ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Detecting and Preventing DDoS Attacks in Cloud

Dr. S.SaravanaKumar[1], R.SenthilKumar [2], R.Arun prasad[3], S.Thiraviam[4], J.Vignesh[5]

Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[1]

Associate Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[2]

UG Student, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[3,4, 5]

ABSTRACT: Cloud is becoming a dominant computing platform. Naturally, a question that arises is whether we can beat notorious DDoS attacks in a cloud environment. Researchers have demonstrated that the essential issue of DDoS attack and defence is resource competition between defenders and attackers. A cloud usually possesses profound resources, and has full control and dynamic allocation capability of its resources. Therefore, cloud offers us the potential to overcome DDoS attacks. However, individual cloud hosted servers are still vulnerable to DDoS attacks if they still run in the traditional way. In this paper, we propose a dynamic resource allocation strategy to counter DDoS attacks against individual cloud customers. When a DDoS attack occurs, we employ the idle resources of the cloud to clone sufficient intrusion prevention servers for the victim in order to quickly filter out attack packets and guarantee the quality of the service for benign users simultaneously. We establish a mathematical model to approximate the needs of our resource investment based on queueing theory. Through careful system analysis and real-world data set experiments, we conclude that we can defeat DDoS attacks in a cloud environment.

1.1 INTRODUCTION

1.1.1 Aim

The main aim of the project is protect applications against DDoS attacks in cloud computing. Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. In this project, we have used a distance-based DDoS technique which uses a simple but effective exponential smoothing technique to predict the flooding attack.

1.1.2 Synopsis:

Cloud is becoming a dominant computing platform. Naturally, a question that arises is whether we can beat notorious DDoS attacks in a cloud environment. Researchers have demonstrated that the essential issue of DDoS attack and defence is resource competition between defenders and attackers. A cloud usually possesses profound resources, and has full control and dynamic allocation capability of its resources. Therefore, cloud offers us the potential to overcome DDoS attacks. However, individual cloud hosted servers are still vulnerable to DDoS attacks if they still run in the traditional way. In this paper, we propose a dynamic resource allocation strategy to counter DDoS attacks against individual cloud customers. When a DDoS attack occurs, we employ the idle resources of the cloud to clone sufficient intrusion prevention servers for the victim in order to quickly filter out attack packets and guarantee the quality of the service for benign users simultaneously. We establish a mathematical model to approximate the needs of our resource investment based on queueing theory. Through careful system analysis and real-world data set experiments, we conclude that we can defeat DDoS attacks in a cloud environment.

II. SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. There have been a lot of methodologies and tools devised to detect DDoS attacks and reduce the damage they cause. Still, most of the methods cannot simultaneously achieve.

- Efficient detection with a small number of false alarms

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

- Real-time transfer of packets.

2.2 PROPOSED SYSTEM

In this project we have used average distance estimation based DDoS detection technique. In this technique we estimate the mean value of distance in the next time period by using the exponential smoothing estimation technique. This distance-based traffic separation DDoS detection technique uses MMSE (Minimum Mean Square Error) linear predictor to estimate the traffic rates from different distances. If the real value is out of the legal scope, an anomaly situation is detected. In our mitigation algorithm, we do not involve specific detection methods; rather, we focus on the resource management aspect of detection.

III. DDOS MITIGATION ALGORITHM

3.1 INTRODUCTION

In computing, a **denial-of-service** (**DoS**) or **distributed denial-of-service** (**DDoS**) **attack** is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, distributed denial-of-service attacks are sent by two or more people, or bots, and denial-of-service attacks are sent by one person or system. As of 2014, the frequency of recognized DDoS attacks had reached an average rate of 28 per hour. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit cardpayment gateways, and even root nameservers. Denial-of-service threats are also common in business, and are sometimes responsible for website attacks. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games, such as popular Minecraft multiplayer worlds, known as servers. Increasingly, DoS attacks have also been used as a form of resistance. Richard Stallman has stated that DoS is a form of 'Internet Street Protests' The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately. Denial-of-service attacks are considered violations of the Internet Architecture Board's Internet proper use policy, and also violate the acceptable use policies of virtually all Internet service providers. They also commonly constitute violations of the laws of individual nations. The first demonstrated DDoS attack was introduced by well known hacker Khan C. Smith during a 1998 illegal Defcon event and later exposed for its use Botnet mechanisms during a lawsuit filed by Earthlink which claims has caused billions in economic damages.

