International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 3, Issue 4, July 2014, 113-124

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

SCATTERED ALTER POSITION ATTACKER DETECTION OF APP-DDOS ATTACKS WITH GAUSSIAN-POLYNOMIAL DISTRIBUTION MODEL

VINCE PAUL A[1] & K. PRASADH[2]

[1]Research Scholar, Singhania University, Jaipur, Rajasthan, India

[2]Principal, Mookambika Technical Campus, Moovattupuzha, Kerala, India

ABSTRACT

App-DDoS attack is Application layer Distributed Denial of Service attack which attempt to avoid a server from donating the services to the rightful users. It is more proficient for the attackers to exhaust the resources like bandwidth and processing power. This type of App-DDoS attack slows down the server responses to the clients and occasionally it may also refuses their accesses. The previous work presented a Gaussian distribution factor to enhance the attack resistance scheme in the application DDoS attacks followed by a polynomial distribution method. This method is used for organizing the packet data which is sent with application services but fails to provide the detection accuracy and cost.

Approach: To improve the detection accuracy and cost factor of the network, in this work, we are going to present a Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT) integrated with Gaussian- Polynomial Distribution Model. The idea is to detect abrupt changes across network domains at the earliest time. Early detection of DDoS attacks minimizes the damages to the fatality systems serviced by the provider.

Results: Performance of Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT) is evaluated in terms of traffic rate, TCT detection rate based on threshold value.

Conclusion: Investigational outcome show that network domains are sufficient to yield 98 percent detection accuracy when compared with the present work.

KEYWORDS: Scattered Alter Position Detection, App-DDOS Attacks, Transform Composite Trees, Gaussian, Polynomial Distribution Model, Attack Resistance

INTRODUCTION

Nowadays, protection systems against App-Distributed Denial-of Service (App-DDoS) attacks are mostly built on detecting overflow consequences rather than the causes of the interchange stream. Overflow result when excess of packet waits on communication links. Regrettably, the damage has been done when the overflow consequence is observed. Thus, it is extremely popular to detect App-DDoS attacks at the earliest possible time, instead of waiting for the overflow to become widespread. The basic form of an App-DDoS attack is the simple high bandwidth DDoS attack. In the effortless brute force overflow, the attacker sends a lot of traffic which consumes the network resources such as bandwidth of the server's incoming link. This can be achieved by sending a huge amount of traffic over a raw socket, each impersonate the requirements of a normal client.

To realize a competent defense system, we must manipulate the network topology and use disseminated traffic monitoring and detection. In reality, we build an App-DDoS defense system over a limited number of network domains

serviced by the equivalent Internet service provider (ISP). These ISP network domains envelop the edge networks where the confined systems are actually associated.

Distributed denial of service attacks are a huge danger to service availability in cloud computing. In recent years, DDoS attacks have amplified tremendously in bandwidth and technique. In this article, Ruiping Lua., and Kin Choong Yow., 2011, propose a novel approach to moderate DDoS attacks by means of an intelligent fast-flux swarm network. An intelligent swarm network is necessary to make sure autonomous coordination and allocation of swarm nodes to execute its relaying operations. It adapted the Intelligent Water Drop algorithm for distributed and parallel optimization. The fast-flux technique was used to preserve connectivity between swarm nodes, clients, and servers.

Udi Ben-Porat., et. Al., 2012 proposed a metric based on the vulnerability of a system. This vulnerability metric evaluates a Hash table data structure which is commonly used in network mechanisms. It shows that Closed Hash is much more vulnerable to DDoS attacks than Open Hash, even though the two systems are considered to be equivalent by traditional performance evaluation. It applies this metric to queuing mechanisms which are common to computer and communications systems. Further more, hash table whose requests are controlled by a queue still suffer from performance degradation.

App-DDoS attack is a type of DDoS attack in the application layer which sends out requests which are interchangeable from genuine requests in the network layer. Most application layer protocols, namely HTTP1.0/1.1, FTP and SOAP are built on TCP and they exchange a few terms with users using congregation which consist of one or many requests. As App-DDoS attacks are interchangeable from rightful requests based on packets and protocols of network layer. Most existing scheme uses packet rate as a metric to recognize attackers. But intelligent users can regulate the packet rate based on server's response to avoid detection. Even IP address based filtering is not possible as attackers might cover at the back of proxies and even the IP addresses can be spoofed.

