International Journal of Advanced Computer Research
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
Volume-5 Issue-19 June-2015

Dynamic Security Architecture among E-Commerce Websites

Ramesh R*and Divya G
Assistant Professor, Adi Shankara Institute of Engineering and Technology, Kerala, India

Received: 04-April-2015; Revised: 28-May-2015; Accepted: 03-June-2015

Abstract

Nowadays privileged channel is utilized by the ISPs and other websites for handling privilege services of important clients only, there by normal clients are discriminated against getting access to privilege channel service. Thus a new global movement known as "Net Neutrality" for providing an open and non-discriminating Internet is fast popularizing in India, Europe and other parts of the world. We are proposing a system among E-Commerce websites so that without much difficulty even normal clients are able to access a particular destination website through a source website using privilege channel network without any hindrance from the ISP and also provides a security protocol for safer referrals. The existing system of security protocols doesn't allow the e-commerce websites to come forward for making the referral service an option for business opportunity. They are reluctant to initiate site-to-site referral due to security risks and other opportunities they need to sacrifice. The proposed system using site graph shows how mutually trusted web servers can effectively implement a secure referral system by coordinating the traffic flow of referred clients. DDoS attacks and Phishing attacks focused on a particular website can be effectively averted by this coordinated security protocol among e-commerce web servers.

Keywords

Denial of service; referral; e-commerce; website graph.

1. Introduction

Nowadays networks and websites are vulnerable to Distributed Denial-of-Service (DDoS) [2] attacks if necessary security is not enforced in a particular website. DDoS attacks are hard to prevent even when necessary security protocols and firewalls are implemented in the local network that is connected to Internet. Attacks originating from local organizations using service of an ISP are a big concern for internet service providers who often finds themselves in either notifying the respective organization under attack for unwanted packet generation or disconnect the service and take necessary actions.

In recent years e-Commerce business is booming in India with millions of dollars of funds are invested from both India as well as from abroad. Due to the absence of referral system among these e-commerce websites they are losing valuable business opportunity. Referring a person to another person shows the kind of importance or trust upon the referred client. Similarly e-commerce websites can refer clients to another website there by acquiring small business points. In the absence of such a referral system, clients who got disappointed in not finding a product from their popular websites, they go and visit other websites which in turn increases popularity of other websites. So from business point of view, if big e-commerce websites (Flipkart, Snapdeal, etc.) refer clients to smaller websites and vice-versa, like minded or trusted e-commerce websites (Domestic) can increase their foothold in the e-commerce business by forming a consortium against stronger competition from popular websites notably from global e-commerce giants like Amazon, e-Bay etc.

Web Referral Architecture for Privilege service, WRAPS [4], technique helps to augment the security of websites while handling privilege services like payment processing. It uses a partially encrypted Uniform Resource Locator (URL) for providing privilege clients the privilege service even during DDoS attack on a particular destination server. Persistent referral system architecture [1] offers a solution for providing privilege service to normal

*Author for correspondence

clients by calculating importance or privilege level of each client in need of privilege service to other websites. For that the user in need should enable this service in his/her account settings. The enabled PRS system automatically calculates the privilege level of clients and uses that value for obtaining a referral channel to his/her intended destination websites which are registered to his/her source website. So PRS system can be implemented among the e-commerce websites for referral service and normal clients can get a feel of privilege channel service to other websites.

In this paper, we are proposing a system in which the existing reliability of popular e-Commerce websites such as Flip Kart, Snap Deal etc. can be utilized for providing value-added service to other smaller websites. The referral service could be employed from one e-commerce website (source) to another e-commerce website (destination) provided they form a trusted Site-Graph [1] in a transitive model. That is, the referred client should be a member of both source and destination websites.

