International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

EShield: An Effective Detection and Mitigation of Flooding in DDoS Attacks over Large Scale Networks

J. Daniel Francis Selvaraj, I. Diana Jeba Jingle, P. Mano Paul,

Abstract: ***Distributed Denial-of-Service attacks are very hard to be mitigated in wireless network environment. Here in this manuscript, an effective method of flood detection and mitigation architecture is proposed named eShield, which detects and prevent flooding attacks through spoof detection technique. The proposed method uses an architecture and an algorithm. eShield deals with Intrusion Protection and Detection Systems (IPDS) which collaboratively defend flooding attacks at different points in the network. Here eShield detects the supply node with its port variety which were below assault. Inorder to reduce the burden on international IPDS eShield makes use of distinct nearby IPDS for the assaults in flooding which have been carried out collaboratively. The assessment is done through the widespread simulation of eShield and it is proved to be an actual values based on time delay, false positive rates, computation and communication overhead.***

Index Terms: Flooding, Router, Gateway, Bandwidth

I. INTRODUCTION

Internet is the one where we will transfer all resources through networks while communication. Here the transfer of information has been done with any host by interchanging packets. However attackers can take advantage to mitigate internet service by flooding of information as excess amount to server by forming DoS attacks. The attackers use many zombie machines to overflow messages at the same time which forms distributed DoS attack. Amey et al.[1] DDoS attack release the load by bringing the entire network down. To avoid such situation through this paper we focus the detection and prevention mechanism of DDoS attacks which will be worked over malicious code in Large Scale Networks[23][24] .

In this paper a methodology called eShield is proposed to formulate mitigation attacks of IDPS which detects and prevent flooding DDoS attacks at networks level and prevents flooding attacks against clever spoofs. eShield comprises two level architecture in distributed environment with a local group of IPDS at network level & gateway IPDS at ISP level. In this the working for these IPDS involve in guarding network collaboratively over DDoS attacks. This paper proceeds the following section where II defines the related works by summarizes the section. Section III describes the architecture of eShield and its operation. This describes the detection and mitigation algorithm. Section IV deals on its Performance metrics and its simulation metrics to evaluate collaborative eShield algorithm. Section V describes the eShield detection and mitigation algorithm. Finally section V concludes the prevention of DDoS attacks.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)
J. Daniel Francis Selvaraj, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India.
I. Diana Jeba Jingle, Department of CSE, Christ University, Bengaluru, India.
P. Mano Paul, Department of CSE, Presidency University, Bengalurur, India.

II. RELATED WORKS

Denial of Service (DoS) is a powerful attack which makes a network system more advanced and make the system to downgrade its performance. This can be done by professional hackers or attackers while transferring money and stoppage of other benefits. This sample survey deals for providing possible solution of proposed problems and produce feasible analysis of those approaches during examination. A desirable solution to prevent DoS compared to the existing system is given in this manuscript. Fircol[21] is an Intrusion Prevention System which forms a ring for protection around hosts by exchanging traffic information against flooding attacks to defend collaboratively. In firecol we cannot reveal port number which is under attack. In DoS[7] we checked it is more based on IP spoofing. So specific verification of IP spoof may add to solve the DoS related problems. Another way for preventing IP spoof will be done by the filters called ingress and egress filters which will activated over firewall. When original packets have some incorrect address information arranged in topological wireless network this firecol fails. SACK[22] detects flooding SYN attacks against spoof. This done by verifying TCP port and victim server being attacked by exploiting SYN/ACK-CliACK pair.

SACK limitation may identify only flood SYN attacks against reputed spoof. However we can detect by verifying FPR and FNR as given as a detection of short delay. TVA[17] uses to control traffic flood which is unauthorized and discard those through single autonomous system. This attains better output and the problems of TVA is it will store all capability of information shared on individual user on router and these router with some queues which cannot be protected all original users. DWARD[9] identifies and filter traffic attacks independently by formulating a drop of excess traffic by suppressing traffic rate in bidirectional ways from the target by reducing the load in the victim node.

On the other hand this DWARD does not detect until all connection temporary storage fills and it deals with increased time delay and causes more communication overhead.