Application layer DDoS attacks employ rightful HTTP requests to overflow victim's resources. Attacker's attacks the sufferer web servers by HTTP function named GET requests and pulling large files from victim server. Occasionally attackers can run large number of queries through sufferers search engine and bring the server down without responding to the clients.

The method we propose consists of detecting the attackers and leading to the performing the accuracy using the Scattered Alter Position Detection (SAD) structural design integrated with Transform Composite Trees (TCT)a and Gaussian- Polynomial Distribution Model. Early detection of DDoS attacks minimizes the overflow damages to the sufferer systems serviced by the provider. The system makes the assault-transport routers for working cooperatively. Each ISP domain has a TCT server to composite the overflow alerts reported by the routers. TCT domain servers work together among themselves to generate the ultimate conclusion.

LITERATURE REVIEW

Nowadays, DDoS attacks are not simple task in detecting application layer. DDOS attack is a critical threat to the internet. Saketh Kumar shakkari and G. Varalakshmi., 2011, propose a simple algorithm to detect the DDOS attack. The algorithm is going to calculate transmission delay in the net work. Consider the transmission delay the algorithm profits to do some computations to detect the DDOS attack. Since DoS attacks are attempts to disable the functionality of the target, as opposite to ahead operational control, they are a great deal more difficult to defend against than traditional

invasive exploits, and are practically impossible to eliminate. Gaston Ormazabal1., et. Al., 2008 designed and demonstrated effective defenses against SIP-specific DoS attacks, with the capability to operate at carrier-class rates.

This survey Sven Ehlert., et.Al., 2009 explain three different types of DoS attacks on SIP networks, called SIP message payload tampering, SIP message flow tampering and SIP message flooding. We survey dissimilar approaches to counter these types of attacks. S. Renuka Devi and P. Yogesh., 2012 proposes a detection scheme based on the information theory based metrics. The proposed scheme has two phases: Behaviors monitoring and Detection. In the first phase, the Web user browsing behavior (HTTP request rate, page viewing time and sequence of the requested objects) is captured from the system log during non attack cases. Based on the observation, Entropy of requests per session and the trust score for each user is calculated.

A lightweight mechanism is proposed by Ms. Manisha., et. Al., 2011 which uses trust to distinguish legitimate users and attackers. Trust to client is evaluated based on his visiting history and requests are scheduled in declining order of trust. Jéerôme François., et. Al., 2012 address the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of Fire Col. The core of FireCol is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. Khaled Salah., et. Al., 2012, present an analytical queuing model based on the embedded Markov chain to study and examine the performance of rule-based firewalls when subjected to normal traffic flows as well as DoS attack flows targeting different rule positions.

During a distributed denial-of-service (DDoS) attack, network-connected personal computers are made to attack other computers via the Internet. A victim computer under DDoS attack exhausts its computing resources as it is completed to process a huge amount of DDoS traffic by Sanjeev Kumar., and Sirisha Surisetty., 2012. MyungKeun Yoon., et. Al., 2011, intend a new spread estimator that delivers good performance in tight memory space where all existing estimators no longer work. The new estimator not only achieves space compactness, but operates more professionally than the existing ones.

Zhenhai Duan., et. Al., 2012 develop an effectual spam zombie detection system named SPOT by monitoring outgoing messages of a network. SPOT is intended based on a powerful statistical tool called Sequential Probability Ratio Test, which has bounded false positive and false negative error rates. Enrico Cambiaso., et. Al., 2012 examine the most common slow Denial of Service attacks to web applications, proposing a taxonomy to classify such attacks. The proposal of our work is to build an overview and to classify slow DoS attacks for a better understanding of their action strategy, thus helping developers and network administrators to design proper protection methodologies.

Jun Wu., et. Al., 2010, present a neural network approach to detecting the DDoS attacks towards the domain name system. A multi-layer feed-forward neural network is engaged as a classifier based on the chosen features that reflect the characteristics of DDoS attacks. The performance and the computational competence of the neural network classifier are both evaluated.

To prevent the App-Distributed Denial of Services attack Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT) integrated with Gaussian- Polynomial Distribution Model is presented.