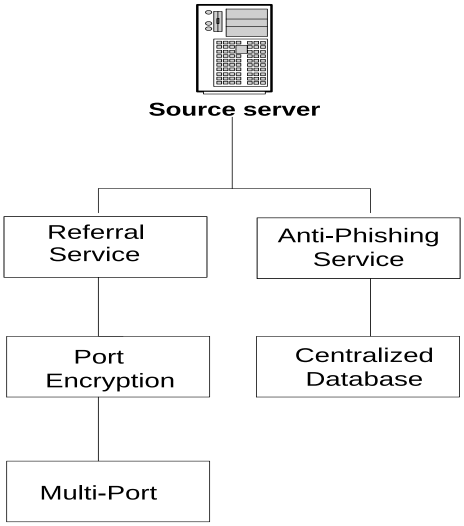

Figure 1: Proposed dual service using PRS

The proposed system along with offering clients (both privileged and normal) privilege channel service (to destination servers from source servers), it can also be used for creating an anti-phishing mechanism at the source servers. For the second technique to become operational we need to design a centralized database system at websites offering referral service. Nowadays the bulk of the anti-phishing mechanism works are shifted towards web browsers. Web browsers integrated with anti-phishing toolbars can provide the users the real domain name if they try to visit malicious websites posing as legitimate website. Web browsers need to enable this service prior to checking the URLs for phishing attacks. There are several approaches to prevent phishing attacks. The main function of anti-phishing mechanism is to avert phishing attempts and to notify the clients. Some of the client-side anti-phishing tools are Quick Heal, McAfee Site Advisor, and Phish Tank Site Checker etc.

Phishing attacks varies from low risk attacks like diverting a user to a malicious website to high risk attacks like masquerading an user to a malicious website which poses to be his/her bank prompting for authentication details. So online banking systems are the most concerned about such attacks in the internet.

2. Related Works

All anti phishing software [5], [9] is made up of computer programs which will attempt to identify the phishing content that may be contained in a website or email that has been sent to you. This software is normally to be found as an integrated tool within web browsers and email servers and will display the real name of the domain for the website that you are visiting. In doing this it is hoped it will prevent sites which are fraudulent from being able to masquerade as ones that are actually legitimate. Today such a function may well be included as a built in feature of a lot of web browsers.

If you are looking for a web browser which has anti phishing software as an integral tool within its system then you should look at installing such ones as follows:

1. Microsoft Windows Internet Explorer v 7.
2. Firefox v 2.0.0.4.
3. Google Safe Browsing (which can be used with Firefox).

All of these are highly effective in helping to prevent you from becoming another victim of this latest trend in people obtaining your personal information fraudulently to then use it for criminal purposes.

However if you are looking for a software program that is completely free but acts like a firewall for websites and will help to protect you from any kind of online attack then you may want to consider downloading Fraud Eliminator. This software has been developed in order to provide you with comprehensive protection while you are using the internet in your home from any kind of online fraud scheme or phishing attack.

This particular anti phishing software package when downloaded installs a toolbar that then protects you by automatically identifying and blocking anything that is considered to be online fraud. Also it provides you with the chance to fight back against what has occurred by allowing you to report the incident to company who developed the software at their central database. But not only is it helping to protect you from fraud schemes and phishing attacks, you will find that it comes with other toolbar functions that we all require today. These include capabilities to search for information as well as a protection system to protect the user against pop ups which they can configure to their own particular requirements. However the biggest advantage to this particular software package compared to all the others on the market today is that this one will actually identify the country where every website that you look at has originated from. When browsing the net it compares each website that you view against their list of URLs which might be either phishing websites or sites which have been hacked. Plus each hour you will discover that the software contacts the company's main database in order to update the blocked list so you know that you are constantly being protected against any possible scams in the future. Thus you have several different anti phishing software programs to choose from.

However there are several anti-phishing tools a person can now use in order to help prevent such attacks from occurring in the future. Below we will be taking a closer look at just what some of these are.