DARB[20] methodology uses active method for the detection using probing method and these TTL based detection deals on its rate-limit which counteraction to filter flooding SYN attacks independently. This consumes more bandwidth, computation power in overhead while detection and counteraction methods autonomously. A priority based mechanism which is used for blocking attacks has been proposed by Ge Zhang et al [5] on SIP proxies which causes external process with time delay and lower it throughout when interact with servers which has been verified externally. Haidar Safa et al. [6] proposes a methodology called CDMS which is implemented over edge routers of spoofed attacks to prevent the sufferer. CDMS[8] serves as a communication protocol which encourages collaboration between different network to prevent host from being attacked. This technique always focus on releasing the overhead at the router, which may cause time delay by filtering and detecting an attack.

Sudip Misra et al. [25] proposes DLSR method which might also use gaining knowledge of Automata(la) used to prevent the server being overloaded with illegal visitors from customers the concept of gaining knowledge of Automata (los angeles) and stops the server from overloaded with many number of illegitimate visitors from colliding and makes the server to feature its routine technique. The main limitation of DLSR is to validate user IP and spoofed IP address which causes more time delay while detecting and filtering an attack.

Patrick P.C. et al. [11] uses a statistical CUSUM method for perceiving signal attack over wireless networks in timely approach. This technique makes use of a web detection algorithm and does not come across site visitors assault that has a spoofed IP cope with and signal load at the manage plane. This approach blocks unique or benign and also malicious site visitors whilst it reaches its threshold.

Supranamaya Ranjan et al.[15] proposes a Distributed approach to detect and prevent packets from being attacks that devastate the resources of system such as bandwidth. DDoS approach[]2 such as by providing a disbelief assignment that belonging all session of TCP, UDP, ICMP and assign doubtful values and decide which session has to be forwarded and when. Here the conceptual scheduler improves by performing rate-limiting by overwhelming limited memory over the request and response of memory buffer. Here DDoS approach consumes more processing time by lowering its throughput. Joseph Chee Ming Teo et al [10][14][18] proposes to protect heterogeneous network and produces a group key agreement protocol against DoS attacks. This causes greater communication overhead in different networks. Wei Chen et al [16] proposes data structure which summarizes a storage-efficient and change-point discovery approach to categorize three-way TCP handshake method as a confirmation from incomplete ones. This leads to large memory comsumption over communication approaches. Sungwon Yi et al [12] introduces Content Addressable Memory (CAM) which has been executed with two level cache to detect dynamically and isolate the unresponsive TCP data flows. But it leads to large memory consumption with quick access. Dimitris Geneiata et al. [3] proposes a monitor to detect and filter flooding attacks over proxy attacks which is formulated through a filter based approach. The monitor's is to record the part bloom filter over any state of incoming session in three altered filters and this also been indexed using hash function. The filter used here creates an alarming system to trigger an event and report if any entries in the filter increase more than the threshold limit to its appropriate level. In Diana et.al. [18] an efficient way of reducing time delay and cost effective metric is proposed to detect an attack. However, hashing leads to computational overhead and CPU utilization of filters. Dimitris Geneiatakis et al [3] approach proposes by succeeding a signaling attack over SIP servers using a new header and this mechanism uses new pre-shared key which were leads to the attacks in password metrics and it will be vulnerable to basic attacks.

III. ESHIELD ARCHITECTURE

A. The eShield System

The *eShield* system (Figure. 1) maintains a IPDS group locally and that was installed over the routers in local networks and also in a single global IPDS that was installed in gateway router over the networks. Each *eShield* used in IPDS will analyzes the congestion within its range over detection window. A*dmission controller* in eShield architecture accepts the right node only if it passes the registering process. The nodes may initially have to register with its network using its IP address, MAC address, time of registration. At the end of registration procedures, the gateway IPDS informs the node about its total allowed bandwidth consumption, N and TTL. The *admission controller* checks for bandwidth abnormality and accepts the right node and forwards them to the *timer manager*. By means of a schedule, the *timer manager* will sent the data periodically by each node and maintains the values which is being sent. Those values in clock then compared and additionally matched its similarity index with its threshold fee. The nodes that matches prevailing threshold gained and then can be forward to visitor surfer for examining community with their traffic difficulties. Ultimately, admission controller, timer supervisor and the visitor surfer informs the mitigation manager focus their statement in abnormalities of every node, clock fee and the visitors. By the obtained values *mitigation manager* decides the traffic in the network to be blocked/continued. Meanwhile the overall traffic cannot be observed properly we promote the procedure to multiple components which used in effective detection and filtering mechanism to prevent attacks.