SCATTERED ALTER POSITION DETECTION (SAD) STRUCTURAL DESIGN

A distributed server are maintained in the network contains many Open System Information (OSI) Model.

This OSI model contains the 7 types of layers in which the application layer provides the application services. These application services are endangered for attacks termed as Distributed Denial of service attacks. Normally, attackers commence DDoS attacks by expressing an immense amount of attack sources to launch an ineffective traffic to the victim.

After the application services are identified, the Gaussian-Polynomial distribution model is used to distribute the application services based on their categorization. The packet streaming is used with the distribution model of application services for routing the packet data and destroy the App-DDoS attacks by equating the distribution of application services with network traffic. It resists the attacks and provides the improved security.

The Scattered Alter position Detection mechanism uses the transform composite tree to detect the attacker accurately with the less cost. The Gaussian - Polynomial distribution of the attack resistance scheme and Scattered Alter Position Detection (SAD) design is briefly described under below sections.

The architecture diagram of the Scattered Alter Position Detection (SAD) structural design logic using Transform Composite Trees (TCT) integrated with Gaussian- Polynomial Distribution Model is shown in the Figure 1.

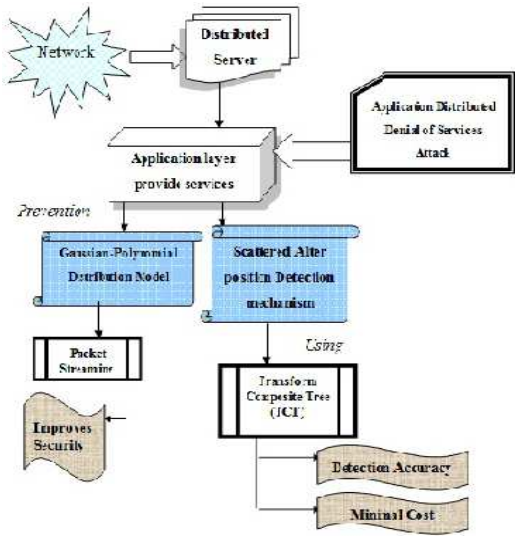

Figure 1: Architecture Diagram of Integral Logical Derivative Rule

The above diagram describes the App-DDoS attacks are prevented using the Gaussian distribution model and Scattered Alter position Detection mechanism. Our SAD approach is exclusive and offers the very first attempt to explore SAD over shared network domains. We detect the App-DDoS overflow attacks by monitoring irregular traffic flows. This monitoring and detection is performed from router to router as the TCT is vigorously constructed. We approved out exhaustive experiments to estimate the SAD scheme. The performance results demonstrate high detection accuracy and low cost effective. This TCT mechanism is designed at the router level for detecting sudden changes in traffic flows. When a App-DDoS attack is launched, the routers watch changes in the spatio-temporal sharing of traffic volumes. The domain server uses the router description traffic surge reports to construct the TCT. Usually, these changes in traffic flows present directionality orientation toward the victim scheme. Arbitrary fluctuations incurred with rightful traffic flows do not present the orientation effects.

SAD Mechanism Using Transform Composite Tree

The SAD mechanism detects App-DDoS overflow attacks by monitoring the transmission patterns of abrupt

traffic changes at dispersed network points. Once an adequately great TCT is constructed to exceed a preset threshold, an attack is declared. This segment presents the principles behind the SAD system. We focus on traffic model alter discovery at the router level.

Principles of Scattered Alter Position Detection

In alter position, it pre changes and post changes the distributions. We adopt a nonparametric approach for simplicity. Let $k_1, k_2,...,k_n$ be discrete point instants and $y(k_n, j)$ be the number of packets established by a router during time slot m at port j. The historical approximation of the average number of packets is defined iteratively by

$$\overline{y}\ (K_n, j) = (1-\alpha)\ \overline{Y}\ (k_{n-1}, j) + \alpha.y(k_n, j) \quad (1)$$

Where, $0 < \gamma < 1$ is an inaction factor showing the sensitivity of the long-term average behavior to the present traffic variation. A superior α implies more dependence on the present variation. We define below T_{in} deviation of input traffic from the average time slot k_n

$$T_{in}\ (k_n, j) = \max\{0, T_{in}(k_{n-1}, j) + y(k_n, j) - \overline{Y}\ k_n, j)\} \quad (2)$$

The subscript in indicates that this is the statistics of the incoming traffic. While a App-DDoS overflow attack is launched, the increasing deviation is obviously higher than the unsystematic fluctuations. Since $T_{in}(k_n, j)$ is responsive to the changes in the average monitored traffic. We measure the irregular divergence from the historical average as follows.