1. **PhishTank SiteChecker:** This tool blocks any phishing websites whose details are held by the PhishTank Community. Should you unexpectedly visit a website that is known to PhishTank then the SiteChecker displays a page stating that this site has been blocked rather than actually displaying it. This anti phishing tool can easily be downloaded on to your PC.
2. **Google Safe Browsing:** This tool will alert the user when the page that they are visiting is requesting personal or financial information under what it considers to be false pretenses. It uses a combination of advanced algorithms as well as reports that have been provided to it regarding pages which are misleading and will usually be able to inform the user automatically that they have gained access to a site which is trying to gain their personal or financial information in a fraudulent way. Again this particular tool can be downloaded directly from the internet on to your PC.
3. **WOT:** This particular tool allows the user to ensure that they steer well clear of fraudulent and phishing websites by letting you see what the reputation of the website is like through your browser. By being able to see what kind of reputation a site has, a person is then better able to distinguish a legitimate site from one which is phishing. All the testimonies that are contained within this site have been provided by people who have become part of the WOT community and are looking for ways to prevent other people from becoming victims of those sites that perpetrate such scams. All throughout the paper, target or destination server means the website to which the clients are referred to and source server means the website that offers the anti-phishing service or referral service.

The familiar method for preventing suspected DDoS attack is to enforce a simple CAPTCHA test [8] at the entry point of websites or during authentication. There are wide ranging methods for web server protection like Overlay node method [12], [13], [14], Secure overlay architecture [6], Capability Token technique [7] and [11], WRAPS [4] and [15] etc. In the overlay node based approach special purpose routers know as overlay nodes will get activated whenever there is a suspicious DDoS attack attempt. These nodes form an alternative path from source routers to target or edge routers, there by diverting the packet flow from authentic users to their intended destinations. The overlay based approach requires the need for installing special purpose routers for taking suitable actions, so it relies on router based protection system. In another approach, target servers can involve in security protection perimeter in taking vital decisions to prevent attacks by offering reliable authentic clients capability tokens. But this technique is prone to single point of failure, making the authentic clients from not getting the tokens itself.

In Web referral architecture for privilege service mechanism, the privilege clients are given privilege channel access by providing a fictitious URL containing capability token. This token performs periodic refresh so that it can protect against brute force attacks and against malicious attackers possessing this fictitious URL. This approach provides a strong security protocol there by a privileged user is provided with fool proof security service for acquiring a privilege channel access to target server. Target servers may provide banking services or other value-added services. In part III, proposed system and its implementations are discussed. The section IV to section VII covers the results evaluation, limitations and future works that are possible by the extension of the proposed system.

3. Design

The only requirement is that you need to know at least one website's address in the corresponding web graph where your target website belongs. The below shown architecture shows the fundamental architecture for the proposed referral system where you can avoid phishing attacks, DNS based IP spoofing attacks while using referral service. It's a coordinated architecture among websites but it doesn't imply an alternative to already existing Hypertext Transfer Protocol Secure (HTTPS) for secure transmission.

As we all know, today's E-commerce websites are reluctant to offer web referral service due to the lack of a security protocol among the web servers that are willing to offer so. The proposed paper is well focused on the need for establishing a secure security protocol that not only takes care of privileged client access control but also provides a chance to those needy normal clients who wishes to get referred from a source website to a destination website. E-commerce web services offer product purchase at concession rate. Nowadays, source web servers are not having the provision for referring clients in a normal fashion other than existing system based on web referral architecture based on referral service only during privilege service access. The need for referred purchase is ever-increasing since the launch of e-commerce websites. The launch of payment services like cash-on-delivery (COD) service in India made website like FlipKart.com, Snapdeal very popular. The Income-tax department of India recently enforced taxes for online purchases as it starts growing from a miniature service to virtually offering all items purchased through a global network of retailers, which itself shows the increasing trend in usage of e-commerce websites for purchasing. Website graph gives an idea of how websites are connected with each other, who belongs to the upper hierarchy and who belongs to lower site rank [3].

Much to the surprise of web site graph, it is possible to show that the members belonging to a path of trusted neighbours, can be protected against distributed denial-of-service attacks with the help of a web security architecture so naïve and secure enough, which offers alternative path during DDoS attacks from source server to a particular destination server.

