessary to discover true anomalous behaviors. Generally, IDSs aim to unearth anomalies [11, 14, 30, 37]. They raise alerts for any anomaly they find, when they find it, and do so independently of all other anomalies they may find. However, going beyond individual alerts, it may be possible to find logical evidence of connections among them. Sometime, attacks may be intensive with a large number of generated alerts. Actual alerts can also be mixed with false alerts. The sheer volume of alerts is likely to become unmanageable. As a result, it becomes difficult to evaluate alerts properly and quickly to take appropriate actions, and hence to respond properly.

1.1 Motivation

It is necessary to enhance the performance of alert correlation and also to minimize the damage from attacks.

Some techniques for alert correlation have been presented by Ning *et al.* [29]. These techniques are two complementary alert correlation methods based on alert attributes' similarities, and attack prerequisites and consequences. In particular, the work is based on the indirect causal relationships between alerts.

Our work's aim is to confirm the presence of TCP-SYN flooding DDoS activity by analyzing causal information for alert analysis in the network traffic using Granger Causality. In varied fields like economics [20], neuroscience [13] and cardiovascular control [31], Granger Causality analysis has been used to study data series to uncover the presence of causal behavior.

1.2 Background

The components of an intrusion detection system cooperatively gather and produce a concise summary of events on the network with respect to security. The IDS also establishes correlation among the collected alerts. To do so, it may use an alert correlation procedure. This correlation procedure can be divided into multiple steps where each step performs a part of the whole task. The performance of the correlation process depends upon the serial execution by these steps. The total time needed can be derived by adding the number of processed alerts by each step.

Elshoush and Osman [15] propose a new correlation framework based on a model that reduces the number of processed alerts as early as possible by discarding irrelevant and false alerts in the first phase. Modified algorithm for fusing the alerts is also proposed. The intruders' intentions are grouped into attack scenarios and thus used to detect future attacks.

Li and Tian [28] propose an alert correlation approach based on their XSWRL ontology. They focus on how to develop the intrusion alert correlation system according to an alert correlation approach. They use a system with multiple agents and sensors. The sensors collect security relevant information, and the agents process the information. The State Sensor collects information about the security state and the Local State Agent and Center State Agent pre-process the security state information and convert it to ontology. The Attack Sensor collects information about the attack, and the Local Alert Agent and Center Alert Agent pre-process the alert information and convert it to ontology. The Attack Correlator correlates the attacks and outputs the attack sessions.

Bateni *et al.* [4] discuss an automated alert correlation process, in which they use Fuzzy Logic [26] and an Artificial Immune System (AIS) [22]. This approach discovers and learns the degree of correlation between two alerts. This knowledge is used to understand the attack scenarios. Based on its fuzzy rules, the system computes the correlation probabilities.

Yu and Frincke [45] propose a novel framework called Hidden Colored Petri-Net for Alert Correlation and Understanding (HCPN-ACU). According to them, a system misuser usually follows a sequential procedure to violate security policies creating a sequence with earlier steps preparing for the later ones. These steps may result in alerts. These alerts can be used to discover the attacker's action.

Zhu and Ghorbani [46] demonstrate a method using learning techniques: Multilayer Perceptrons (MLP) [34] and Support Vector Machines (SVM) [21]. The outputs of these techniques can be converted to probabilities and then combined for evaluation of correlation between previous alerts and current alerts. This suggests a causal relationship between two alerts, helping in the constructing attack scenarios.

Roschke *et al.* [33] use prior knowledge about the target system for an efficient correlation process. They design a correlation algorithm based on attack graphs (AG). The existing vulnerabilities and their AGs are used for representation of environment information and potential exploits.

Kang and Mohaisen [24] design a system to reduce the number of false positive alerts. These false positive alerts are generated by the existing DDoS mitigation methods along with true alerts. The authors perform a preliminary analysis of real DDoS data. They also propose a system that uses ensemble classifier techniques to work in tandem with the existing rule-based system to ease the burden on the mitigation team.

Wang and Chiou [44] develop a system to extract attack strategies using dynamic feature weights. It extracts attack scenarios from attackers by observing the connectivity and relationships among the receiving alerts.

GhasemiGol and Bafghi [17] develop an intrusion-alert correlation system based on the the information found in the raw alerts without using any pre-constructed knowledge. They define the concept of alert partial entropy and use it to find alert clusters with the same information. These alert clusters are represented as hyper-alerts, and a graph of hyper alerts provide a global view of intrusion alerts.

Raftopoulos and Dimitropoulos [32] introduce an IDS alert correlator called Extrusion Detection Guard (EDGe). It detects infected hosts within a monitored network from IDS alerts. EDGe detects several malwares that exhibit multi-stage behavior. It can also identify the family and even variants of certain malware to re-mediate and prioritize incidents.

1.3 Contribution

We make the following contributions in this paper.

- We introduce TCP-SYN flooding DDoS attack confirmation mechanism based on the causal behavior in the network traffic using Granger causality.
- We establish and validate the proposed method using benchmark and our own DDoS traffic datasets.