3.2 IDEA

Instead of blocking/accepting flows we shape their source IPs.
Conditional Legitimate Probability (CLP) [5] is the probability of a flow to be legal.

$$CLP(p) = \frac{Nn \cdot Pn(A = ap) \cdot Pn(B = bn) \cdot \ldots}{Nm \cdot Pm(A = ap) \cdot Pm(B = bn) \cdot \ldots}$$

where Nn is the number of normal packets, Nm the number of measured packets(mixture of normal and attack traffic) and P(A = ap) the probability of a feature A to be ap.
CLP is calculated on the basis of previously observed traffic, e.g. histograms on
source IP prefixes, packet sizes or server ports The higher the CLP, the higher the assigned bandwidth during a DDoS incident Challenge.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

3.1.3 TRAFFIC SHAPING

✓ Easy and fast algorithm for high packet rates
✓ Specialized for DDoS mitigation (filter parameter only source IP)
✓ IP ranges are continuous intervals r over IP addresses [rstart, rend] with a defined bandwidth limit
✓ List of ranges can be sorted to perform binary search:
o ri, rj 2 R, i < j : rendi < rstart j
✓ Every arriving packet is accepted, queued or dropped, similar to Random Early
✓ Detection (RED) [4] in the Packet Handler function.
✓ A triggered function Timer Handler sends packets (with respect to the definedbandwidth) and calculates the used bandwidth
✓ Complexity for each incoming packet is O(log2 n), where n is the number of IPranges with bandwidth limits.
✓ Worst case complexity: every source IP address has a different target bandwidth O(log2 232) = 32 lookups for each incoming packet.

3.1.4. SHAPING ALGORITHM

1: function packet handler(Packet p)
2: r range including. p.source IP using binary search
3: if r not found then
4: accept(p) and return
5: q queue of r
6: if not q.empty or r.sent+p.size > r.limit then
7: if q.size < q.max size then
8: q.push(p)
9: steel(p)
10: else drop(p)
11: else
12: r.sent + = p.size
13: accept(p)
14: function timer handler
15: for all ranges r do
16: r.sent 0; finished false
17: q queue of r
18: while not q.empty and not finished do
19: p q.front()
20: if r.sent + p.size < r.limit then
21: send(p)
22: q.pop()
23: r.sent += p.size
24: else finished true

3.1.5 EVALUATION

•Measuring throughput of a legal (not shaped) user on a 1GBit/s link depending on the number of shaped IP ranges.
• tc throughput decreases at 400 shaped ranges, not enough to mitigate DDoS Attacks

IV. MODULES

1. Cloud Application Development
a) Weather Service application development.
b) Web Service creation.
2. Web Proxy Implementation
a) Proxy Design

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

b) Proxy Web services Implementation

3. Prevent DDoS Attack

a) Average Distance Estimation

4.1 MODULES EXPLANATION

1) Cloud Application Development

The cloud application is Weather Information application which resides on cloud server. This application communicates with web services to provide service to users.

a) Weather Information application:

This module is responsible for obtaining user's input and response with valid output.

b) Web Service creation:

Creating web services which are communicate with cloud application for necessary operations.

2) Web Proxy Implementation

The web proxy works as middleware between the cloud server and the browser. The proxy also resides on cloud server which is monitoring the requests and responses to the server. It is the key to detect DDoS attacks.

a) Proxy Design:

The proxy is responsible for monitoring requests to the client application. It detects the system name, IP address, requested URL, time and monitors it which is invoked from the client.

b) Proxy Web services Implementation:

The proxy communicates with some web service methods in order to monitor web requests. This sub module is responsible for creating proxy web services.