B. eShield Components

The *eShield* approach is comprised of several IPDS with the following collaborative components.

1) The *admission controller* checks whether the nodes follow the allotted channel bandwidth correctly. This checking corresponds to check if $k(b_i, b_i') \leq \varpi$ where b_i is the fraction of bandwidth allowed to a node and b_i' is the deviation from b_i.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Failing node to use b_i which has been deviated to b_i'. The deviation of b_i, b_i' must not exceed ϖ . i.e., if $k(b_i, b_i') \leq \varpi$ then the node is under normal state. If $k(b_i, b_i') > \varpi$ then the node is under attack state.

2) The *timer manager* is responsible for maintaining the clock value. If the clock values match the threshold, then the node is under normal state. Otherwise, the node is under abnormal state.

3) The *traffic surfer* calculates the TCP flow metric and identifies the abnormal flow and the corresponding port.

4) The *mitigation manager* checks the reports being sent by the other three components and decides to accept or to reject the node based on the level of attack. The mitigation manager coordinates the entire IPDS which are located at different location in the network. When a local IPDS detects an attack, it informs its neighboring IPDS about the attacker by sending the attacker's IP address. To extend the prevention or the IPDS that focus on the detects of attack along with the neighboring IPDS blocks the traffic from that attacker and collaboratively informs the gateway IPDS which reject that node by blocking future traffic from that attacker.