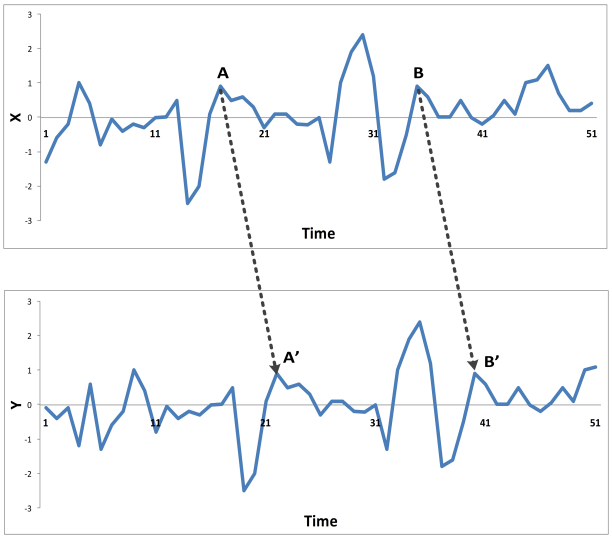

Figure 2: Example of Granger causality

1.4 Organization

The organization of the paper is as follows. Section 2 introduces Granger Causality and TCP Flooding attacks. Section 3 presents the framework for detection of TCP-SYN flooding attacks and experimental results. Finally, Section 4 provides the concluding remarks and future scope of the work.

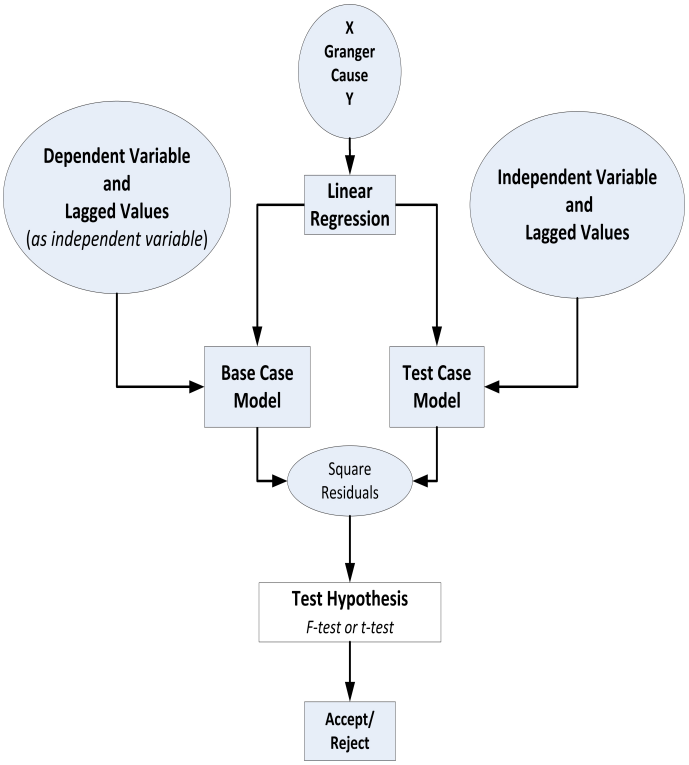

Figure 3: The mathematical picture

2 Granger Causality and TCP Flooding

2.1 Granger Causality

Detecting causal behavior among variables is an important issue in statistics, although it remains a problem without a guaranteed solution. Granger causality was introduced in 1960 for testing causal behavior among variables and applications of Granger causality in neuroscience have recently become popular. According to Granger, the causality relationship follows two principles: [19],

1) The cause happens prior to its effect, and

2) Unique information is contained in the cause about the future values of its effect.

Granger causality can be used to find causal relation among variables. The concept of Granger causality is based on the ability to predict. in Figure 2, we see if a data series X "Granger-Causes" ("G-Causes") another data series Y, we can predict that past values of X might contain information to predict Y, and we can also predict beyond past values of Y alone. So, using the F-test or the t-test we can devise a G-Cause test as a hypothesis test, as shown in Figure 3, to identify whether one time series can forecast another time series. Suppose that X and Y are two stationary time series that are statistically dependent on each other. When is it justified to say that the one series X causes the other series Y? Questions of this kind are important when planning to devise actions, implementing new policies, or subjecting patients to a treatment. Nonetheless, the notion of causality has been evasive and formal approaches to define causality have been much debated and criticized.

Granger Causality vs Causality

- Granger Causality measures whether X happens before Y and helps predict Y.
- X Granger-Causing Y may entail real causality, but we can't be sure.
- If X does not Granger-Cause y, we can be more confident about X does not cause Y.