3) Prevent DDoS Attack

In this project we have used average distance estimation based DDoS detection technique. In this technique we estimate the mean value of distance in the next time period by using the exponential smoothing estimation technique. This distance-based traffic separation DDoS detection technique uses MMSE (Minimum Mean Square Error) linear predictor to estimate the traffic rates from different distances.We calculate the distance value based on the TTL field of an IP header directly during transit, each intermediate router deducts one from the TTL value of an IP packet. Therefore, the distance of the packet is the final TTL value subtracted from the initial value. Therefore, the initial value can be determined by choosing the smallest initial value of all the possible values which are larger than the final TTL value. The detection of anomaly relies on the description of normality and deviation. The exponential smoothing estimation technique is chosen because of its successful application in the real time measurement of the round trip time of IP traffic. The exponential smoothing estimation model predicts the mean value of distance dt+1 at time t+1 using:

$$d_{t+1} = d_t + w * (M_t - d_t)$$

Here, dt is a distance value at time t predicted at time t-1, Mt is the measured distance value at time t, w is a smoothing gain, and Mt − dt is the error in that prediction at time t. If w is higher, the last prediction error has the more weight in predicting the next distance value. As a result, the predicted values represent the actual distance value fluctuation more closely.

To determine whether the current distance value is abnormal or not, mean absolute deviation (MAD) can be utilized:

$$MAD = \frac{1}{n} * \sum_{i=1}^{n} | e_t |$$

Where, *n* is the number of all past errors and *et* is the prediction error at time *t*. However, it is not realistic to maintain all the past errors. Therefore, we use the exponential smoothing technique to calculate MAD based on the approximation equation as defined below:

$$MAD_{t+1} = r * \ | e_t | + (1 - r) * MAD_t$$

Where, *MADt* is the MAD value at time *t*. *r* is a smoothing gain. If the real value at the next moment is out of the legal scope, an anomaly situation is detected.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

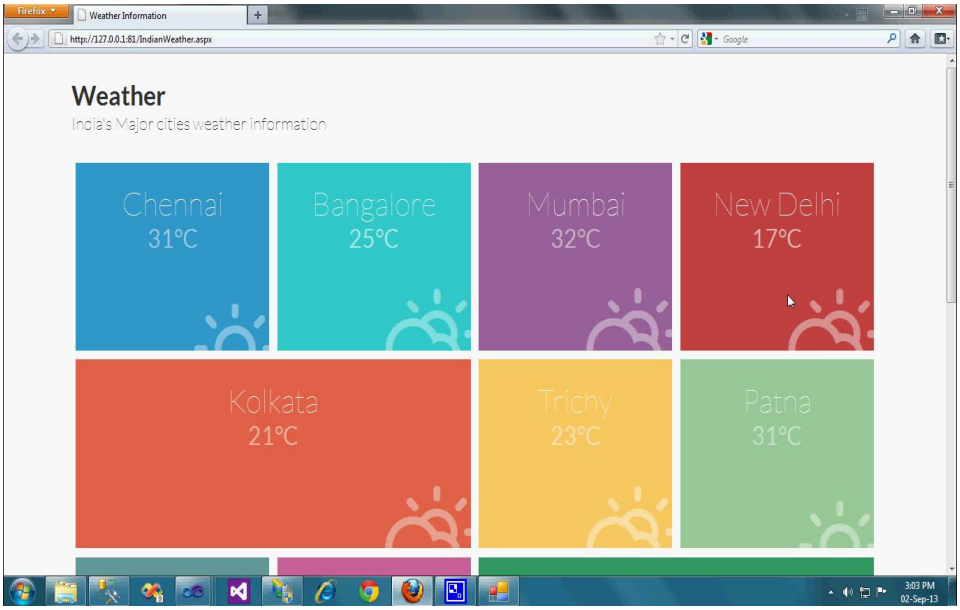
International Journal of Innovative Research in Computer and Communication Engineering

