# Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment

***Anteneh Girma***
Systems and Computer Science Department
Howard University
agirma@howard.edu

***Moses Garuba***
Systems and Computer Science Department
Howard University
moses@scs.howard.edu

***Jiang Li***
Systems and Computer Science Department
Howard University
lij@scs.howard.edu

***Chunmei Liu***
Systems and Computer Science Department
Howard University
chunmei@scs.howard.edu

***Abstract--*** Cloud service availability has been one of the major concerns of cloud service providers (CSP), while hosting different cloud based information technology services by managing different resources on the internet. The vulnerability of internet, the distribute nature of cloud computing, various security issues related to cloud computing service models, and cloud's main attributes contribute to its susceptibility of security threats associated with cloud service availability. One of the major sophisticated threats that happen to be very difficult and challenging to counter due to its distributed nature and resulted in cloud service disruption is Distributed Denial of Service (DDoS) attacks. Even though there are number of intrusion detection solutions proposed by different research groups, and cloud service providers (CSP) are currently using different detection solutions by promising that their product is well secured, there is no such a perfect solution that prevents the DDoS attack. The characteristics of DDoS attack, i.e., having different appearance with different scenarios, make it difficult to detect. This paper will review and analyze different existing DDoS detecting techniques against different parameters, discusses their advantage and disadvantages, and propose a hybrid statistical model that could significantly mitigate these attacks and be a better alternative solution for current detection problems.

***Key words: Cloud Security, Cloud Service Availability, Co-Variance Matrix, DDoS attacks, Entropy.***

## 1. Introduction

A Distributed Denial of Service (DDoS) attack is a distributed, coordinated attack on the availability of services of a host server (application server, storage, database Server, or DNS server) or network resource, launched indirectly through many compromised systems called botnets on the Internet.

Since its inception, distributed denial-of-service (DDoS) attacks have evolved over the years. As mentioned above, DDoS attacks have been a major challenge to the researchers and big security issue to the cloud computing environment. In modern very sophisticated approaches, by assuming multiple targets on the cloud resources, applications or network, hackers use multiple vectors and do not take any risk of missing their target cloud resources in a single attack campaign. DDoS attacks can range from simple network attacks to all cloud resources attacks. They can be volumetric, designed to disrupt a host service and make it unreachable, or attack application layers, targeting a specific service on the host. DDoS use of multiple botnet machines to amplify attacks could make it very challenging to stop it or to trace back the hackers [1].

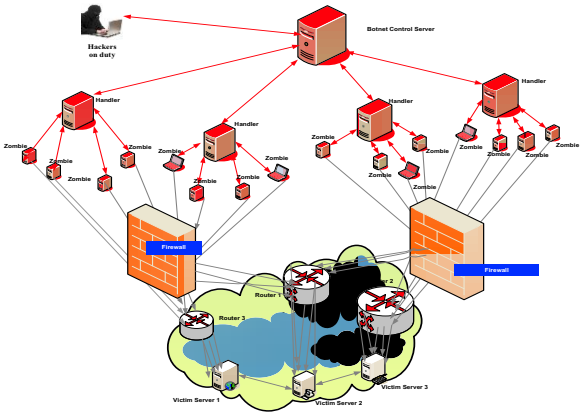



*Fig. 1 Typical DDoS attack organization*

## 2. Impacts of DDoS Attacks and Their Types

DDoS attacks have tremendous impacts on CSP's business. Such impact is different depends on the volume of resources hosted by the providers and the time it is affected by the service disruption. The more cloud service disrupted,

978-1-4799-8828-0/15 $31.00 © 2015 IEEE
DOI 10.1109/ITNG.2015.40

the higher will be the chance that customer attrition follows. If the customer pursue for any financial restitution, a legal suit will follow, which brings about more financial loss to the CSP and huge reputation loss. Hence, it is always important to prevent or mitigate DDoS attacks using all available means.

Resource and bandwidth depletion attacks are the two main types of DDoS attacks. Resource attacks target and flooded the targeted cloud resources so that the legitimate users could be denied access to it. The bandwidth attacks is targets and flooded the victim network resources with traffic coming from different attacking source systems called botnets that prevents the normal traffic from reaching the intended victim system[2]. Different types of DDoS attacks along with their types and behavior occurring in the cloud computing model are listed in [3]. Among these major types of DDoS attacks targeting applications includes DNS flood attacks, HTTP flood attacks, Low and Slow attacks, and HTTPS flood attacks.