Destination servers are either important servers who offer vital services like banking, mobile recharging, bill payments etc. or other e-commerce websites which are ready to provide other source servers some value added service for the clients been referred. Source servers are servers which are either small websites may be recently launched or other e-commerce websites which are ready to refer its clients to a destination website, which in turn provides referred clients product they want in a concession rate. Concession rates and other value added services like number of clicks made by clients to destination websites are taken into consideration for evaluating reputations of source servers. Destination web servers offer the referred clients from source servers to purchase products at a concession rate. Thereby not only destination servers get some profit, source servers are also been given some value added points in return for their service of referral and number of clicks made.

Another important thing about referral is that the smaller websites or other unimportant websites are given a chance to improve their site rank [3]. Google's search engine works on the principle of page rank. Page rank basically improves when an unimportant website got a link directed from an important website.

In the proposed paper, an automated tool called Persistent Referral Service, ***PRS***[1],[10],will be running automatically checking and updating each and every clients priority level by evaluating his/her behaviour in that particular website. This priority level can be represented in 2 bits, and can be used either at network layer or at application layer. At network layer, priority level, **pr**, can be used for scheduling the packets at any of the terminal or edge routers. And at the application layer, **pr** can be utilized for managing client specific services. The referral protocol handles client's service from source to destination website. When source server refers its clients, it must inform the destination server the priority of the client been referred. PRS performs this operation. The security mechanism is in need of an edge router in the case of WRAPS [4].

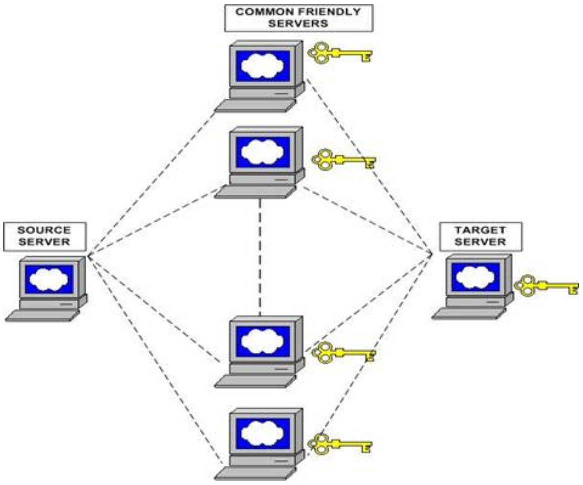

Figure 2: Proposed Architecture

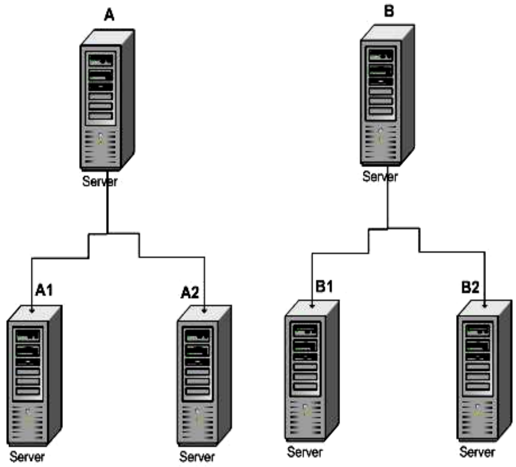

Figure 3: Server Hierarchy for proposed system

The proposed system consists of 3 main entities: source servers, destination servers and common friendly web servers called third party servers. As discussed in section I, source servers' main purpose is to refer clients along with security parameters and priority. Destination servers provides referred clients the needed services, it could be banking service, e-commerce service, normal services or other value-added services. The main prerequisite for choosing a third party server is that it should be trusted by both source server as well as destination server. Existing methodologies rely either upon destination oriented [17], [18], [19] or router oriented [16],[20] security systems for traffic flow controlling. Source servers are not part of the security mechanisms that has been used nowadays. Also such destination oriented and router oriented security mechanisms focused on handling important traffic flows which means normal clients been left with no option for getting such privilege channel access.

