ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Denial-Of-Service Attack Detection Using Artificial Neural Network Based On Genetic Algorithm and Multivariate Correlaton Analysis

Abhilasha B. Pawade, Prof.Santosh T. Waghmode

Department of Computer Engineering, Imperial College of Engg and Research, Pune, India

ABSTRACT-Organized systems or interconnected systems likeWeb servers, Database servers, Cloud Computing servers etc. are now under viruses from network attackers. Denial-Of-Service (DOS) attacks reason for serious crash on this computing systems.The main objective is identifying known and unknown DoS attacks efficiently by learning the patterns of genuine network traffic using multivariate correlatin analysis and artificial neural network. We present a DoS attack detection system that uses Multivariate Correlation Analysis (MCA) and ANN. For exact network traffic description by extracting the geometrical correlations between network traffic features we uses MCA and ANN based attack detection for decision making. Our MCA-based DoS attack detection system uses principle of anomaly based detection in attack recognition. It makes our solution able to identify known and unknown DoS attacks efficiently by learning the patterns of legal network traffic .We are using Genetic Algorithm instead of triangle area map.Genetic algorithms are used to identify more possible attacks.Using KDD Cup 99 dataset efficiency of our proposed system evaluated or calculated.The influences of normalized data and non-normalized data on the performance of the proposed detection system are examined. The results proves that our system is very reliable outperforms two other previously developed state of the art approaches in terms of detection correctness.

KEYWORDS: Multivariate Correlation Analysis,Feature Normalization,Genetic Algorithm,Artificial Neural Network,Denial Of Service Attack

I. INTRODUCTION

DDOS that is Distributed Denial of Service is type of DOS attack in which many compromised systems are there.These compromised systems are generally contaminated with a Trojan which are used to target a single system and it causes a Denial of Service (DoS) attack.DDoS attack sufferes consist end under attack system. Also it consists of all systems which are prohibited by the hacker and unkindly used in the distributed attack.The arriving traffic flooding the sufferer originates from several different sources potentially hundreds of thousands or other in DDoSattack. It makes it unfeasible to stop the attack basically by jamming a single IP address efficiently. Additionally this is very complicated to differentiate genuine user traffic from attack traffic when widen crosswise so many points of origin.

This paper focuses on the detection of DDoS attacks which keeps it away from above mentioned issues.It does not focuses on their casual vectors.Generally non distributed denial-of- service attacks utilize susceptibility to disturb a service by sending few carefully untrue packets. Primarily.For flooding a particular sufferer with enormous traffic uses DDoS attacks. Because of high efficiency the status of attacks in opposition to any kind of service as there is no need to spot. In the casualty it utilizes any particular service particular fault. Because of this, this paper focuses entirely on flooding DDoS attacks. A single intrusion prevention system (IPS) or intrusion detection system (IDS) can barely identify such DDoSattacks.Though they are not situated very close to the casualty. In final case, the IDS/IPS may collide because it needs to contract with an overpowering volume of packets (some flooding attacks reach 10–100 Gb/s). By allowing such vast traffic to transfer through the Internet.It only identify or block it at the host IDS/IPS may strictly strains Internet resources.The foundation of MCA is collected of intrusion prevention systems (IPSs) situated at

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

the Internet service providers (ISPs) level.To protect and work together by exchanging chosen traffic information the IPSs makeup implicit protection rings around the hosts. By using wide simulations the estimate of MCA and an actual dataset is offered.Also its hold up for incremental use in real networks by viewing MCA efficiency and low overhead.