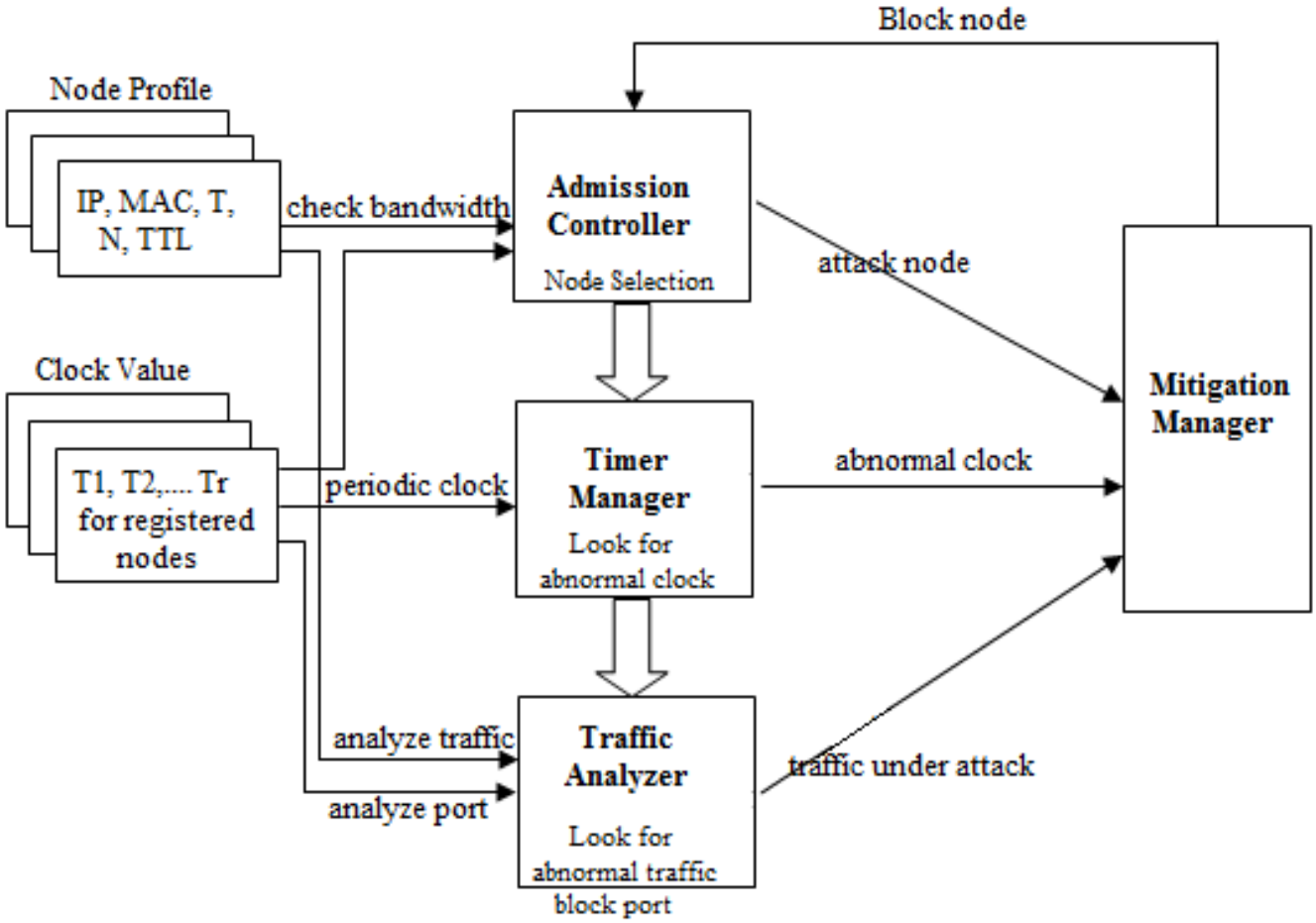

Figure 2. The eShield System

eShield protects potential victims based on clock values. The clock value includes the node's system clock that is monitored periodically. The *eShield* system uses a trusted *gateway IPDS* to which the nodes have to register in order to obtain the total allowed bandwidth consumption and TTL. The *gateway IPDS* maintains a record of registered IP addresses which may be the victims for the attackers for injecting packet floods. All communications between the IPDS and users are being secured using a key of public or private encryption scheme. The *gateway IPDS* co-ordinates the mitigation process within a network and outside the network. The *eShield* system also uses a collection of local IPDS which collaboratively involve in admission control, time management and traffic analysis. The local IPDS regularly update this information in its table.

A. *eShield Metrics*

eShield maintains the following metrics.

1) Bandwidth: The bandwidth b_i is the part of channel bandwidth allowed to any node $n \in N$ where N is the network with n number of nodes.

$$b_i = \frac{B}{N_n} \quad (1)$$

where B is total bandwidth allocation for the network signaling and N_n is the total number of registered node in the network. In an unsaturated network, not all users are active. Thus,

$$\sum_{i=1}^{m} b_i \leq B \quad (2)$$

and in a saturated network, all registered nodes are available and has packets to communicate. Thus,

$$\sum_{i=1}^{m} b_i = B \quad (3)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

where b_i is valid only for a particular TTL and after TTL expires, all nodes will acquire new b_i.

2) Clock Value: The timer manager maintains the clock values $\sum_{n=1}^{r} T_n$ for each node n at periodic intervals. It then calculates whether the clock values match the threshold by using the formula,

$$\sum_{n=1}^{r} T_{n-1} - T_n = \Delta \quad (4)$$

where T_{n-1} previous clock value of a node and T_n is the current clock value of that node. If the clock values match the threshold, then the node is under normal state. Otherwise, the node is under abnormal state.

3) TCP flow metric: The fraction of bandwidth utilized per-glide all through a period is given by,

$$N_{bf_c} \leq \frac{b_i}{N_c} \quad (5)$$

and the part of bandwidth usages for the consumption of overall flows per-node during several time interval is given by,

$$\sum_{c=1}^{n} N_{bf_c} \leq \frac{b_i}{N_c} \quad (6)$$

where N_c is the flow number between a consecutive nodes, and b_i is the fraction of channel bandwidth allowed to a node i.

B. *Mitigation Algorithm:*

Input: b_i, *incoming traffic flow at node* n; $i = 1,2,..m$
T_n, *the periodic timer values*
$n = 1 \ldots . r$ *and* $n \in N$

for all nodes $n \in N$
  if $\left(k(b_i, b_i') \leq \varpi\right)$ *then*
    return false (n)
    else if $(T_{n-1} - T_n \neq \Delta)$*then*
      $n = false$
      return
      else if $N_{bf_c} \leq \frac{b_i}{N_c}$ *and* $\sum_{c=1}^{n} N_{bf_c} \leq \frac{b_i}{N_c}$ *then*
        $n = false$
        raise attack alert
        return
      endif
    endif
  endif

IV. PERFORMANCE RESULTS

We mainly used a Simulator of NS-2 tools for the evaluation of the eShield system in the over the flooding DDoS attacks. Here we compared the statistics performance of eShield with Firecol.