2.2 DDoS attack

DDoS attacks are intended to deny legitimate users access to network resources. As shown in Figure 4, an attacker launches the attack through some handlers and zombies creating a botnet. In a botnet, there may be hundreds or thousands of compromised sources that generating voluminous traffic to flood the victim. It is extremely difficult to differentiate legitimate traffic from attack traffic. The sources may be spread across all over the globe [1,3,35,40]. In early days, DDoS attacks were launched in 4 steps:

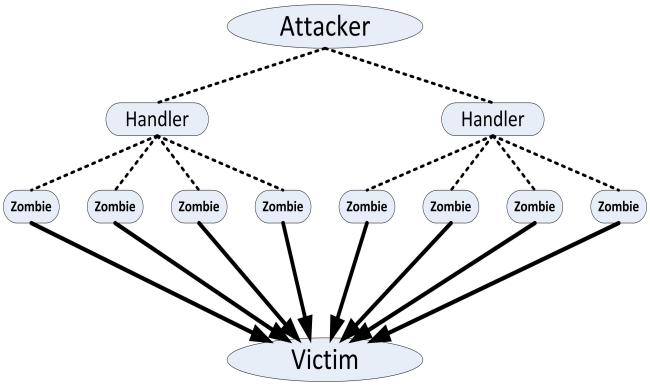

Figure 4: DDoS attack scenario

scanning, trade-off, deployment and propagation. Gradually, automation has been introduced into each of these steps, although the steps are still similar.

1) The attacker collects network configuration information using port scanners to identify vulnerabilities in the network.

2) The attacker exploits identified vulnerabilities to launch the attacks.

3) If the attack launch is successful, the attacker installs additional software to manage continuous access channels in the network.

4) The attacker tries to clean up any evidence left due to the previous actions. In this step, daemons that crashed (during the second step) are restarted, logs are cleared and modified system software designed to hide the presence of rogue software from normal system commands is installed.

2.2.1 TCP SYN Floods

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. Manipulating the 3-way handshake in a TCP connection, an attacker sends a lot of ordinary SYN segments to the victim machine to create a TCP flooding attack. A TCP SYN flood is successful when the victim machine's TCP connection queue gets exhausted, thus denying legitimate requests. A TCP flooding attack at a medium rate can also create disturbances in routers. TCP SYN flooding is an asymmetric attack because a weak attacker can halt a very powerful system. When a lot of users simultaneously access a website for the same resource, it can lead to unavailability of the website temporarily creating flash traffic [5, 6].

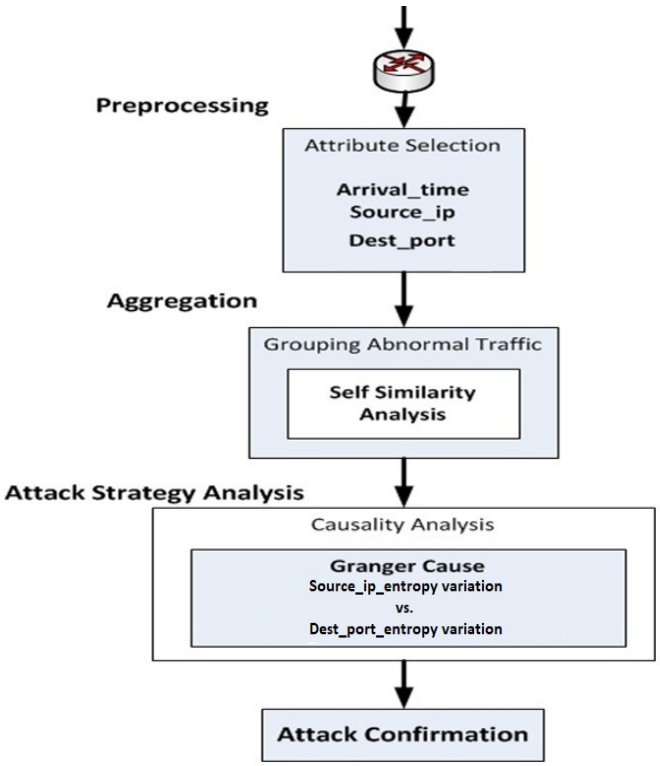

Figure 6: Framework for attack confirmation

2.3 Causality in TCP Flooding Traffic

As we have observed already, during a TCP flooding attack, the number of unknown IP addresses changes rapidly, and the number of ports used by these IP addresses is much higher, and they change rapidly. We hypothesize that there is a causal relationship between the entropies of source-IP variation and port variation. During the attack time frame, the variations in entropy affect each other. The concept of Granger causality gives us a way to analyze the pattern of IP address variation entropy and port number variation entropy when abnormal traffic is injected in to the network.

3 Framework and Results

We define the problem as follows.

Problem Statement: The objective is to discover TCP flooding DDoS attacks in network traffic, whether the attack traffic is low rate or high rate by evaluating the causality in network traffic using Granger causality.

Datasets and Experimental Setup: We use MATLAB R2016a 64 bit edition for our experiments, and perform our experiments on a workstation with a 2.30Ghz processor, 64 GB RAM and a 64 bit Windows 10 operating system. In our experiments, we consider TCP traffic from four standard benchmark datasets. The first