To avoid our server from DDOS attacks we are using MCA system to identify these attacks. In such a way MCA is intended that makes it a service to which customers can subscribe. By computing and exchanging faith scores on possible attacks we participating IPSs beside the path to a subscribed customer join forces (vertical communication). The host they defend the IPSs form implicit protection rings around. When the level of a potential attack is high implicit rings utilizes horizontal communication. The threat is calculated based on the whole traffic bandwidth.This whole traffic bandwidth going to the customer compared to the maximum bandwidth it supports. MCA identifies flooding DDoS attacks and it also helps in identifying other flooding scenarios. Other scenarios of flash crowds and for botnet-based DDoS attacks.In This Paper we are using Artificial Neural Network which has self evolving system so no need to provide manual inputs or feedback for similar type of attack.We are using Genetic Algorithm instead of triangle area map.Genetic algorithms are used to identify more possible attacks.Using KDD Cup 99 dataset efficiency of our proposed system evaluated or calculated.The influences of normalized data and non-normalized data on the performance of the proposed detection system are examined. The results proves that our system is very reliable outperforms two other previously developed state of the art approaches in terms of detection correctness.

II. REVIEW OF LETERATURE

1. Title: Worldwide ISP security report

Author: Arbor, Lexington

Description: In help with the Internet security operations community Arbor Networks, Inc has completed this fourth edition of an ongoing series of annual operational security surveys. This survey, covering a 12-month period from August 2007 through July 2008. It is designed to supply data useful to network operators.Because of which they can make informed decisions about their use of network security technology. These decisions defend their mission critical infrastructure.This also provide as a general resource for the Internet operations and engineering community, recording information on trends and employment of various infrastructure security techniques.

The daily aspects of security in commercial networks are the main focus of survey respondents issued by Operational network securities .In this survey provides results are more exactly represent real world concerns than theoretical and emerging attack vectors which are addressed and speculated about somewhere else[22].

Key Finding In the last three surveys the ISP Security Battle front expands. To combate distributed denial of service (DDoS) attacks most of available security resources are spent by internet service providers. ISPs explains a far more diversified security landscape and significant concerns over domain name system (DNS) spoofing, border gateway protocol (BGP) hijacking and spam this year. Now half of the surveyed ISPs consider their DNS services susceptible approximately.Associated service delivery infrastructure, including voice over IP (VoIP), session border controllers (SBCs) and load balancers are concerned over by others. In 2000, 40 Gigabits from relatively humble megabit beginnings are exceeded attacks. This year largest DDoS attacks have grown a hundred fold to break the 40 gigabit barrier now. Attack size growth continues to extensively outpace the corresponding increase in fundamental transmission speed and ISP infrastructure investment. Aslo it shows the yearly reported maximum attack size.

2.Title: Survey of network- based defense mechanisms countering the DoS and DDoS problems

Author:T. Peng, C. Leckie, and K. Ramamohanarao

Description: Initially internet was designed for openness and scalability.Because of yardsic infrastructures certainly working as envisioned certainly. Cost or Price of this success has been poor security. For example, the Internet Protocol

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

(IP) was designed to hold simplicity of attachment of hosts to networks.It also provides little support for verifying the contents of IP packet header fields. Because of this, itis possible to forged the source address of packets.Therefore difficult to recognize the source of traffic. There is no inherent support in the IP layer to ensure whether a source is approved to access a service. Packets are delivered to their destination, and the server at the destination must make a decision whether to accept and service these packets. Even though defenses like firewalls can be added to defend servers. How to distinguish legal requests for service from nasty access attempts is key challenge for defense. For a server to confirm the validity of those requests if is simple for sources to generate service requests, then it is hard to guard the server from nasty requests. Nasty requests waste the resources of the server. All these issues creates the opportunity for a class of attack known as a denial of service attack [23].