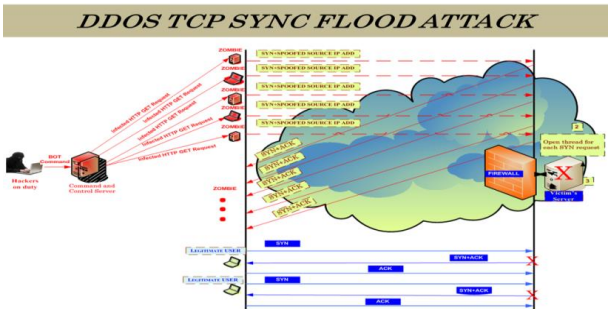



**Figure 2, Sample DDoS Flood attacks that target the network**

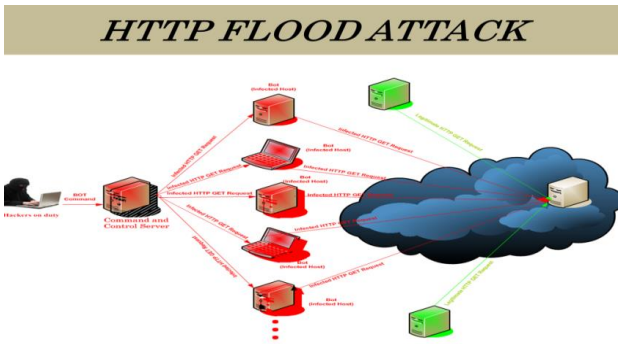



**Figure 3, Sample DDoS Flood attacks that target applications**

The other DDoS attacks that target the network include: UDP flood attacks, ICMP (Ping) attacks, TCP-SYN Flood attacks, TCP-PUSH-ACK attack TCP PSH+ACK Flood attacks. There are a wide variety of DDoS attack tools available today. Agent-Handler attacking tools [4, 5] and IRC-Based attacking tools [7, 8] are among them. The variant forms of DDoS attack tools like Agobot [9], Mstream [10] and Trinoo [11] are still used by attacker today. These tools are often taken by attackers and modified slightly so there are many derivative DDoS attacks that are created from earlier tools and the core technique.

## 3. Literature Review

Many researches have been conducted and as many number of different DDoS detection techniques have been proposed. Among these was a simple and efficient hidden markov model scheme for host based anomaly intrusion detection [12]. An entropy based anomaly detection system to prevent DDoS attacks in cloud was reviewed, explored, investigated and proposed as an alternative solution [13]. After investigating the correlativity changes of monitored network features during flood attacks, a covariance-Matrix modelling and detecting various flooding attacks was proposed [14].

An experimented result was also analyzed and presented to support a model that was instrumental to propose a model to detect flood based DoS attack in cloud environment. It provided research results that support how effectively the flood attacks are detected [15]. Researchers also discussed how entropy based collaborative detection of DDoS attacks on community networks could effectively works in theory by applying information theory parameter called entropy rate [16]. Different types of DDoS attacks at different layers of OSI model were discussed and presented, and finally, analyzed the impact of DDoS attacks on cloud environment [17]. The analysis of covariance model for DDoS Detection was discussed and the researchers described how the method can effectively differentiate the traffic between the normal and attack traffic. They also showed how the linear complexity of the method makes its real time detection practical [18].

Another detecting solution framework to predict multi-step attacks before they pose a serious security risk is by using hidden markov model. The study based the real time intrusion prediction on optimized alerts since alerts correlations play a critical role in prediction [19]. The design

of two independent architectures for HTTP and FTP which uses an extended hidden semi-markov model to describe the browsing habits of web searchers and detecting DDoS attacks were discussed and investigated [20]. A survey of different mechanism of DDoS attacks, its detection, and the various approaches to handle them was discussed and explored, to enable the clients review and understand those different parameters having impacts in their decision making process while selecting the right DDoS detecting scheme [21].