Consider a scenario where a potential buyer visits an e-commerce website and couldn't find his/her product there. He will certainly visit other popular websites known or else visit Google for searching and eventually he will be directed to necessary website which is having the required product ready to be delivered to his/her home. So the potential buyers will buy their product at all cost whenever they needed one. Imagine a situation where a product is not available in one website, called www.pdtbuy.com so the potential client visits other websites. What if the first website he visited www.pdtbuy.com, refers the client to another website called destination website where he can buy the product also in concession rate. Website www.pdtbuy.com is not only referring clients to destination website but also providing some value-added services to the respective destination website by referring potential buyers. By this way source websites like the one mentioned as example www.pdtbuy.com will get some reputation points.

The existing website to website relationship to some extent is limited to services like payments, software downloads etc. E-commerce websites are not prepared for such referral service mentioned in above scenario as destination websites may not trust source servers, or there is no credible security protocol among e-commerce websites for doing so.

The proposed system offers a secure solution for e-commerce websites for performing referral service. Figure 2 shows the architecture been used for evaluating the proposed setup.

4. Architectural Evaluation and Results

Figure 2 shows how the traffic flows in the proposed architecture from source to destination websites through third party server [10]. The operation starts with the registration of source websites with respective destination website. In figure 3, A and B are 2 top level domains. A1, A2 are 2 low level domains of A and B1, B2 are 2 low level domains of B. The system developed can be implemented in each website of a particular path of a tree in sitegraph and each node within this path can be selected as a common friendly server between any 2 nodes on the path from root to leaf node of the sitegraph. The only precondition should be that the path must contain minimum 3 nodes. Usage of separately built sitegraph, which shows friendly web-tree relationship among e-commerce websites, is best suited as we can easily obtain the trusted web server for implementing the security protocol. This security protocol can be implemented in transitive nature there by the security perimeter can be enlarged preventing more websites from attacks.

Destination websites will provide security parameters containing encrypted tokens [11], source identifiers, destination identifiers, and the URL of third party server. The destination ID is source website specific, so changes from one source to another. URL of third party is agreed upon by the respective source and destination web servers for providing redirection operations. The source website specific tokens' decryption key details and encryption algorithm are shared with third party only. So once source website starts referring a client, using PRS it calculates the privilege level of client, then in the referral request source will be sending the security parameters to third party server. Only the third party web server knew about the actual URL of destination website through which the respective source e-commerce website are given agreed privilege services by destination website. So the destination e–commerce websites have the choice of providing source e-commerce sites specific offers or concessions for referred clients. And this concession may or may not be provided for normal clients visiting destination web server. The implemented proposed system took the inspiration from capabilities based approach [7], [11] and WRAPS [4] methods for its final design architecture.

The encryption-decryption algorithm is agreed upon by the respective destination and third party servers for the proposed system. The destination web servers can utilize stronger encryption techniques based on the trust level with corresponding third party server. The privilege level can be utilized for traffic engineering techniques both at application layer for session creation and at network layer for scheduling traffic flows.

Discussions:

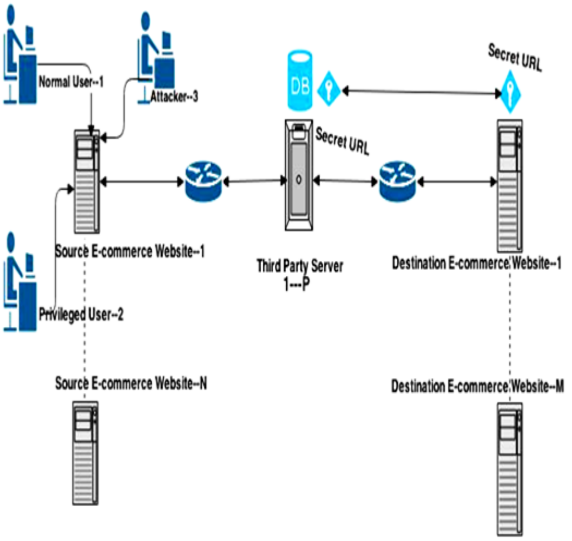
Normal User--1
Attacker--3
DB
Secret URL
Secret URL
Source E-commerce Website--1
Third Party Server 1---P
Destination E-commerce Website--1
Privileged User--2
Source E-commerce Website--N
Destination E-commerce Website--M