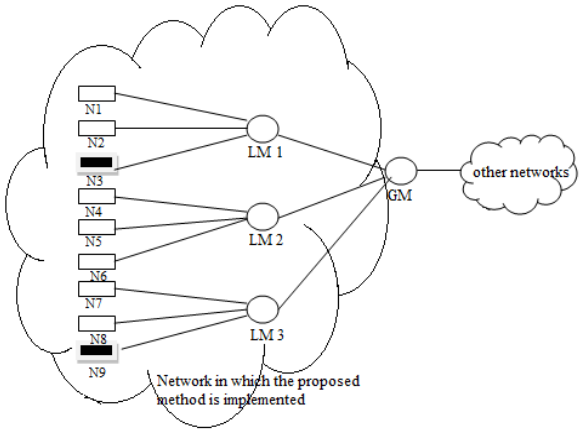

Figure 2.A sample topology for evaluation of the proposed method. GM is the gateway monitor, LM1, LM2 and LM 3 are the local monitors, N1-N9 represent wireless nodes of which N3 and N9 represent attack nodes.

The metrics used for comparison are: 1) FPR 2) DT (Detection Time) 3) Scalability & 4) Percentage of collaborative IPDS. Figure 2 shows a sample mesh topology network of nine nodes out of which we assumed nodes N3 and N9 as attack nodes. The network contains 50% of local IPDS. The gateway IPDS monitors communication within an outside the network and all the local IPDS communicate within the network. All registered and selected nodes within the networks are set to be synchronized. The false rate is the amount of original visitors wrongly assigned and which were detected as mischievous consumer. Every IPDS method and save universal current TCP connection facts, it holds extra fake quotes. Here, this may now not get stricken by the final traffic detection and filtering behavior. Figure 3 indicates the false positive rates of Firecol and eShield w.r.t the variety of local detection on IPDS. The false positive ratio is coarsely improved to greater than 5% which is acceptable and now not having any impact in very last detection of consequences from filtering.

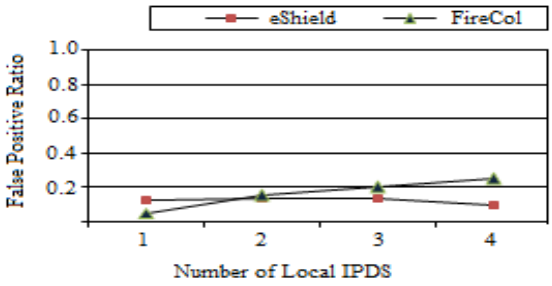

Figure 3. Comparison of False Positive Rate

The process of deliberating the attack detection time is the overall postpone that well-known shows the detection among the attack happens and approximately its detected time. The detection in flooding attack is primarily focused over regular intervals of scalability and its detection time. Figure 4 shows detection of Firecol and eShield, which can stumble on the start and end an attack where begin may be inside one detection time and an attack can be inside two detection time durations.The eShield methodology will accomplish filtering and with more exact detection over a short delay. If the local IPDS percentage when it increases, then the detection time of attacks will required less time.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

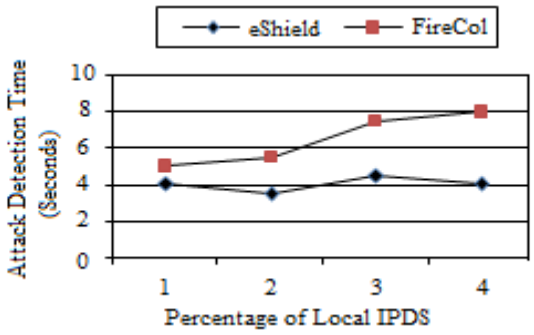

Figure 4. Comparison of Attack Detection Time

The scalability is closely dependent on the number of local IPDS located in the network. For a network with 500 nodes, the *eShield* system requires 166 local IPDS. However, to overcome the complexity in communication, we encourage all IPDS to forward only collaborative messages among themselves and to gateway IPDS. Each IPDS confirm an attacker if the probability of IPDS collaboration messages reaches a certain threshold, say, th.

eShield efficiency trusts on the association among dissimilar IPDS techniques. The *eShield* cannot be enabled over all routers in the network. The IPDS devices like routers then performs a detection of malware attacks and it forwards the messages through the adjacent routers with filtering mechanism and also detected over the gateway IPDS sources. When an IPDS does not receive the collaborative information from its neighboring routers. i.e.; when the percentage of participating IPDS is less than 50%, the IPDS does not get adequate data to decide thus results in few false positive in identified nodes over networks.