3. Title: The zombie roundup: Understanding, detecting, and disrupting botnets

Author: E. Cooke, F. Jahanian, and D. Mcpherson

Description: Global Internet threads are undergoing a deep transformation from attacks designed only to hold back infrastructure to those that also target people and organizations. A large pool of compromised hosts sitting in homes, schools, businesses, and governments around the world are behind these new attacks. These systems are contaminated with a bot. this bot communicates with a bot controller.Other bots forms what is generally referred to as a zombie army or botnet. Zombie army or Botnets are a very real.Botnets hurriedly evolving problem.Still this problem not well understood or studied. We outline the beginning and structure of bots and botnets which also use data from the operator community in this paper.Today to demonstratethe botnet problem experiments of the Internet Motion Sensor project and honeypot experiment are done.After that we study the usefulness of identifying botnets by frankly monitoring IRC communication or other command and control activity which prove a more broad approach which is required. Concluding by telling a system to identify botnets which use advanced command and control systems by correlating secondary detection data from many sources. It is terrifying new class of attacks which directly impacts the everyday lives of millions of people and endangers businesses around the world. New attacks steal or hacks personal information which can be used to damage reputations and it also brings about significant financial losses. The symptoms of the problem like filtering the spam, hardening web browsers, or building applications that warn in opposition to phishing tricks which are focused by current alleviation techniques. To commit attacks it is crucial to disturb and dismantle infrastructure these tools are important. A large pool of compromised hosts sitting in homes, schools, businesses, and governments around the world are core of all these threats. Impured systems with a bot communicates with a bot controller. Other bots are used to form what is generally referred to as a zombie army or botnet. A bot can be differentiated from other threats by a communication channel to a controller.

III. SYSTEM ARCHITECTURE

Design Goals

The design goals for DoS Attack Detection were:
1) Basic Feature Generation for individual records from network traffic.

2) Feature Normalization is done by using Basic Feature Generation andMultivariation Correlation Analysis is done.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

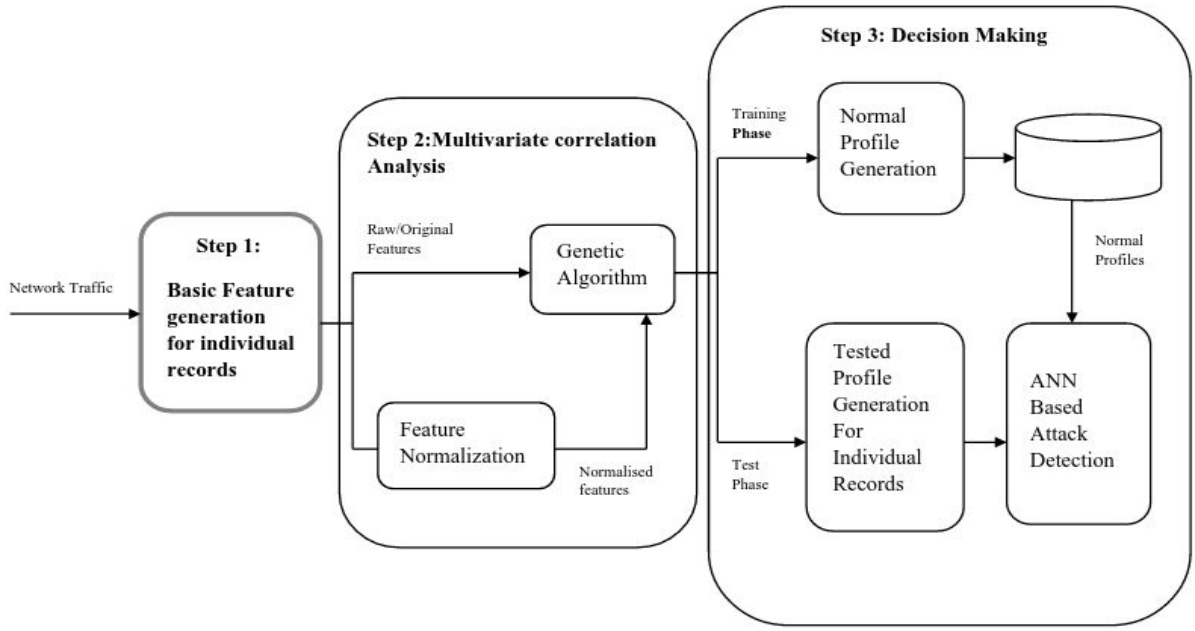
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

3) DoS Attack Detection using Artificial Neural Network.