Figure 4: Overall Architecture Working

Figure 4 shows the working of the proposed system. In the figure there is 'N' number of source websites, 'M' number of destination websites and 'P' is the maximum number of third party web servers. Source e-Commerce websites and destination e-Commerce websites enter into a contract for providing a two way referral service. The respective third party server selected needs to be agreed upon by both source and destination websites.

The value of P=Max {M-1, N-1, M+N-2}, where

N-1 means there is only one unique destination website and there are N source websites and third party server may be any one of the N-1 source websites;

M-1 means there is only one unique source website and there are M destinations websites and third party server may be any one of the M-1 destination websites;

M+N-2 means there are M unique destination websites; N unique source websites and third party server will be any one among the M+N-2 websites (1 source website and 1 destination website).

Initially source e-Commerce website and destination e-Commerce register with each other. Destination websites may be other source e-commerce websites or other popular e-Commerce website. After registration source website will get security parameters and an encrypted token from the respective destination website for accessing the third party server during referral service access. Meantime the respective third party server will get the secret URL and the decryption key required to check the encrypted token of source website. The secret URL, the decryption key, source ID and destination ID will be different for each unique source-destination pair. So the secret URL of a particular destination website given to a third party server for providing privilege service will be different depending upon the source website or may be changed according to the third party server selected. So after completing the verification of security parameters of the source website and the tokens, the secret URL will be provided to the source website. So the normal clients having an account in both source website and the desired destination website will get privilege channel service without discrimination from privileged or important users.

5. Limitations

The PRS system should be manually enabled in the user's source website. And for users who don't prefer referral service even if this service is enabled provides no useful function. Then the concern that users must have accounts in both the source and destination websites can be sorted out by utilizing authentication service from source websites in destination websites and getting the privilege points. And the effectiveness of the overall security system depends on the security policy of the individual source websites itself.

6. Conclusion

The proposed system clearly shows that there is immense potential that needs to be tapped from the referral system among trusted websites or among common segment websites. The basic requirement for having an account in any of the website for a user increases the authenticity during referral and also pin points the attacker in case of any misbehaviour. The referral importance of the clients been referred is predicted based upon the user's social behaviour in the respective website where the user has a registered account. By the implementation of this system in the existing E-commerce websites, clients are able use privilege channel access to their desired destination websites. Also to some extent phishing threats can be averted if website graph is used for accessing unknown or malicious websites.

7. Future Works

"Net Neutrality" is a new buzzword in social media created as a result of an uproar against the decisions of the ISPs especially Mobile service providers for charging application specific usage over Internet while using free Internet-based calls and messaging services. Lots of debate is going on in this regard for an open and non-discriminatory Internet. The proposed methodology can be utilized among E-commerce or other likeminded service websites for offering privilege services for normal clients.

Acknowledgment

The authors thank the HOD-CS, ASIET, Kalady for providing valuable guidelines and resources required for the implementation phase and helping in conducting experiments.

References

[1] Ramesh.R, Pankaj Kumar G," Persistent Referral Service for Mitigating DDos Attacks using Search Engines: PRS", Appeared in Proc. of Int. Conf. Information Security, 2011.

[2] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki "Distributed Denial of Service Attacks", The Internet Protocol Journal, National Technical University of Athens, Cisco Systems Inc, Volume 7, Number 4, December 2004.

[3] Wu, Jie, and Karl Aberer. Using siterank for p2p web retrieval. No. LSIR-REPORT-2004-011. 2004.