V. CONCLUSION

In this paper, an effective eShield mechanism with its architecture was proposed which results in the flood detection and prevention of flooding nodes and also this reports the detailed victim node and prevent the port being attacked. eShield architecture does not makes a way to evade the detection schemes. Also the time taken to start and end of an attack is less than the detection intervals, meanwhile through simulations, this was demonstrated with *eShield* methodology performs faster than Firecol and eShield also provides the most accurate detection method when compared to other approaches.

REFERENCES

1. A Shevtekar, K Anantharam & N Ansari, (2005). "Low Rate TCP Denial-Of-Service Attack Detection At Edge Routers," IEEE Commns Letters, Volume. 9, Number. 4, 2005
2. Cert Advisory Ca-1996-21 (1996). "TCP SYN Flooding And IP Spoofing Attacks", CERT, vol.21, 1996.
3. D. Geneiatakis, C. Lambrinoudakis, (2007). "A lightweight protection mechanism against signaling attacks in a SIP-based VoIP environment", Jo. of Telecommns Systems (Springer), Volume 36, Issue 4, pp 153-159.
4. D. Geneiatakis, N. Vrakas, C. Lambrinoudakis, (2009) "Utilizing Bloom Filters For Detecting Flooding Attacks Against SIP Based Services," Elsevier Jo. of Computers & Security, Vol. 28, Iss. 7, Pages 578-591.
5. Ge Zhang, Fischer-Hubner, S. Ehlert , (2010). "Blocking attacks on SIP VoIP proxies caused by external processing", Jo. of Telecommn. Systems (Springer), Volume 45, Issue 1, pp 61-76.
6. H. Safa, M. Chouman, H. Artail, M. Karam, (2008) "A Collaborative Defense Mechanism Against SYN Flooding Attacks In IP Networks", Elsevier Jo. of Network & Computer Applns, Vol. 31 Iss.4.
7. I.B. Mopari, S.G. Pukale, M.L. Dhore, (2009). "Detection Of DDoS Attack And Defense Against IP Spoofing", Proceedings of the International Conference On Advances In Computing, Commn. And Control, ICAC3'09, Mumbai, India, PP. 489-493.
8. J.Ioannidis & S. Bellovin, (2002), "Implementing Pushback: Router-Based Defense Against Dos Attacks", In Proc. NDSS.
9. Jelena Mirkovic, Peter Reiher, (2005) "D-WARD: A Source-End Defense Against Flooding Denial-Of-Service Attacks," IEEE Trans. On Dependable & Secure Computing, Vol. 2, No. 3.
10. Joseph Chee Ming Teo, Chik How Tan, Jim Mee Ng, (2007). "Denial-of-service attack resilience dynamic group key agreement for heterogeneous networks", Journal of Telecommn. Systems, Volume 35, Issue 3-4, pp 141-160.
11. Patrick P.C. Lee A, Tian Bu B, Thomas Woob, (2009) "On The Detection Of Signaling Dos Attacks On 3G/Wimax Wireless Networks," Elsevier Jo. On Computer Networks (53).
12. Sungwon Yi, Xidong Deng, George Kesidis, Chita R. Das, (2008). "A dynamic quarantine scheme for controlling unresponsive TCP sessions", Volume 37, Issue 4, pp 169-189.
13. Sudip Misra, P. Venkata Krishna, Kiran Isaac Abraham, Navin Sasikumar, S. Fredun, (2010) "An Adaptive Learning Routing Protocol For The Prevention Of Distributed Denial Of Service Attacks In Wireless Mesh Networks," ACM Jo. of Computers & Math. With Appns., Vol. 60, Issue 2.
14. Suman Jana and Sneha K. Kasera, (2010), "On Fast And Accurate Detection Of Unauthorized Wireless Access Points Using Clock Skews," IEEE Trans. On Mobile Computing, Vol. 9, No. 3.
15. S. Ranjan, R. Swaminathan, M. Uysal, A. Nucci & E. Knightly, (2009), "DDoS-Shield: DDoS-Resilient Scheduling To Counter Application Layer Attacks," IEEE/ACM Trans. On Networking, Vol. 17, No. 1.
16. Wei Chen, Dit-Yan Yeung, (2006). "Throttling spoofed SYN flooding traffic at the source", Journal of Telecommn. Systems, Volume 33, Issue 1-3, pp 47-65.
17. Xiaowei Yang, Wetherall, D. Anderson, T., (2008), "TVA: A DoS-Limiting Network Architecture", IEEE / ACM Trans. On Networking, Vol. 16 , Issue 6.
18. I. Diana Jeba Jingle, Elijah Blessing, P. Mano Paul (2012), "Distributed Detection of DoS Using Clock Values in Wireless Broadband Networks", International Jo. of Engg. and Advanced Tech. (IJEAT), ISSN: 2249 – 8958, Vol. 1, Iss. 5, 2012
19. P. Mano Paul and R. Ravi, (2018), "A Collaborative Reputation-based Vector Space Model for Email Spam Filtering", Journal of Computational and Theoretical Nanoscience, Vol. 15, No.2, Pages 474-479, American Scientific Publishers, 2018
20. Suman Jana and Sneha K. Kasera, (2010), "On Fast And Accurate Detection Of Unauthorized Wireless Access Points Using Clock Skews," IEEE Trans. On Mobile Computing, Vol. 9, No. 3.
21. Jerome Francis, I. Aib, & R. Boutaba, (2012), "Firecol: A Collaborative Protection Network For The Detection Of Flooding Ddos Attacks," IEEE/ACM Trans. On Networking, Vol. 20, No. 6.
22. C. Sun1 C. Hu2 B. Liu3, (2012), "SACK2: effective SYN flood detection against skillful spoofs," IET Inf. Secur., Vol. 6, Issue. 3, pp. 149–156.
23. P. Mano Paul, Dr. R. Ravi (2018), "A novel Email Spam Detection protocol for next generation networks" Taga Jo. of Graphic Tech, Technical Assoc. of the Graphic Arts, Vol.14, Pages 124-133, 2018
24. P. Mano Paul and R. Ravi (2018), "Cooperative Vector Based Reactive System For Protecting Email Against Spammers in Wireless Networks", Jo. of Electrical Engg., Edition 4, Volume 18, ISSN: 1582-4594.
25. N. Saxena, M. Denko, Di. Banerji, (2010), "A Hierarchical Architecture For Detecting Selfish Behaviour In Community Wireless Mesh Networks", Elsevier Jo. Of Computer Commns.