The scopes of DDoS flooding attack problems and attempts to combat them have been explored by categorizing the DDoS flooding attacks and classifying existing countermeasures based on different parameters [22]. A comprehensive survey presented DDoS attacks, detection methods, detection tools used in wired networks and internet, and future research direction [23]. The Security problem associated with cloud computing becomes more complex due to entering of new dimensions in problem scope related to its own main attributes. Researchers also proposed a detection scheme based on the information theory based metrics. The proposed scheme has two phases: Behavior monitoring and Detection. Based on the observation, Entropy of requests per session and the trust score for each user is calculated [24].

DDoS attacks could be detected using the application of Dempster Shafer Theory. The theory was applied to detect DDOS threat in cloud environment. It is an approach for combining evidence in attack conditions [6]. The effectiveness of an anomaly based detection and characterization system highly dependent on accuracy of threshold value setting. And this approach described a novel framework that deals with the detection pf variety of DDoS attacks [25]. Cloud specific Intrusion Detection System was proposed and described a defense mechanism against the DDoS attacks. This defense mechanism discusses how to detect the DDoS attack before it succeeds [26]. Effectively detecting the bandwidth limit of a cloud network and the bandwidth currently in use helps to know when a DDOS attacks begin [27]. An approach described based on fundamentals of information theory specifically Kolmogorov complexity to detecting distributed denial of service (DDoS) attacks was proposed. Despite its complexity the scheme enabled early detection [28].

## 4. Analysis of Existing System

Considering how hackers are using very sophisticated attacking tools and methods to intrude and disrupt systems, the road ahead for the next generation of intrusion detection system is very challenging and need a collective effort. Besides preventing these attacks, it should also be realized that any intended detection scheme should take into consideration of the advancement of the networking technology and major changes in systems like cloud computing environment. The main challenge in detecting such attacks efficiently is the reduction of the false alarm rate.

Different types of DDoS detection methods have been proposed based on different architectures namely, victim-end, source-end, and in-network [29]. These methods includes statistical methods, soft computing methods, knowledge based methods, and data mining and machine learning methods. While the important aspect of these detection schemes is to defend itself from attacks, those traditional intrusion detection systems have not adapted to new technological paradigms like mobile and wireless networks [22]. Different schemes have been used with these detection mechanisms. The following table discusses the advantages and disadvantages of different detection schemes.

## 5. Proposed System

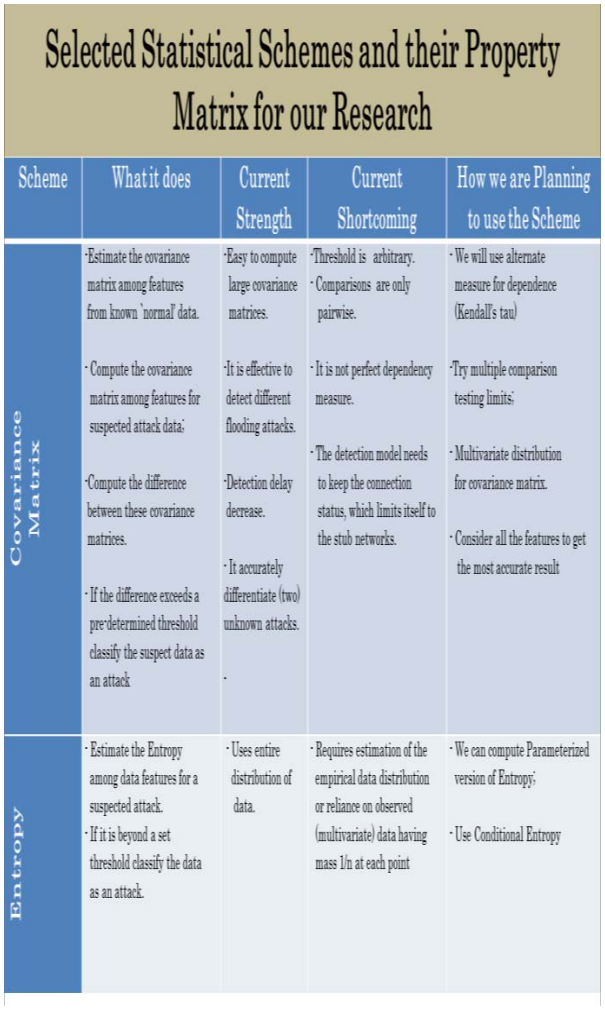
We propose a hybrid model by noticing that two approaches the covariance matrix based and the entropy based system – are heuristically similar in that both classify a DDoS attack via measuring heightened dependency in the data.