Let the Divergence from Standard (DS) be the indicator of such an attack. The incoming traffic DS is defined below at port j at time k_n.

$$DS_{in}(k_n, j) = T_{in}(k_n, j) / \overline{Y}\ (k_n, j) \quad (3)$$

If the DS exceeds a router threshold β, the measured traffic course is considered a suspicious attack. The threshold β measures the magnitude of traffic course over the average traffic value. This parameter is preset based on previous router use knowledge. If there is no App-DDoS attack then only a small deviation rate below β exist.

For outgoing traffic, we define x (k_n, j) as the number of packets at time k_n leaving at port j and as the historical average of departed packets. Similarly,

$$\overline{X}\ (K_n, j) = (1-\alpha)\ \overline{X}\ (k_{n-1}, j) + \alpha.x(k_n, j) \quad (4)$$

$$T_{out}\ (k_n, j) = \max\{0, T_{out}(k_{n-1}, j) + x(k_n, j) - \overline{X}\ k_n, j)\} \quad (5)$$

The above equations will be used to specify the altered position detection algorithms.

Transform Composite Tree at Server

TCT construction is done at each TCT server of a particular network domain. Different tree are generated in multiple network domains. The comprehensive TCT is generated by merging all sub trees. While the overflow traffic

merges at the victim end, the routers all along the paths detain suspicious traffic patterns. The router reports the identifier of an excellent flow causing the traffic course. Because all routers are under the same ISP authority and work considerately, each router knows their instantaneous neighbors.

Using the reported position information, the domain server detects the traffic overflow based on the TCT constructed. The attentive message provides the upstream and downstream router identifiers. The attentive message provides the information for the TCT server to include the routers in the TCT sub tree. The main purpose of sending the flow status message is to report where the apprehensive flows are captured.

To indicate the location of a disbelieving flow, the router identifier must send. We need to identify the excellent flow identifier of the n-bit prefix of the destination IP addresses. To construct the TCT, the status report provides the information. The domain server constructs the TCT steadily after receiving the attentive reports.

Gaussian Polynomial Distribution Model Using Packet Streaming

A Gaussian- Polynomial Distribution model is a detached resistance model that identifies the attack by distributing information in the middle of contributing routers. The definitive objective of App-DDoS conflict is to modify the attack secure to the attack sources so that consistently network and server re-sources will be conserved. Consequently, routers secure to attack sources must be competent to recognize attack rapidly and precisely. Nevertheless, if the attack sources for an App-DDoS attack are greatly dispersed, modest attack will be experimented by a particular router. When distributing a Gaussian-polynomial over any number of other terms, you distribute each term in the first factor over all of the terms in the second factor. When the distribution is done, you combine anything that goes together to make simpler.

A Gaussian-Polynomial distribution for attack resistance scheme for App-DDoS attacks in the server is the probability distribution of the products obtained from a polynomial and Gaussian experiment. The polynomial formula describes the probability of any product from a polynomial experiment and Gaussian formula is the probability applied on the Gaussian experiment. Suppose a Gaussian-polynomial experiment consists of n application services, and each application services can result in any of k possible packet streams.

Algorithm for the (SAD) Structural Design Using (TCT) Integrated with Gaussian- Polynomial Distribution Model

Our SAD system was designed to have strong collaborations among all domain servers along the excellent flow paths. This algorithm specifies the merge of TCT sub trees for detecting DDoS attacks across multiple network domains with the Gaussian-polynomial distribution model to improve the security. The TCT sub trees constructed at all negotiate domains must be merged to give way a global TCT at the destination domain.

Input: TCT reports from participating domain server where the server detection threshold θ.

Output: The global TCT over multiple domains. Raise the attentive for an forthcoming App- DDoS attack.