Fig, Block Diagram for System

The core of MCA is collected of intrusion prevention systems (IPSs).It is situated at the Internet service provider (ISPs) level.By exchanging selected traffic information the IPSs form virtual protection rings around the hosts to guard and cooperate with each other.In above system architecture basic features are generated for individual records from Network Traffic and then by using genetic algorithm and feature normalization in Multivariate Correlation Analysis and after that decision making is done by using Artificial Neural Network by comparing generated normal profiles and generated tested profiles. In this Project MCA and ANN blocked the users, whose creating DDOS attack in the web application.Then put that user on block list.

ALGORITHMS:

Algorithm for Normalization:-K-means Algorithm

Step 1:- We Begin with a decision on the value of k =number of clusters.

Step 2:- Then we put any initial partition which classifies the data into k clusters.

You may assign training samples randomly or systematically as the following:

1. Take the first k training sample as single element clusters.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

2. Assign each of the remaining (N-k) training sample to the cluster with the nearest centroid. After each assignment, recompute the centroid of the gaining cluster.

Step 3:- Take each sample in sequence. Then compute its distance from centroid each of clusters.If sample is not currently in cluster with the closest centroid switch this sample to the cluster and update centroid of the cluster gaining the new sample and the cluster losing the sample.

Step 4:-Repeat step 3 until convergence is achieved that is until a pass through the training sample causes no new assignments.

Genetic Algorithm:-

- **Initialization**
- Initially many individual solutions are randomly generated to form an initial population. The population size depends on the nature of the problem, but typically contains several hundreds or thousands of possible solutions.
- Usually, the population is generated randomly, covering the entire range of possible solutions (the search space).
- Occasionally, the solutions may be "seeded" in areas where optimal solutions are likely to be found.

- **Selection**
- During each successive generation, a proportion of the existing population is selected to raise a new generation.
- Individual solutions are selected through a fitness-based process, where fitter solutions (as measured by a fitness function) are typically more possible to be selected.
- Definite selection methods rate the fitness of each solution and preferentially select the best solutions. Other methods rate only a random sample of the population, as this process may be very time-consuming.
- Most functions are stochastic and designed so that a small proportion of less fit solutions are selected. This helps keep the diversity of the population large and preventing premature convergence on poor solutions. Popular and well-studied selection methods include roulette wheel selection and tournament selection.

ANN Algorithm:- (Training Backpropagation Algorithm)

- The Backpropagation algorithm learns in the same way as single perceptron.
- It searches for weight values that minimize the total error of the network over the set of training examples (training set).
- Backpropagation consists of the repeated application of the following two passes:

Forward pass: In this step, the network is activated on one example and the error of (each neuron of) the output layer is computed.

Backward pass: in this step the network error is used for updating the weights. The error is propagated backwards from the output layer through the network layer by layer. This is done by recursively computing the local gradient of each neuron.

- Backpropagation adjusts the weights of the NN in order to minimize the network total mean squared error.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

IV. RESULT

The system is built on Eclipse IDE and MySQL database using technologies Javascript and JDK 1.7 and Tomcat Apache. We are using KDD Cup 99 Dataset for for efficiency of system . The proposed system gives the estimated results. On the practical results shows our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy. Here following table shows the accuracy as well time complexity how it is better than traditional approaches.

These tables show that the execution timetime and number of iterations.

Index	Time(ms)
1	323
2	238
3	264
4	225
5	219
6	250
7	253

TABLE NAME:- (1 TIME REQUIRED FOR DATA PROCESSING IN PROPOSED VS EXISTING APPROACHES)

The following graph shows comparision of Execution Time.

Where,

X-Axis is No. of Iterations,

Y-Axis is Time in Milliseconds.

According to following graph fluctuations of graph are very less that means our proposed syetm is very reliable.