**Table.1 Existing detecting systems advantage and disadvantage**

*Existing Detection Schemes Advantages and Disadvantages*

| | Scheme | Advantage | Disadvantage |
|---|---|---|---|
| 1 | Hidden Semi Markov Model. [30] | It potentially detect application layer DDoS attacks by applying theory of information. | High complexity of its algorithm. |
| 2 | Entropy [14] | Accurate | Calculation merges decrease concentration [17] |
| 4 | Dempster Shafer Theory [31] | Accommodate uncertain states, reduce false negative rate, and increase detection rate.[6] | Computational complexity increase exponentially with the number of elements in the frame of discernment. |
| 4 | Aggregate congestion control (ACC) [32] | Limits the subsets of traffic defined by some characteristics such as destination or source IP address rather than IP sources. | It is not effective against uniformly distributed attack sources because of volumetric traffic. |
| 5 | Kolmogorov [28] Complexity Metrics | Does not require special filtering rules and easy to implement. | Needs other techniques to reduce its complexity. |
| 6 | Covariance Matrices (14) | Effective and very accurate , does not rely upon any presumptions on the normal network packets distributions. | Need to consider all the features to get the most accurate result. |
| 7 | D-WARD [33,34] | Detect DDoS flooding attack by monitoring the source traffic on bidirectional base. | It consume more resources, it does not protect the CSP network. |
| 8 | TOPS [35] | Provide an efficient method for detecting packet flow imbalances based on a hashing scheme. | High False negative rate. Attackers can increase the proportion of the traffic rates (from both directions) by downloading big files. |

**Table.2 Selected Statistical Schemes and Their Property Matrix**



Selected Statistical Schemes and their Property Matrix for our Research

| Scheme | What it does | Current Strength | Current Shortcoming | How we are Planning to use the Scheme |
|---|---|---|---|---|
| Covariance Matrix | ·Estimate the covariance matrix among features from known `normal' data.<br>· Compute the covariance matrix among features for suspected attack data;<br>·Compute the difference between these covariance matrices.<br>· If the difference exceeds a pre·determined threshold classify the suspect data as an attack | ·Easy to compute large covariance matrices.<br>·It is effective to detect different flooding attacks.<br>·Detection delay decrease.<br>· It accurately differentiate (two) unknown attacks. | ·Threshold is arbitrary.<br>· Comparisons are only pairwise.<br>· It is not perfect dependency measure.<br>· The detection model needs to keep the connection status, which limits itself to the stub networks. | · We will use alternate measure for dependence (Kendall's tau)<br>·Try multiple comparison testing limits;<br>· Multivariate distribution for covariance matrix.<br>· Consider all the features to get the most accurate result |
| Entropy | · Estimate the Entropy among data features for a suspected attack.<br>· If it is beyond a set threshold classify the data as an attack. | · Uses entire distribution of data. | · Requires estimation of the empirical data distribution or reliance on observed (multivariate) data having mass 1/n at each point | · We can compute Parameterized version of Entropy;<br>· Use Conditional Entropy |

## 5.1 Our Heuristic:

Let **X** be a *p x T* multivariate vector where *p* is number of network 'features' or variables and *T* is the number of (discrete time interval) observations. The basic idea is to identify the presence of atypical dependence in a sample after establishing baseline dependence. This then classifies an attack.

In statistical terms we evaluate the dependency among **X** for an ordinary, non-attack, regime - let's call it $T\_0=T(\mathbf{X})$, where *T* is some statistic of the multivariate data and **X** is the baseline or non-attack, training, data. Then the task is to evaluate the `distance', via this statistic, between the training data and `new' data; large values of this distance indicate an `attack'. In notation

## 5.2 Covariance Matrix approach:

Here, we take $T(\mathbf{X})$ as the covariance matrix $p < p^*$ network features. Most papers estimate this covariance matrix for *t* observations - i.e. the training portion - where no attacks are present. Then this matrix is compared with (sample) covariance matrices in times of suspected attacks. These comparisons involve imposing a difference threshold, beyond which the new covariance matrices The main paper we've read, the comparisons are element wise and a new 0-1 matrix is formed element by element.