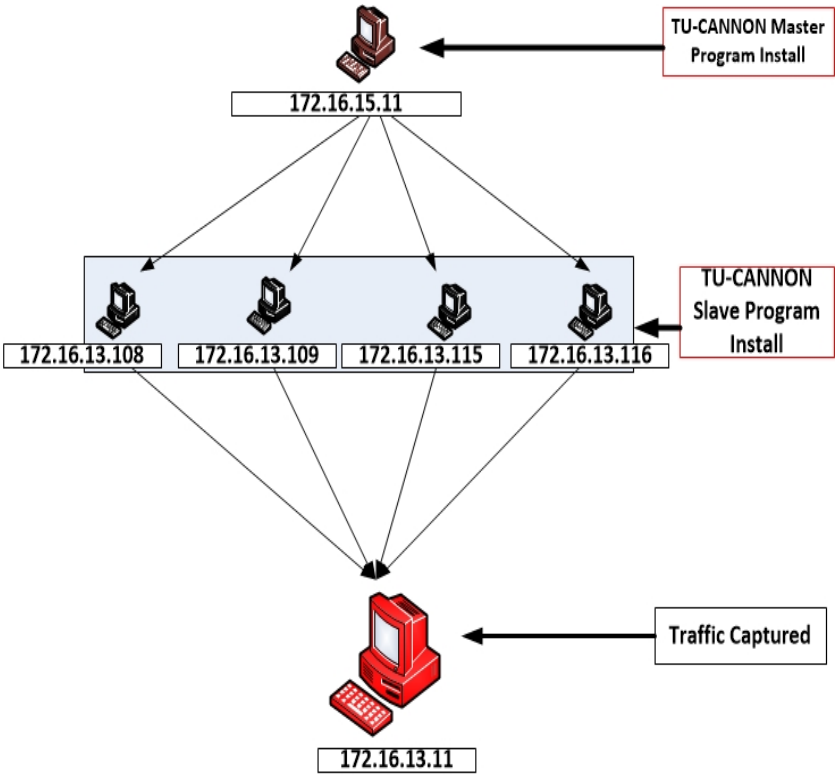

Figure 5: Experimental setup

one is the MIT-DARPA dataset [27] of normal and attack traffic. The second one is CAIDA-2007 DDoS attack traffic [16]. The MIT–DARPA and CAIDA–2007 datasets contain both low rate and high rate DDoS traffic traces. The third dataset is the ISCX-IDS dataset [41]. The last one is the TU-DDoS dataset for which we use the TU-CANNON tool for generation of the TCP flooding traffic using our own environment as shown in Figure 5 [9].

TU–CANNON Tool: Two main programs are executed in this traffic generation tool, viz., a server program and a client program. Using the server program, communication is established with the machines (bots) in the test-bed. This program can be used to generate different traffic streams having different properties such as the protocol type (TCP, UDP and ICMP), the attack pattern (constant rate attack, increasing rate attack and pulsing attack) and the type of source IP (actual IP of the machine or randomly generated, valid but spoofed IP address), the number of threads (where each thread executes one copy of the slave program inside a single bot machine) and the range of ports of the victim to send the traffic [3]. As shown in Figure 5, we divide the computers for three separate functions. One computer executes the TU–CANNON master program and this computer recruits four other computers as slave, where the TU–CANNON slave program executes. When the master starts, it waits for slaves to connect to it. The last computer captures the attack traffic. The client program is used to send the attack traffic as per the command sent from the master. When the client program starts, it connects to the server whose IP is specified as input to the client program.

3.1 Procedural Framework and Results

Figure 6 shows the framework of our method as well as the sequence of steps in our algorithmic procedure. There are four basic steps, viz., (a) Pre-processing, (b) Aggregation, (c) Attack strategy analysis, and (d) Attack confirmation. The execution processes and the results are discussed below.

3.1.1 Pre-processing

To establish the causal behavior in the network traffic, the arrival time of the packets, the source address and the destination port need to be considered in our approach. Source IP values are in IPV4 format. Our procedure isn't concerned about the format of the IP addresses, whether in IPV4 or IPV6 format, as we convert them to decimal.

3.1.2 Aggregation

In aggregation, the main focus is all about gathering similar alerts together. We can see different definitions of alert aggregation in the literature. According to some, alerts are said to be similar to each other if their attributes are similar except time difference. On the other hand, some enhance the concept of aggregation as clustering or grouping all the alerts having the same root cause. Due to the