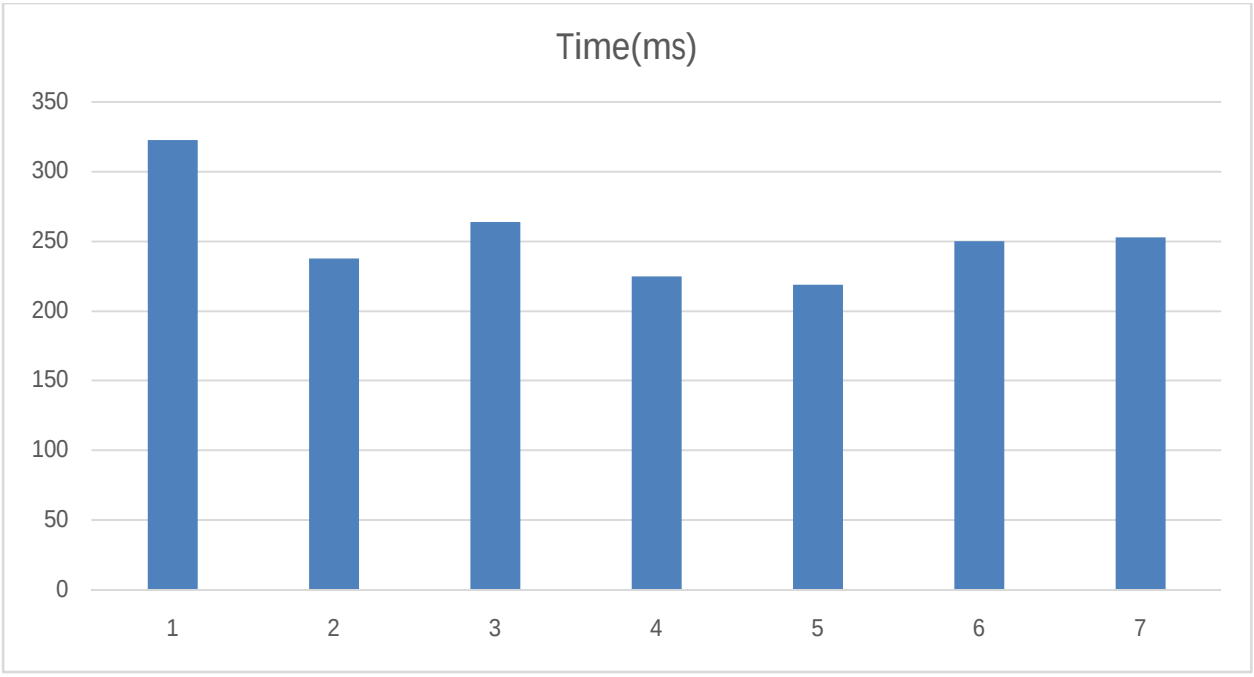
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017



System performance measure proposed vs existing

V. CONCLUSION

This paper presented Denial of service attack detection based on MCA which is powered by genetic algorithm and ANN.We proposed MCA, a scalable solution for the early detection of flooding DDoS attacks. Belief scores are shared within a ring-based overlay network of IPSs.

It is performed as close to attack sources as possible, providing a protection to subscribed customers and saving valuable network resources.

Experiments showed good performance and robustness of MCA and highlighted good practices for its configuration. Also, the analysis of MCA demonstrated its light computational as well as communication overhead. Being offered as an added value service to customers, the accounting for MCA is therefore facilitated, which represents a good incentive for its deployment by ISPs.We will further test our DoS attack detection system using real world data.As a future work, we plan to extend MCA to support different IPS rule structures.