AUTHORS PROFILE

J. Daniel Francis Selvaraj is the Assistant Professor of Sri Krishna College of Engineering and Technology, Coimbatore, India. His Bachelor Degree of Engineering from JJ College of Enginnering and Technology in Information Technology branch, Bharathidasan University, India in 2003. He Obtained his Master of Engineering degree from Department of Computer Science and Engineering from Manonmanian Sundaranar University, Tirunelveli, India in 2005. His area of research interests is Artificial Intelligence, Mobile Ad-hoc Networks and Network Security.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Dr. I. Diana Jeba Jingle is the Assistant Professor of Christ University, Bangalore, India. He received her Bachelor of Technology is in the department of Information Technology from Sun college of Engineering and Technology, Anna University, Tamil Nadu, India in 2006 and she received her Master of Engineering degree in Computer Science Engineering from Francis Xavier College of Engineering, Anna University, India in 2008. She obtained her Ph.D in CSE Department from karunya University, India. Her area of research interests is in wireless networks, Cyber security, Mobile Ad-hoc Networks, Internet of Things, Internet of Everythings etc.

Dr. P. Mano Paul is the Assistant Professor from Presidency University, Bangalore, India. He received his Bachelor of Engineering in the department of Information Technology from Noorul Islam College of Engineering, Manonmaniam Sundaranar university, India in 2002. He received his Master of Engineering from Department of Computer Science and Engineering, University Department from Manonmanian Sundaranar University, India in 2005. He completed his Ph.D in the department of Computer Science and Engineering from Anna University, Guindy campus, chennai, India. His research interests is in the area of Cyber Security, Mobile Ad-hoc Networks and Big-Data etc.