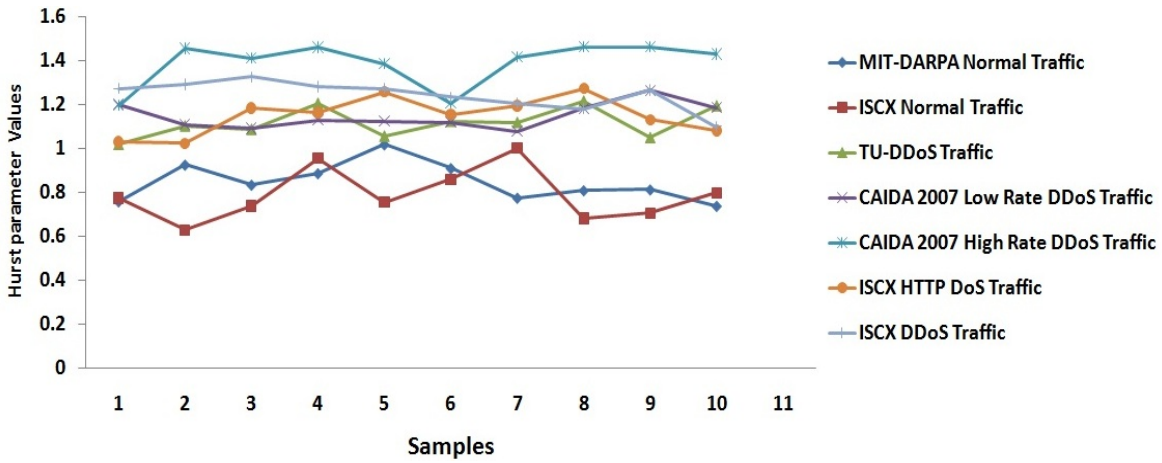

Figure 7: Hurst parameter values for different types of traffic

Table 1: Success rates for different network traffic/datasets

Dataset/Traffic Used	Accept/Reject NULL Hypothesis	Success rate (%)
MIT–DARPA Normal Traffic	Accept	96
ISCX Normal Traffic	Accept	97
MIT DARPA Attack Traffic	Reject	97
CAIDA–2007 High-rate Attack Traffic	Reject	97
CAIDA–2007 Low-rate Attack Traffic	Reject	98
ISCX Attack Traffic	Reject	95
TUCANNON Generated	Reject	98

large number of alerts produced by low-level sensors for a single malicious activity, alert aggregation has proven to be highly effective in reducing alert volume. Similar alerts tend to have similar root causes or similar effects on resources of the Internet. Clustered alerts are suitable for analysis by administrators and facilitate analysis for identification of causality or false positive analysis. In our experiment, we use Hurst parameter-based self-similarity evaluation of traffic with abnormal patterns [12]. Normal and abnormal traffic patterns are grouped depending upon the evaluated Hurst parameter value. In Figure 7, we can distinctly separate normal and abnormal traffic based on the Hurst value. Our aim is not only to separate normal and abnormal traffic, but also to confirm the presence of TCP flooding attack by analyzing causal behavior of the abnormal traffic.

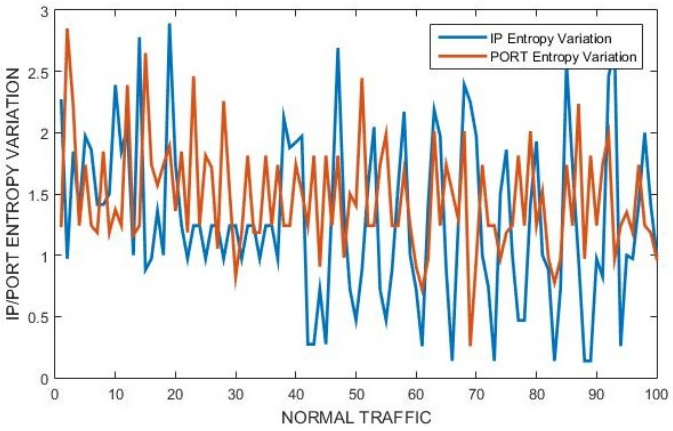

Figure 8: Source IP and port entropy variations for normal traffic

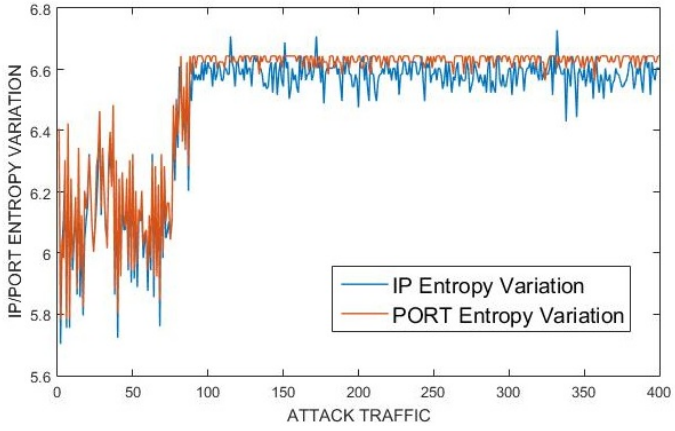

Figure 9: Source IP and port entropy variations for attack traffic

Table 2: Execution time for different attack traffic datasets with varying numbers of incoming packets

Datasets	Time (in Sec.)		
	500 Packets	1000 Packets	2000 Packets
MIT–DARPA Normal	0.080	0.118	0.122
ISCX Normal	0.078	0.115	0.119
MIT DARPA Attack	0.082	0.120	0.125
CAIDA–2017 High–rate Attack	0.080	0.119	0.121
CAIDA–2017 Low–rate Attack	0.079	0.117	0.120
ISCX Attack	0.081	0.118	0.123
TU-CANNON Generated Attack	0.084	0.120	0.122

3.1.3 Attack Strategy Analysis

If a time series is a stationary process, statistical t-test is performed using the level values of two (or more) variables. If the variables are non-stationary, then the test is performed using the first (or higher) differences. Any particularly lagging value of one of the variables is retained in the regression if

1) It is significant according to a t-test, and
2) It and the other lagging values of the variable jointly add explanatory power to the model according to an F-test.

The null hypothesis of Granger causality is not rejected if and only if no values of an explanatory variable have been retained in the regression. We use F-test for evaluation of Granger causality. Table 1 shows acceptability of the null hypothesis and also success rate of acceptance or rejection of null hypothesis for different network traffic datasets.