Procedure:

Step 1: Identify the application services present in the server
Step 2: If (App-DDoS attack)
Step 3: Apply Gaussian-Polynomial distribution model,
Step 4: Distribute the services based on its categorization
Step 5: Improves the security with minimal time
Step 6: End If
Step 7: Build the neighboring TCT sub tree sporadically
Step 8: Getting sub trees from other TCT servers
Step 9: If (neighboring sub tree) then
Check the excellent flow ID,
Step 10: If (target domain) then
Set distance q = 1
Step 11: Combine sub trees from domains at distance q to the present global tree
Step 12: q $\leftarrow$ q + 1
Step 13: While (unrestrained sub trees),
Generate the TCT profile
Step 14: If (TCT outline >= θ) then
DDoS attack is detected and raises an attentive
Step 15: Else check the root router position
Step 16: If (root router connected to other domain) then
Step 17: Sent the universal TCT to the destination domain server
Step 18: Else Raise an attack attentive based on the universal tree combined.
Step 19: End If
Step 20: End While

The ultimate declaration of an App-DDoS attack is the result of threshold discovery using the universal TCT. Not only the fatality network launches suitable countermeasures, but also some trace back actions are to be along the excellent flow paths. The proceedings comprise reducing of suspicious packets or rate limiting aligned with the flows.

EXPERIMENTAL EVALUATION

The experimental evaluation was carried to implement the proposed Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT) integrated with Gaussian- Polynomial Distribution Model in the NS2 simulator. The network topology is generated by NS2. In our simulation initially 30 clients were taken. Each nodes play again one user's outline composed from synthetic data sources. The fraction of arbitrarily chosen attack nodes to entire nodes is 20%. In addition, guess the attackers can suspend some of the request section of normal surfers and play again this segment to commence the App-DDoS attacks to the victim Web server.

The interval between two continuous attack requests is determined depends on three samples counting stable rate attacks, growing rate attacks and arbitrary pulsing attacks. During the simulation, 35 nodes were contributed in the process. There were six nodes termed as server nodes and remaining nodes were termed as client nodes. Attacker nodes were initiated when Server checkered client arbitrarily one by one. The proposed Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT) for detection accuracy in App-DDoS attacks is measured in terms of

- Traffic rate
- TCT detection rate
- Cost Efficiency

RESULTS AND DISCUSSIONS

In this work, we efficiently evaluated the detection accuracy using the Scattered Alter position Detection with the Transform Composite Tree. The experiments are efficiently conducted with the group of clients with servers to estimate the performance. The below table and graph describes the performance of the Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT) with a Flow Correlation Efficient (FCC) and Polynomial Distribution Model (PDM).

Traffic Rate: The Scattered Alter position Detection performs a lesser traffic on the sample point of flows in the simulator.

Table 1: Sampling Point of Flows vs. Number of Traffic

Sampling Point of Flows	Number of Traffic		
	Proposed SAD-TCT	FCC Scheme	PDM Model
20	210	400	530
40	215	420	550
60	225	435	565
80	230	445	575
100	245	465	580
120	255	480	595
140	260	485	620
160	275	495	625
180	280	510	660

The sampling point of flows are used to calculate the number of traffic occurring on the proposed Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT), Flow Correlation Efficient (FCC) and Polynomial Distribution Model (PDM). The above table (table 1) describes the number of traffic based on the number of samples participate in it.

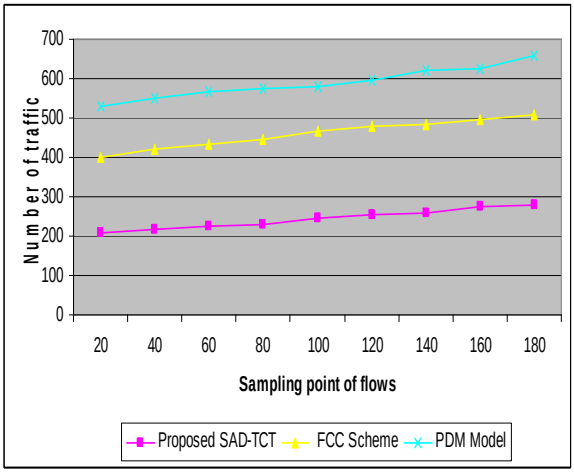

Figure 2: Sampling Point of Flows vs. Number of Traffic

Figure 2 describes the traffic rate occurring on the system. The proposed SAD-TCT efficiently identified the traffic rate occurrence. The traffic rate occurred are reduced by the Transform Composite Tree (TCT) in which the domain count posts a movable higher vault on the expected number of ISP domains. The outcome of the proposed Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT) is analyzed. In the proposed SAD-TCT scheme, each generated neighboring and universal tree are mapped to a balanced equivalence. The variance in number of traffic occurrence in the proposed scheme is 30-40% low than the other schemes which are compared.