## 5.3 Kendall's Tau approach:

We substitute Kendall's tau – a measure of probabilistic dependence in place of correlation which is a measure of linear dependence – for bivariate correlation and multiple correlations. In analogy with the covariance, the same thresholding, etc. can be done.

## 5.4 Entropic approach:

We can also use the entropy across all features of the data, in terms of the model: across the entire dimension of the multivariate vector. Here we look for a large distance between the baseline entropy and the entropy of the data (i.e. calculated across some time steps) as the signal for an attack – in the place of indexed dependence in the covariance and Kendall's tau matrices. In a sense, this method is more `complete': the mass from the entire probability distribution (via the model and estimator) is used and not just the expectation.

# 6. Conclusion

In this paper, we proposed an effective alternative hybrid scheme against DDoS attacks based on Entropy and Covariance Matrices. We are looking forward to apply a different approach with a comprehensive hybrid detection scheme at both the network and host level. Because, many of the available DDoS detection schemes performance found to be below the par and DDoS attacks are growing exponentially, it prompts the real need of having a comprehensive solution. We believe that this proposed scheme with double check points is expected to be a better alternative solution in mitigating the risk significantly by producing a better result.

## *7. Reference*


[1] An NTT Communications, “Successfully combating DDoS Attacks”, White Paper, August 2012

[2] Amit Khajuria1, Roshan Srivastava, “Analysis of the DDoS Defense Strategies in Cloud Computing”, international journal of enhanced research in management & computer applications vol. 2, issue 2, February 2013

[3] Radware Ltd, “The Ultimate Guide to Everything You Need To Know About DDoS Attacks”, 2013

[4] David Dittrich. “The “Stacheldraht” Distributed Denial of Service Attack Tool”. University of Washington, December 31, 1999, http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt (8 April 2003).

[5] Sven Dietrich, Neil Long, and David Dittrich, “Analyzing Distributed Denial of Service Tools: The Shaft Case”, USENIX Association, Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, Louisiana, 2000

[6] A.M. Lonea, D.E. Popescu, H. Tianfield, “Detecting DDoS Attacks in Cloud Computing Environment”, International Journal of Computing and communication, ISSN 1841-9836 8(1):70-78, February, 2013.

[7] CERT Coordination Center, Carnegie Mellon Software Engineering Institute, “CERT® Incident Note IN-2001-13”, November 27, 2001. http://www.cert.org/advisories/CA-2001-20.html. (14 March 2003).

[8] “CERT® Advisory CA-2001-20 Continuing Threats to Home Users”, CERT Coordination Center, Carnegie Mellon Software Engineering Institute. July 23, 2001. http://www.cert.org/advisories/CA-2001-20.html. (14 March 2003)

[9] F-Secure.F-SecureVirusDescriptions: Agobot. http://www.f-secure.com/v-descs/ agobot.shtmlS, 2003.

[10] Dittrich D. “The ‘‘mstream’’ distributed denial of service attack tool”, University of Washington, http://staff.washington.edu/dittrich/misc/mstream.analysis.txtS, 2000.

[11] Dittrich D. “The DoS Project’s ‘‘trinoo’’ distributed denial of service attack tool”, University of Washington, http://staff.washington.edu/dittrich/misc/trinoo.analysis, 1999

[12] Jiankun Hu, Xinghuo Yu, D. Qiu, Hsiao-Hwa Chen, “A Simple and Efficient Hidden Markov Model Scheme for Host-based Anomaly Intrusion Detection”, IEEE network, February 2009.

[13] A.S. Syed Navaz, V. Sangeetha, C. Prabhadevi, “Entropy Based Anomaly Detection System to Prevent DDoS Attacks in Cloud”, International journal of computer applications (0975-8887), January 2013.