[F, CV]=Grangercause(X, Y, α, Maxlag): The various terms in the formula are explained below. From F-test, we can obtain two output values: F and CV (Critical Value).

X: Port entropy variation in abnormal traffic group.

Y: Source IP address entropy variation in the abnormal traffic group. Both entropy values, X and Y follow Shannon entrop [38].

α: Value of the significance level can be set by the user ($\alpha = 0.05$). The significance level, denoted as alpha (α), is the probability of rejecting the null hypothesis when it is true. For example, a significance level of 0.05 indicates a 5 percentage risk of concluding that a difference exists when there is no actual difference [23].

Maxlag: Maximum lag value among two time series. Optimum lag length selection is chosen using the Bayesian Information Criterion [36].

Output: If F > CV, we reject the null hypothesis that Source IP address entropy does not Granger-Cause Port entropy variation. Otherwise, we accept the null hypothesis.

3.1.4 Attack Confirmation

The source IP variation entropy and port variation entropy are shown in Figures 8 and 9, for the attack traffic generated in our setup and for normal traffic, respectively. Based on the F-test, we confirm whether the TCP Flooding attack has occurred or not in the network traffic. If the null hypothesis gets accepted, it confirms the presence of TCP flooding attack. The success rates of acceptance or rejection of NULL hypothesis for different datasets has been tabulated in Table 1. A couple of the datasets contain high-rate and low-rate DDoS traffic traces. In Table 2, we show execution times for different attack traffic datasets with varying numbers of incoming packets.

3.2 Comparison

In the past, several authors have explored alert correlation for network traffic analysis to detect attack scenarios. However, our approach in this paper differs significantly from [29], [45], [46], [4], [17], and [44]. In Table 3, we show a comparison of our method with these methods.

4 Conclusion and Future Direction

To confirm the occurrence of a TCP flooding DDoS attack, it is essential to analyze the abnormal traffic as quickly as possible. In network anomaly detection, it is highly beneficial to achieve false positive and false negative rates as close to zero as possible. Keeping this in mind, we develop our approach to confirm the presence of TCP flooding DDoS attacks based on causal behavior in network traffic using Granger causality. We demonstrate that the method performs satisfactorily over benchmark datasets. The F-test evaluation on traffic datasets confirms the attack in the traffic distinctly.

In future, we plan to study the causal behavior in other flooding DDoS attack types. We also aim to explore the applicability of our approach in Ad–hoc network.

Table 3: Comparison with [29], [45], [46], [4], [17], and [44]

Author, Year	Aim	Approach	Dataset(s) Used	Performance
Ning *et al.* [29], 2004	To build attack scenarios	Integration of complementary alert correlation	MIT-DARPA 2000	Construction of integrated correlation graph
Yu and Frincke [45], 2004	To create a model for attacker behaviors, intrusion prerequisites and consequences, security policies and alerts	Construction of a framework, using Hidden Colored PetriNet for alert correlation and understanding	MIT-DARPA 2000	False alert rate is 93-95 %
Zhu and Ghorbani [46], 2006	To extract attack strategies automatically from a large volume of intrusion alerts	Use of Multilayer Perceptron (MLP) and Support Vector Machine (SVM)	MIT-DARPA 2000	Construction of graph representing attack strategies, the training results of MLP and SVM are 0.0002-0.9900 and 0.1252-0.9926, the correlation weight in alert correlation matrix (ACM) is in range from 0.01 to 3533.93 and the forward correlation strength in ACM is in range from 0 to 0.857
Bateni *et al.* [4], 2013	To build automated alert correlation	Use of Artificial Immune System and Fuzzy Logic	MIT-DARPA 2000	For 1000 alert, execution time is 19 seconds and for 2000 alerts, execution time is 76 seconds
GhasemiGol and Ghaemi-Bafghi [17], 2014	To build an entropy-based alert correlation system	Use of prior information in raw alerts without using any predefined knowledge	MIT-DARPA 2000	Reduction ratio of 99.98%
Wang and Chiou [44], 2016	To build an alert correlation system with automatic extraction of attack strategies	Use of equality constraint sets (ECS) and storage in the alert correlation matrix (ACM)	MIT-DARPA 2000	Provides precise attack scenarios, the value of alert correlation matrix (ACM) is in range from 0 to 241.64 and the forward correlation strength is in range from 0 to 1
Our Work, This paper	To discover TCP flooding DDoS attacks in network traffic alert	Using Granger causality to evaluate the causality in network traffic	MIT-DARPA 2000, CAIDA-2007 (contains both low-rate and high-rate), ISCX-IDS dataset and TU-DDoS dataset (using TU-CANNON)	Success rate is 95-98%. Execution times are 0.078-0.084, 0.115-0.120, and 0.119-0.125 seconds for 500, 1000 and 2000 packets, respectively

References

[1] A. A. Ahmed and N. A. K. Zaman, "Attack intention recognition: A review," *International Journal of Network Security*, vol. 19, no. 2, pp. 244–250, 2017.