REFERENCES

[1] V. Paxson, "Bro: A System for Detecting Network Intruders in Realtime," Computer Networks, vol. 31, pp. 2435-2463, 1999
[2] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E.Vzquez, "Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges,"Computers& Security, vol. 28,pp. 18-28, 2009.
3] D. E. Denning, "An Intrusion-detection Model," IEEE Transactionson Software Engineering, pp. 222-232, 1987.
[4] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoSattackdetection method using cluster analysis," Expert ystems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.
[5] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, "Intrusion detectionusing fuzzy association rules," Applied Soft Computing, vol. 9,no. 2, pp. 462-469, 2009.
[6] J. Yu, H. Lee, M.-S.Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," Computer Communications,vol. 31, no. 17, pp. 4212-4219, 2008.
[7] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm forNetwork Intrusion Detection," Trans. Sys. Man Cyber. Part B, vol.38, no. 2, pp. 577-583, 2008.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

[8] C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoSAttacks over Multiple Network Domains," Parallel and DistributedSystems, IEEE Transactions on, vol. 18, pp. 1649-1662, 2007.
[9] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods forAnomaly Detection in Aggregate Traffic," Networking, IEEE/ACMTransactions on, vol. 19, no. 2, pp. 512-525, 2011.
[10] S. T. Sarasamma, Q. A. Zhu, and J. Huff, "Hierarchical KohonenenNet for Anomaly Detection in Network ecurity,"Systems, Man,and Cybernetics, Part B: Cybernetics, IEEE Transactions on, vol. 35,pp. 302-312, 2005.
[11] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow CorrelationCoefficient," Parallel and Distributed Systems, IEEE Transactionson, vol. 23, pp. 1073-1080, 2012.
[12] S. Jin, D. S. Yeung, and X. Wang, "Network Intrusion Detection inCovariance Feature Space,"Pattern Recognition, vol. 40, pp. 2185-2197, 2007.
[13] C. F. Tsai and C. Y. Lin, "A Triangle Area Based Nearest NeighborsApproach to Intrusion Detection,"Pattern Recognition, vol. 43, pp. 222-229, 2010.
[14] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R. P. Liu, "RePIDS: Amulti tier Real-time Payload-based Intrusion Detection System,"Computer Networks, vol. 57, pp. 811-824, 2013.
[15] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Denialof-Service Attack Detection Based on Multivariate CorrelationAnalysis," Neural Information Processing, 2011, pp. 756-765.
[16] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "TriangleArea-Based Multivariate Correlation Analysis for Effective Denialof-Service Attack Detection," The 2012 IEEE 11th InternationalConference on Trust, Security and Privacy in Computing andCommunications, Liverpool, United Kingdom, 2012, pp. 33-40.
[17] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Costbased modeling for fraud and intrusion detection: results from theJAM project," The DARPA Information Survivability Conferenceand Exposition 2000 (DISCEX '00), Vol.2, pp. 130-144, 2000.
[18] G. V. Moustakides, "Quickest detection of abrupt changes for aclass of random processes," Information Theory, IEEE Transactionson, vol. 44, pp. 1965-1968, 1998.
[19] A. A. Cardenas, J. S. Baras, and V. Ramezani, "Distributed changedetection for worms, DDoS and other network attacks," The American Control Conference, Vol.2, pp. 1008-1013, 2004.
[20] W. Wang, X. Zhang, S. Gombault, and S. J. Knapskog, "Attribute Normalization in Network Intrusion Detection," The 10th International Symposium on Pervasive Systems, Algorithms, andNetworks (ISPAN), 2009, pp. 448-453.
[21] M.Tavallaee, E. Bagheri, L. Wei, and A. A. Ghorbani, "A DetailedAnalysis of the KDD Cup 99 Data Set," The The Second IEEE International Conference on Computational Intelligence for Securityand Defense Applications, 2009, pp. 1-6.
[22]A.Networks,Arbor,Lexington,MA,"WorldwideISP Security report,"Tech.Re.,2010.
[23] Peng,T.,Leckie,C., and Ramamohanrao,K.2007.Survey of network-based defense mechanisms countering the DoS and DDoSproblems.ACM Comput.Surv.39,1,Article 3(April 2007),42 pages DOI=10.1145/1216370.1216373 http://doi.acm.org/10.1145/1216370.1216373.
[24]E.Coockie,F.Jahanian and D.Mcpherson, "The zombie roundup: Understanding,detecting,and disrupting botnets," in Proc.SRUTI,Jun.2005,pp.39-44.