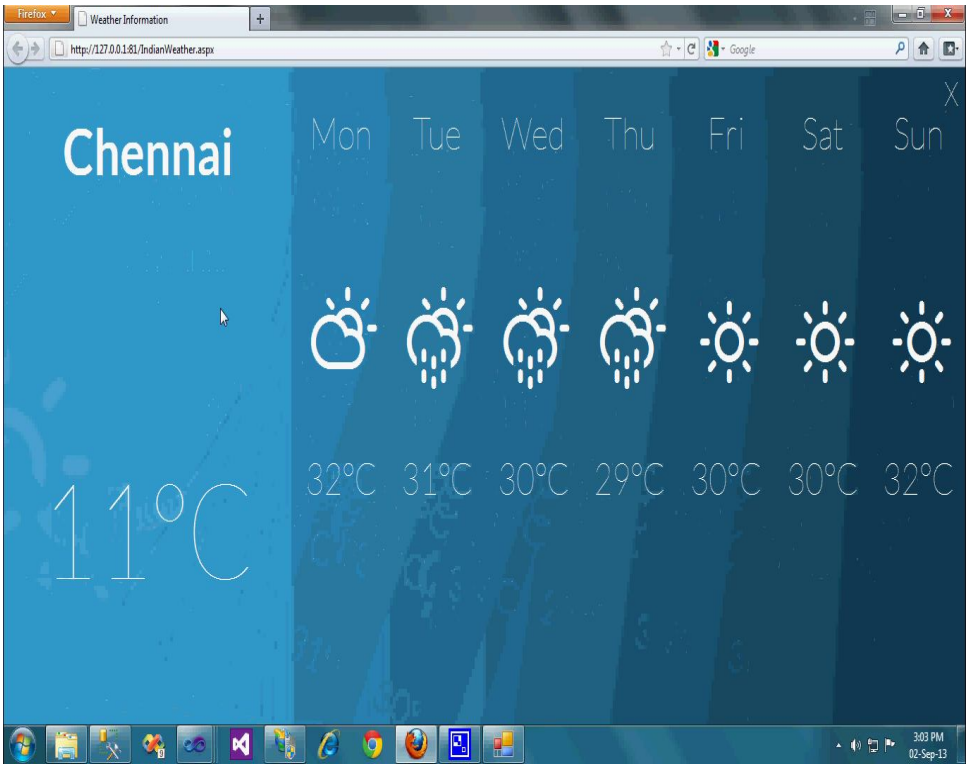
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

SCREEN SHOTS

WEATHER SERVICE APPLICATION





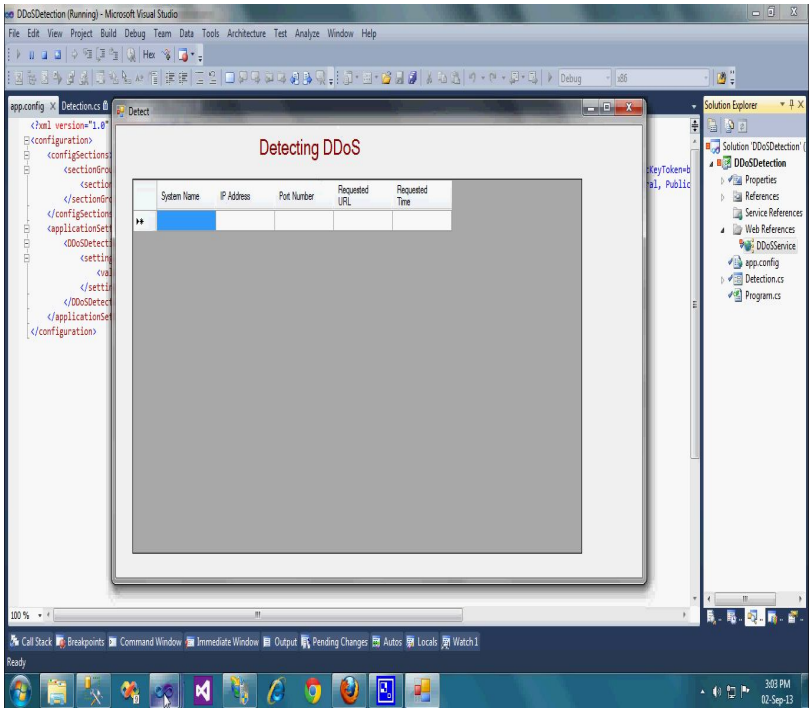
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