[2] A. A. Al-khatib and W. A. Hammood, "Mobile malware and defending systems: Comparison study," *In-*

ternational Journal of Electronics and Information Engineering, vol. 6, no. 2, pp. 116–123, 2017.

[3] R. C. Baishya, N. Hoque, and D. K. Bhattacharyya, "DDoS attack detection using unique source IP deviation," *International Journal of Network Security*, vol. 19, no. 6, pp. 929–939, 2017.

[4] M. Bateni, A. Baraani, and A. Ghorbani, "Using artificial immune system and fuzzy logic for alert correlation," *International Journal of Network Security*, vol. 15, no. 3, pp. 190–204, 2013.

[5] S. Behal and K. Kumar, "Characterization and comparison of DDoS attack tools and traffic generators: A review," *International Journal of Network Security*, vol. 19, no. 3, pp. 383–393, 2017.

[6] S. Behal, K. Kumar, and M. Sachdeva, "Discriminating flash events from DDoS attacks: A comprehensive review," *International Journal of Network Security*, vol. 19, no. 5, pp. 734–741, 2017.

[7] D. K. Bhattacharyya and J. K. Kalita, *Network anomaly detection: A machine learning perspective*. CRC Press, 2013.

[8] D. K. Bhattacharyya and J. K. Kalita, *DDoS attacks: evolution, detection, prevention, reaction, and tolerance*. CRC Press, 2016.

[9] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Towards generating real-life datasets for network intrusion detection," *International Journal of Network Security*, vol. 17, no. 6, pp. 683–701, 2015.

[10] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, *Network Traffic Anomaly Detection and Prevention: Concepts, Techniques, and Tools*. Springer, 2017.

[11] A. Chaudhary, V. N. Tiwari, and A. Kumar, "A new intrusion detection system based on soft computing techniques using neuro-fuzzy classifier for packet dropping attack in manets," *International Journal of Network Security*, vol. 18, no. 3, pp. 514–522, 2016.

[12] R. K. Deka and D. K. Bhattacharyya, "Self-similarity based DDoS attack detection using Hurst parameter," *Security and Communication Networks, Wiley Online Library*, vol. 9, no. 17, pp. 4468–4481, 2016.

[13] M. Ding, Y. Chen, and S. L. Bressler, "Granger causality: basic theory and application to neuroscience," *arXiv preprint q-bio/0608035*, 2006.

[14] R. H. Dong, D. F. Wu, and Q. Y. Zhang, "The integrated artificial immune intrusion detection model based on decision-theoretic rough set," *International Journal of Network Security*, vol. 19, no. 6, pp. 880–888, 2017.

[15] H. T. Elshoush and I. M. Osman, "An improved framework for intrusion alert correlation," in *Proceedings of the World Congress on Engineering*, vol. 1, pp. 1–6, Imperial College London, London, U.K., 2012.

[16] CAIDA (Center for Applied Internet Data Analysis). "CAIDA-2007 data," 2007. (`https://www.caida.org/data/passive/ddos-20070804_dataset.xml`)

[17] M. GhasemiGol and A. Ghaemi-Bafghi, "E-correlator: an entropy-based alert correlation system," *Security and Communication Networks, Wiley Online Library*, vol. 8, no. 5, pp. 822–836, 2015.

[18] S. Goswami, N. Hoque, D. K. Bhattacharyya, and J. Kalita, "An unsupervised method for detection of XSS attack," *International Journal of Network Security*, vol. 19, no. 5, pp. 761–775, 2017.

[19] C. W. J. Granger, "Investigating causal relations by econometric models and cross-spectral methods," *Econometrica: Journal of the Econometric Society, JSTOR*, pp. 424–438, 1969.

[20] C. W. J. Granger, B. N. Huangb, and C. W. Yang, "A bivariate causality between stock prices and exchange rates: evidence from recent Asian flu," *The Quarterly Review of Economics and Finance, Elsevier*, vol. 40, no. 3, pp. 337–354, 2000.

[21] Marti A. Hearst, Susan T Dumais, Edgar Osuna, John Platt, and Bernhard Scholkopf, "Support vector machines," *IEEE Intelligent Systems and their applications*, vol. 13, no. 4, pp. 18–28, 1998.

[22] Steven A Hofmeyr and Stephanie Forrest, "Immunity by design: An artificial immune system," in *Proceedings of the 1st Annual Conference on Genetic and Evolutionary Computation-Volume 2*, pp. 1289–1296. Morgan Kaufmann Publishers Inc., 1999.

[23] Tse-Chi Hsu and Leonard S Feldt, "The effect of limitations on the number of criterion score values on the significance level of the f-test," *American Educational Research Journal*, vol. 6, no. 4, pp. 515–527, 1969.

[24] A. R. Kang and A. Mohaisen, "Automatic alerts annotation for improving DDoS mitigation systems," in *IEEE Conference on Communications and Network Security (CNS)*, pp. 362–363, Philadelphia, PA USA, 2016. IEEE.

[25] Kaspersky. "Kaspersky DDoS intelligence report for Q1 2016," 2016. (`https://securelist.com/kaspersky-ddos-intelligence-report`)

[26] George Klir and Bo Yuan, *Fuzzy sets and fuzzy logic*, vol. 4. Prentice hall New Jersey, 1995.