Detection Rate: The detection rate is defined as the rate at which the attackers are identifies in the application server.

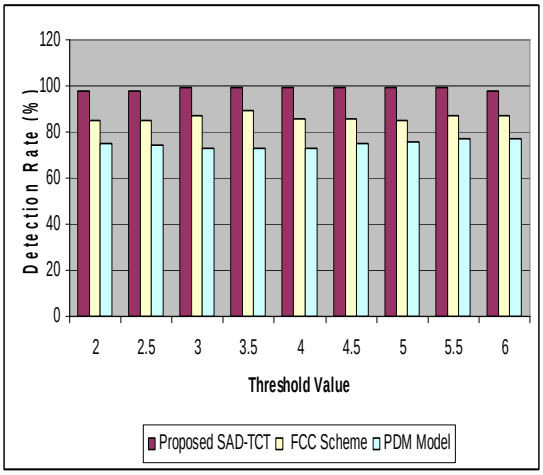

Figure 3: Threshold Value vs. Detection Rate

Figure 3 described the detection rate based on the threshold value. When the traffic flow exceeds the threshold the router raises an attentive. No attentive will be raised if indiscretion is detected at the routers of the existing systems. It is overcome in the proposed Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT). Compared to a Flow correlation coefficient and polynomial distribution model, the proposed SAD-based on the transform composite tree produces approximately 65% higher detection rate.

Cost Efficiency: It is the rate at which the cost is measured. The proposed SAD-TCT produces the lower cost when compared to the all other systems.

Table 2: Threshold Value vs Detection Rate

No. of Nodes	Cost Efficiency		
	Proposed SAD-TCT	FCC Scheme	PDM Model
5	37	62	85
10	36	61	84
15	36	60	83
20	35	58	82
25	34	57	82
30	32	59	81
35	31	58	80
40	33	57	78

Table 3: No. of Nodes vs. Cost Efficiency

Threshold Value	Detection Rate (%)		
	Proposed SAD-TCT	FCC Scheme	PDM Model
2.0	98	85	75
2.5	98	85	74
3.0	99	87	73
3.5	99	89	73
4.0	99	86	73
4.5	99	86	75
5.0	99	85	76
5.5	99	87	77
6.0	98	87	77

Figure 4, described the cost efficiency based on the nodes. The proposed Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT) is compared with the Flow Correlation Efficient (FCC) and Polynomial Distribution Model (PDM) in terms of cost efficiency. The overflows are removed in the server and the traffic is reduced by the TCT scheme to satisfy the client's request. The attacker nodes are removed spontaneously in the proposed scheme.

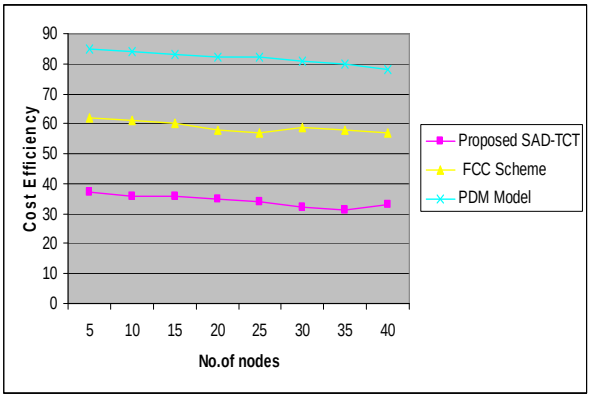

Figure 4: No. of Nodes vs. Cost Efficiency

The performance graph of the proposed Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT) rate is shown in the figure 4. The scattered position with the Gaussian- Polynomial distribution model will identify the DDoS attack on the application services efficiently when compared with the Flow Correlation Efficient (FCC) model and Polynomial Distribution Model (PDM) scheme. The variance in the cost efficiency would be 30 – 40 % less in the proposed Scattered Alter Position Detection (SAD) structural design using Transform Composite Trees (TCT) scheme.