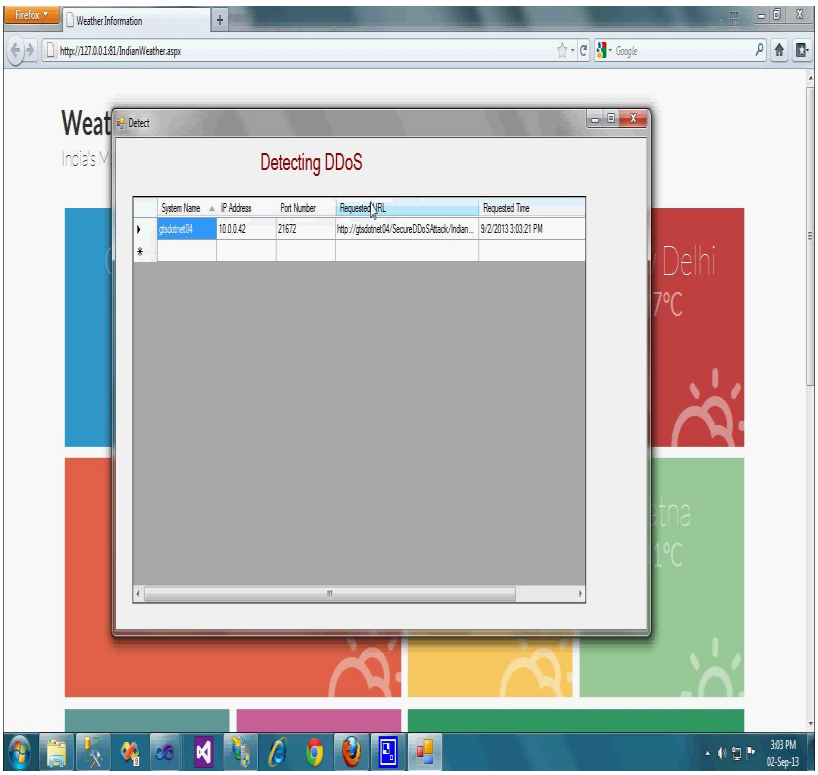
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