[4] X. Wang and M. Reiter, "Wraps: Denial-of-Service Defence through Web Referrals,"Proc. 25th IEEES ymp. Reliable Distributed Systems (SRDS), 2006.

[5] Anti-Phishing Working Group, "Phishing Activity Trends Report, 1st Half 2009".http://www.apwg.org/reports/apwg_report_h1_2009.pdf.

[6] A. Keromytis, V. Misra, and D. Rubenstein, "SOS: Secure Overlay Services," Proc. ACM SIGCOMM '02, Aug. 2002.

[7] T.Anderson, T.Roscoe, and D.Wetherall, “Preventin Internet Denial-of-Service with Capabilities,”Proc. Second Workshop Hot Topics in Networks (HotNets’03), Nov.2003.

[8] Von Ahn, Luis, et al. "CAPTCHA: Using hard AI problems for security." Advances in Cryptology—EUROCRYPT 2003. Springer Berlin Heidelberg, 2003. 294-311.

[9] Chou, N., R. Ledesma, Y. Teraguchi, D. Boneh, and J.C.Mitchell, "Client-Side Defence against Web-Based Identity Theft". In Proceedings of 11th Annual Network and Distributed System Security Symposium (NDSS '04), 2004.

[10] Ramesh. R, Resmi Cherian “Unified Protection System to avert DDoS and Phishing Attacks using Persistent Referral Service”, Appeared in Proc. of Int. Seminar on Wireless Communication, Mobile computing and Emerging technologies (WICOMET), Sep. 2011 .

[11] Yaar, Avi, Adrian Perrig, and Dawn Song. "An endhost capability mechanism to mitigate DDoS flooding attacks." Proceedings of the IEEE Symposium on Security and Privacy, 2004.

[12] R. Stone, “An IP Overlay Network for Tracking Dos Floods,” Proc. USENIX Security Symposium, 2000.

[13] M.Waldvogel and R.Rinaldi, “Efficient Topology-Aware Overlay Network,” Proc. First Workshop Hot Topics in Networks (HotNets ’02), Oct. 2002.

[14] Han, Junghee, David Watson, and Farnani Jahanian. "Topology aware overlay networks." INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. Vol. 4. IEEE, 2005.

[15] Yang, Xiaowei, David Wetherall, and Thomas Anderson. “A DoS-limiting network architecture." ACM SIGCOMM Computer Communication Review. Vol. 35. No. 4. ACM, 2005.

[16] Yaar, Abraham, Adrian Perrig, and Dawn Song. "Pi: A path identification mechanism to defend against DDoS attacks." Security and Privacy, 2003. Proceedings. 2003 Symposium on. IEEE, 2003.

[17] H. Burch and B. Cheswick, “Tracing Anonymous Packets to Their Approximate Source,” Proc. 14th USENIX System Administration Conf., Dec. 1999.

[18] Savage, Stefan, et al. "Network support for IP trace back." IEEE/ACM Transactions on Networking (TON) 9.3 (2001): 226-237.

[19] D.Song and A.Perrig, “Advanced and Authenticated Marking Schemes for IP Trace back,” Proc. IEEE INFOCOM ’01, Apr. 2001.

[20] Jin, Cheng, Haining Wang, and Kang G. Shin. "Hop-count filtering: an effective defense against spoofed DDoS traffic." Proceedings of the 10th ACM conference on Computer and communications security. ACM, 2003.

Ramesh R received B.Tech Degree from Mahatma Gandhi University in 2010 and M.Tech in computer science and engineering from M.G.University. Currently working as Assistant professor at Adi Shankara Institute of Enginerring & Technology.
Email: Ramesh1986ktm@gmail.com

Divya G received B.Tech Degree from Mahatma Gandhi University in 2006 and M.Tech in computer science and engineering from Kerala University. Currently working as Assistant professor at Adi Shankara Institute of Enginerring & Technology.