Finally, it is being observed that the proposed SAD-TCT eradicates the cost consuming process to detect the attackers very efficiently. TCT domain servers work together among themselves to make the final decision with the experimental proof.

CONCLUSIONS

A Scattered Alter position Detection scheme with the Transform Composite Tree (TCT) is used for performing the detection accuracy and cost efficiency by eradicating the Application DDoS attacks. The Gaussian-Polynomial Distribution model is developed as attack resistance scheme for App-DDoS attacks in which the services are distributed

based on its classification prior to packet streaming. It is beneficial system to detect the DDoS overflow attacks at their early stages and to avoid the mass damage on the victim system. We developed a DDoS detection system based on a new TCT mechanism. In addition the performance of the proposed Scattered Alter Position Detection (SAD) design using Transform Composite Trees (TCT) integrated with Gaussian- Polynomial Distribution scheme protects the services from DDoS attacks is measured with metrics such as traffic rate, TCT Detection rate and cost efficiency. In contrast to the FCC, the proposed SAD-TCT scheme is 65 % higher in detection accuracy. An analytical and empirical result shows the 30 – 40 % lesser cost efficiency due to the TCT mechanism of our proposed scheme.

REFERENCES

1. Udi Ben-Porat., Anat Bremler-Barr., and Hanoch Levy., "Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks," IEEE transaction on Computers, Digital Object Indentifier 10.1109/TC.2012.49 0018-9340/12/$31.002012
2. Ruiping Lua., and Kin Choong Yow., "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, 0890-8044/11/$25.00 July/August 2011
3. Saketh Kumar shakkari and G.Varalakshmi., "Detection of application layer DDOS attack for a popular website using delay of transmission," INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES, (IJAEST), Vol No. 10, Issue No. 2, 181 – 184, ISSN: 2230-7818, 2011
4. S. Renuka Devi and P. Yogesh., "DETECTION OF APPLICATION LAYER DDOS ATTACKS USING INFORMATION THEORY BASED METRICS," DOI: 10.5121/csit.2012.2223, pp. 217–223, 2012.
5. Sven Ehlert., Dimitris Geneiatakis., Thomas Magedanz., "Survey of network security systems to counter SIP-based denial-of-service attacks," Elsevier computers & security, 2009
6. Gaston Ormazabal1., Sarvesh Nagpal., Eilon Yardeni., and Henning Schulzrinne., "Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems," Springer journal, 2008
7. Ms. Manisha., M. Patil1., and Prof. U. L. Kulkarni., "Mitigating App-DDoS Attacks on Web Servers," International Journal of Computer Science and Telecommunications [Volume 2, Issue 5, August 2011
8. Jéerôme François., Issam Aib., and Raouf Boutaba., "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks," IEEE/ACM TRANSACTIONS ON NETWORKING, Digital Object Identifier 10.1109/TNET.2012.2194508, 2012
9. Khaled Salah., Khalid Elbadawi., and Raouf Boutaba., "Performance Modeling and Analysis of Network Firewalls," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 9, NO. 1, MARCH 2012
10. Sanjeev Kumar., and Sirisha Surisetty., "Microsoft vs. Apple: Resilience against Distributed Denial-of-Service Attacks," Computer and Reliability Societies, IEEE, 2012
11. MyungKeun Yoon., Tao Li., Shigang Chen., and Jih-Kwon Peir., "Fit a Compact Spread Estimator in Small High-Speed Memory," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 19, NO. 5, OCTOBER 2011
12. Zhenhai Duan., Peng Chen., Fernando Sanchez., Yingfei Dong., Mary Stephenson, and James Michael Barker,

"Detecting Spam Zombies by Monitoring Outgoing Messages," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012

13. Enrico Cambiaso., Gianluca Papaleo., Maurizio Aiello., "Taxonomy of Slow DoS Attacks to Web Applications," Recent Trends in Computer Networks and Distributed Systems Security," Volume 335, 2012
14. Jun Wu., Xin Wang., Xiaodong Lee., Baoping Yan.," Detecting DDoS Attack towards DNS Server Using a Neural Network Classifier," Artificial Neural Networks, ICANN 2010