[27] Massachusetts Institute of Technology (MIT) Lincoln Laboratory. "DARPA intrusion detection data sets," 2000. (`https://www.ll.mit.edu/ideval/data/`)

[28] W. Li and S. Tian, "An ontology-based intrusion alerts correlation system," *Expert Systems with Applications, Elsevier*, vol. 37, no. 10, pp. 7138–7146, 2010.

[29] P. Ning, D. Xu, C. G. Healey, and R. St. Amant, "Building attack scenarios through integration of complementary alert correlation method," in *Network and Distributed System Security Symposium*, vol. 4, pp. 97–111, Catamaran Resort Hotel San Diego, California, USA, 2004.

[30] E. Popoola and A. O. Adewumi, "Efficient feature selection technique for network intrusion detection

system using discrete differential evolution and decision," *International Journal of Network Security*, vol. 19, no. 5, pp. 660–669, 2017.

[31] Alberto Porta, Tito Bassani, Vlasta Bari, Gian D Pinna, Roberto Maestri, and Stefano Guzzetti, "Accounting for respiration is necessary to reliably infer Granger causality from cardiovascular variability series," *IEEE Transactions on Biomedical Engineering*, vol. 59, no. 3, pp. 832–841, 2012.

[32] E. Raftopoulos and X. Dimitropoulos, "IDS alert correlation in the wild with edge," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 10, pp. 1933–1946, 2014.

[33] S. Roschke, F. Cheng, and C. Meinel, "A new alert correlation algorithm based on attack graph," *Computational intelligence in security for information systems*, pp. 58–67, 2011.

[34] Dennis W Ruck, Steven K Rogers, Matthew Kabrisky, Mark E Oxley, and Bruce W Suter, "The multilayer perceptron as an approximation to a bayes optimal discriminant function," *IEEE Transactions on Neural Networks*, vol. 1, no. 4, pp. 296–298, 1990.

[35] I. Sattar, M. Shahid, and Y. Abbas, "A review of techniques to detect and prevent distributed denial of service (DDoS) attack in cloud computing environment," *International Journal of Computer Applications, Foundation of Computer Science*, vol. 115, no. 8, 2015.

[36] G. Schwarz, "Estimating the dimension of a model," *The annals of statistics*, vol. 6, no. 2, pp. 461–464, 1978.

[37] V. M. Shah and A. K. Agarwal, "Reliable alert fusion of multiple intrusion detection systems," *International Journal of Network Security*, vol. 19, no. 2, pp. 182–192, 2017.

[38] C. E. Shannon, "A mathematical theory of communication," *Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[39] S. Sivabalan and P. Radcliffe, "Power efficient secure web servers," *International Journal of Network Security*, vol. 20, no. 2, pp. 303–311, 2018.

[40] J. R. Sun and M. S. Hwang, "A new investigation approach for tracing source IP in DDoS attack from proxy server," in *International Computer Symposium (ICS 2014)*, pp. 850–857, Tunghai University, Taichung, Taiwan, 2014.

[41] University of New Brunswick (UNB). "Intrusion detection evaluation dataset (iscxids2012)," 2912. (`http://www.unb.ca/cic/datasets/ids.html`)

[42] US-CERT. "Udp-based amplification attacks,", 2015.

[43] Verisign. "Q4 2016 DDoS trends report: 167 percent increase in average peak attack size from 2015 to 2016," 2016. (`https://blog.verisign.com/security`)

[44] C. H. Wang and Y. C. Chiou, "Alert correlation system with automatic extraction of attack strategies by using dynamic feature weights," *International Journal of Computer and Communication Engineering, IACSIT Press*, vol. 5, no. 1, p. 1, 2016.

[45] D. Yu and D. Frincke, "A novel framework for alert correlation and understanding," in *The Second International Conference on Applied Cryptography and Network Security, (ACNS 2004)*, vol. 4, pp. 452–466, College Park, Maryland, USA, 2004.

[46] B. Zhu and A. A. Ghorbani, *Alert correlation for extracting attack strategies*. University of New Brunswick, Canada, 2005.

Biography

Rup Kumar Deka is a research Scholar in the Computer Science & Engineering Department at Tezpur University. His research areas include Network Security, Network Management and Cryptography. Mr. Deka has completed B.E. and M.Tech. degree in computer science and is currently pursuing Ph. D. degree.

Dhruba Kumar Bhattacharyya is a Professor in the Computer Science & Engineering Department at Tezpur University. His research areas include Machine Learning, Network Security and Bioinformatics. Prof. Bhattacharyya has published more than 250 research papers in the leading international journals and conference proceedings. In addition, Dr Bhattacharyya has written/edited more than 13 books.

Jugal Kumar Kalita is a Professor in the Department of Computer Science, College of Engineering and Applied Science, University of Colorado, Colorado Springs, United States. Dr. Kalita's research areas include Artificial Intelligence, Bioinformatics, Natural Language Processing, Machine Learning and Network Security. He has published around 200 research papers in the leading international journals and conference proceedings. In addition, Prof. Kalita has written/edited 4 books.