[14] Daniel S. Yeung, Xizhao Wang, “Covariance-Matrix Modeling and detecting Various Flooding Attacks”, IEEE Transactions on Systems, MAN, Cybernetics- Part A: Systems and Humans, Vol. 37. No. 2, March 2007

[15] Mohd Nazir Ismail, Abdulaziz Aborujilah, Shahrulniza Musa, Aamir Shahzad, “Detecting Flooding based DoS attack in cloud computing environment using covariance matrix approach”, ICUIMC (IMCOM), 2013

[[16] Shui Yu and Wanlei Zhou, “Entropy-Based Collaborative detection of DDoS attacks on community networks”, Sixth annual IEEE international conference on pervasive computing and communications, 2008.

[17] J.J. Sha and L.G.Malik, “Impact of DDoS Attacks on Cloud Environment”, International Journal of Research in Computer and Communication Journal Vol2, issue 7, July 2013.

[18] Shuyan Jin and Daniel S. Yeung, “A Covariance Analysis Model for DDoS Attack Detection”, IEEE communications society, 2004.

[19] Alireza Shameli Sendi, Michael Dagenais, Masoume Jabbarifar, “Real time Intrusion prediction based on optimized alerts with hidden markov model”, Journal of networks, Vol 7, no.2, February 2012

[20] Sanjay B Ankali and D.V Ashoka, “Detection Architecture of Application Layer DDoS Attack for Internet”, Advanced Networking and Applications, volume 03, issue 01, Pages 984-990, 2011.

[21] Er. Sakshi Kakkar, Er. Dinesh Kumar, “A survey on distributed denial of services (DDoS)”, International journal of computer science and information technologies Vol. 5(3), 2014.

[22] Animesh Patcha, Jung-Min Park, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends", Science Direct, Computer Networks 51, 2007

[23] Monowar H. Bhuyan, H.J. Kashyap, D.K. Bhattacharyya, J. K. Kalita, "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions", http://www.garykessler.net/library/ddos.html, December 2012.

[24] S. Renuka Devi and P. Yogesh "Detection Of Application Layer DDoS Attacks Using Information Theory Based Metrics", CS & IT-CSCP pp. 217–223, 2012

[25] B.B. Gupta, Manoj Misra, and R.C. Joshi, "An ISP Level Solution to Combat DDoS Attacks Using Combined Statistical Based Approach", Journal of Assurance and Security, Volume 2, Pages 102-110, June 2008.

[26] Upma Goyal, Gayatri Bhatti, and Sandeep Mehmt, "A Dual Mechanism for Defeating DDoS Attacks in Cloud Computing Model", Vol. 2, Issue 3, March 2013.

[27] Biswajit Panda, Bharat Bhargava, Sourav Pati, Dayton Paul, Leszek T. Lilien, and Priyanka Meharia, "Monitoring and Managing Cloud Computing Security Using Denial of Service Bandwidth Allowance", 2012.

[28] A.B. Kulkarni, S.F.Bush, and S.C. Evans, "Detecting Distributed Denial-of-Service Attacks Using Kolmogorov Complexity Metrics", GE Research & Development Center, February 2002.

[29] Saman Taghavi Zargar, David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE communications surveys and tutorials, February 2013.

[30] Y. Xie, and S. Z. Yu, "A Large-scale Hidden Semi-Markov Model for Anomaly Detection on user Browsing Behaviors", IEEE/ACM Transactions on Networking (TON), Vol. 17, no. 1, pp. 54-65, February 2009.

[31] A.M. Lonea, Daniel Elena Popescu, Huaglory Tianfield, "Detecting DDoS attacks in cloud computing environment", International Journal of Computer communication, ISSN 1841-9836, 8(1):70-78, February, 2013.

[32] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network", presented at Computer Communication Review, pp.62-73, 2002.

[33] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the Source", In Proc. of the 10th IEEE International Conference on Network Protocols (ICNP '02), Washington DC, USA, 2002.

[34] J. Mirkovic, G. Prier, and P. Reihe, "Source-End DDoS Defense", In Proc. of 2nd IEEE International Symposium on Network Computing and Applications, April 2003.

[35] S. Abdelsayed, D. Glimsholt, C. Leckie, S. Ryan, and S. Shami, "An Efficient Filter for Denial-of-Service Bandwidth Attacks", Proc. of the 46th IEEE Global Telecommunications Conference (GLOBECOM03), pp. 1353-1357, 2003.