WEB PROXY IMPLEMENTATION



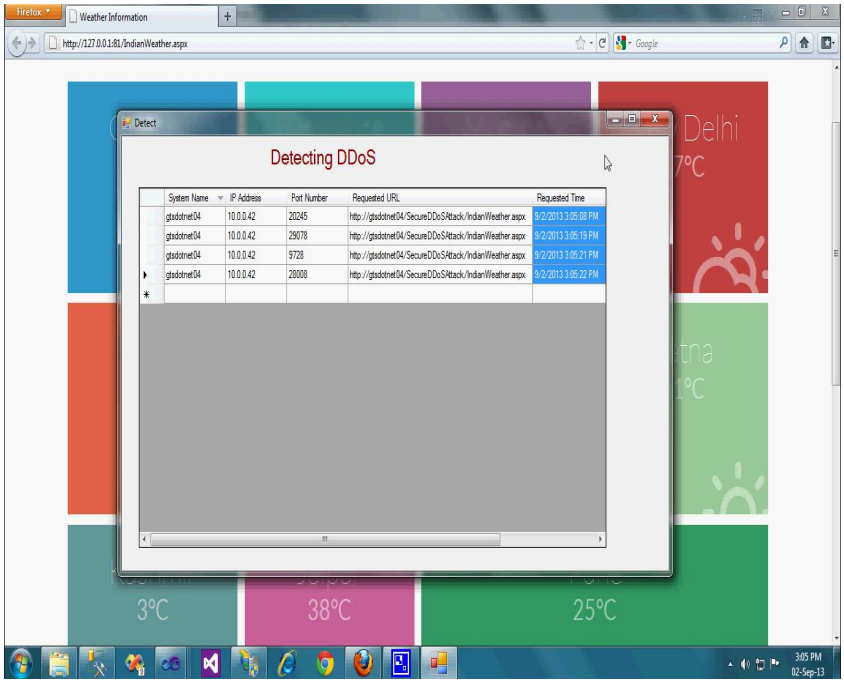


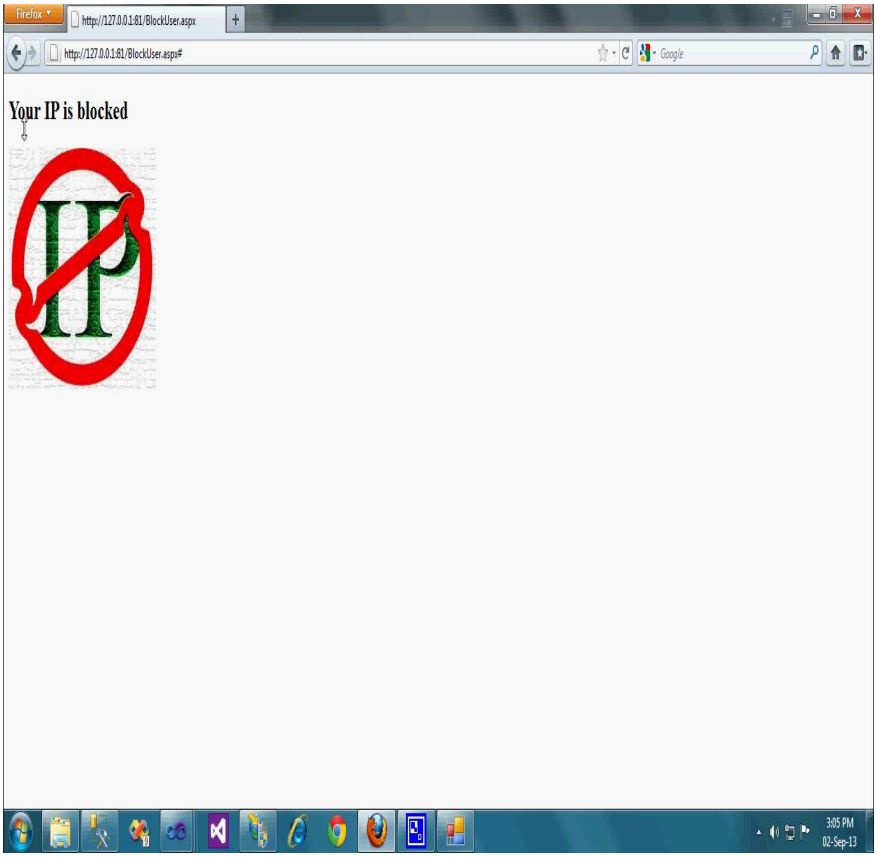
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015





ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

V. CONCLUSION

There is an alarming increase in the number of DDoS attack incidents. Not only, DDoS incidents are growing day by day but the technique to attack, botnet size, and attack traffic are also attaining new heights. Effective defense measures needed to prevent and mitigate these attacks is the current need of the hour. In this paper, we introduce techniques for detecting and controlling flooding and DDoS attacks in MANET. They have most of the problems of wired networks and many more due to their specific features: dynamic topology, limited resources, lack of central management points. First, we have presented specific vulnerabilities of this new environment. Then we have surveyed the attacks that exploit these vulnerabilities and the possible proactive and reactive solutions proposed in the literature. Attacks are classified into passive and active attacks at the top level. Then various Preventive measures are discussed in order to mitigate the effects of DDOS attack in MANET. To conclude, MANET security is a complex and challenging topic.

VI. FUTURE WORK

- Support more than one parameter for shaping
- Investigate FIS trees [3] with O(log2 log2N) lookup complexity.

REFERENCES

[1] Foster, Ian, Yong Zhao, Ioan Raicu, et al, "Cloud Computing and Grid Computing 360-Degree Compared", In Grid Computing Environments Workshop (GCE), Austin, 2008.
[2] Peter Mell and Timothy Grance. The NIST Definition of Cloud Computing. Technical Report SP 800-145 Draft, National Institute of Standards and Technology, Information Technology Laboratory, January 2011.
[3] Martin Litoiu, Murray Woodside, Johnny Wong, Joanna Ng, Gabriel Iszlai, "A Buisness Driven Cloud Optimization Architecture", Proceedings of ACM in SAC'10, pp.380 – 385.
[4] Cai, M., K. Hwang and Y. Chen, "Hybrid Intrusion and Anomaly Detection with Weighted Signature Generation", IEEE Trans. On Dependable and Secure Computing, revised Sept. 2005.
[5] JelenaMirkovic, Janice Martin and Peter Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms", Computer Science Department,University of California, Los Angeles.
[6] The Swiss Education and Research Network, "Default TTL values in TCP/IP,"Available at http://secfr.nerim.net/docs/fingerprint/en/ttldefault.html, 2002.
[7] Zhou, R. and K. Hwang, "Trust-Preserving Overlay Networks for Global Reputation Aggregation in Scalable P2P Systems ", IEEE transaction on Parallel and Distributed Systems, (TPDS), revised March 2006.
[8] Houle, K., G. Weaver, N. Long, and R. Thomas, "Trends in Denial of Service Attack Technology", CERT Coordination Center Document, 2001, www.cert.org/archive/pdf/.
[9] Dittrich, D., "The 'Stacheldraft' Distributed Denial of Service Attack Tool," http://staff.washington.edu/dittrich/, 2000.
[10] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, "COSSACK: coordinated suppression of simultaneous attacks," in Proceedings of DARPA Information Survivability Conference and
Exposition, 2003, pp. 2–13.