International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-1 Issue-5, June 2012

Distributed Detection of DoS Using Clock Values in Wireless Broadband Networks

I.Diana Jeba Jingle, Elijah Blessing Rajsingh, P.Mano Paul

Abstract - Wireless broadband networks are most vulnerable to denial-of-service attacks where attackers can disrupt legitimate communication between hosts in a network by flooding unwanted traffic between legitimate hosts. Flooding attack at the transport layer affects the TCP's 3-way handshake process, thereby denying the services of TCP. It also denies the services of UDP. This paper proposes a novel flooding attack, the most severe denial-of-service attack that occurs at the transport layer of the internet. The main objective of this approach is to install local and global monitoring agents at various points in order to monitor and filter real-time TCP traffic and UDP traffic thereby allowing legitimate traffic to flow in the network during attack traffic filtration process and to avoid buffer overflow at the monitoring agents. Also, a novel algorithm has been proposed by taking the clock values of each node into account for effective detection of the attack. This distributed defense mechanism reduces the burden on a single global monitoring agent thereby introducing local monitoring agents at various points in the network. The performance results show that this approach effectively and accurately detects and filters DOS attacks within a short period.

Index Terms—DOS, Flooding, Handshake, Spoofing.

I. INTRODUCTION

Wireless broadband networks transmit and receive packets at high bandwidth and at high data rates. Wireless Fidelity (Wi-Fi) networks transmit packets at high bandwidth within a small range. Wireless Interoperability for Microwave Access (WiMax) networks transmits packets at high bandwidth but within a moderate range. Wireless Mesh Networks (WMN) transmits packets at high bandwidth in large range. Denial of Service (DOS) attack is common in all these networks in every layers of the internet. The most severe DOS attack is the flooding attack at the transport layer where the TCP's 3-way handshake process is affected. TCP is a connection-oriented reliable message transfer protocol and a connection need to be established between the sender and the receiver prior to transmission and reception of packets. While establishing connections between sender and receiver two types of flooding attacks are possible: 1) Half-open connection flooding and 2) Full-open connection flooding.

Half-open connection flooding works as follows: An attacker with node 1's spoofed IP address tries to connect to node 2 by sending SYN segment. Node2 thinks that the SYN segment belongs to Node1 and opens a TCP connection and replies with a SYN/ACK segment to Node1. The Node2 sends numerous SYN/ACK segments until it receives ACK from the Node1. Since Node1's IP address is spoofed, the SYN/ACK never reaches Node1, but it reaches the attacker. The attacker never sends ACK to Node2. Node1 also never sends ACK to Node2 leaving the connection half-open and no data transfer takes place in this connection. This is called as half-open flooding.

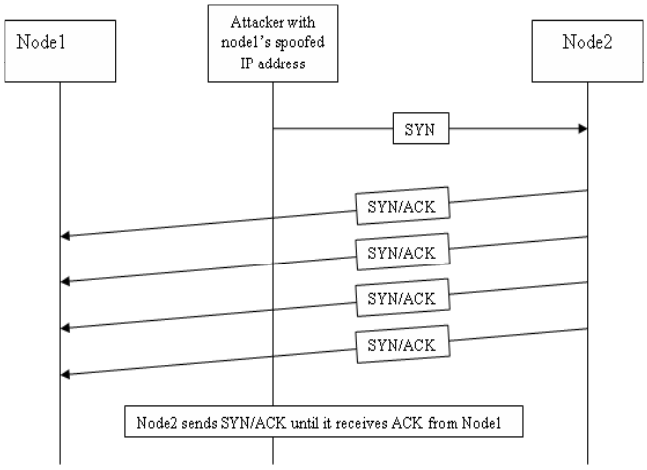

Fig.1. Half-open connection flooding attack

Full-open connection flooding works as follows: An attacker with Node1's spoofed IP address tries to connect to Node2 by sending SYN segment. Node2 thinks that the SYN segment belongs to Node1 and it opens a TCP connection and replies with a SYN/ACK segment to Node1. Since Node1's IP address is spoofed, the SYN/ACK never reaches Node1, but it reaches the attacker. The attacker in turn replies with ACK segment to Node2. Thus a full-connection is established but the attacker never sends and receives data through that connection, leaving that connection full-open. At the transport layer, UDP traffic floods also occur. UDP is a connectionless unreliable protocol and there is no need of connection establishment between the sender and the receiver prior to transmission and reception of packets. In UDP, the attacker tries to flood the victim with more number of request packets thereby denying the services of UDP at the victim node. Due to such TCP and UDP traffic floods many problems occur: 1) The node's link bandwidth is consumed by the attacker. 2) The node's buffer capacity will be fully occupied by the attacker. 3) The node's service capability is wasted (i.e. The legitimate node is denied from providing its service to other legitimate nodes).

Manuscript published on 30 June 2012.
***** Correspondence Author (s)
I.Diana Jeba Jingle*, Department of Computer Science, Loyola Institute of Technology and Sciences, Nagercoil, India
Elijah Blessing Rajsingh, Department of Computer Science and Information Technology, Karunya University, Coimbatore, India,
P.Mano Paul, Department of Computer Science, Loyola Institute of Technology and Sciences, Nagercoil, India.

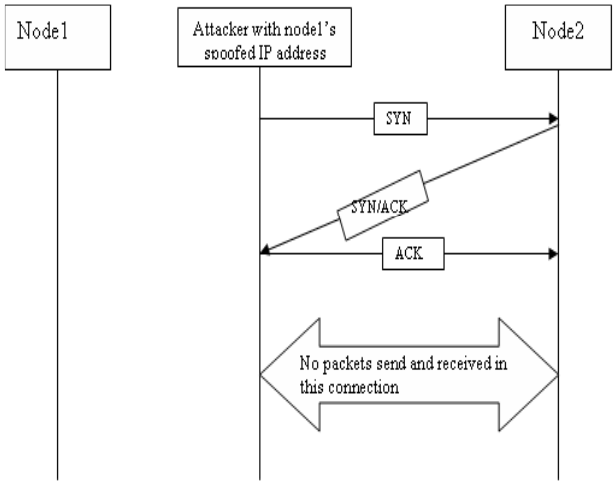

Fig.2. Full-open connection established

Many such full-open connections are established and they flood Node2.

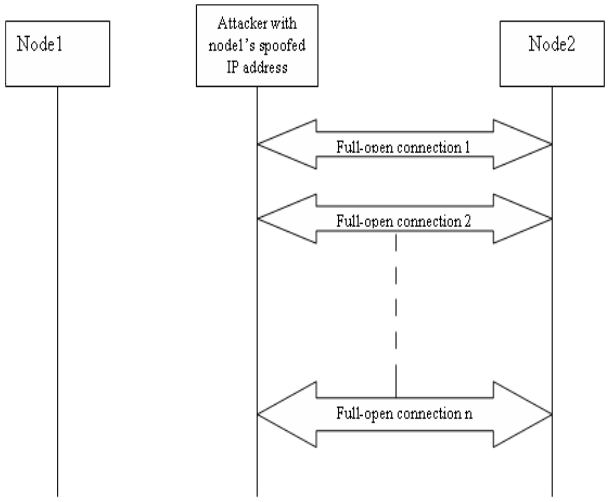

Fig.3. Many such Full-open connections flooding node2 with no packets send and received

The remainder of this paper is organized as follows: Section II describes the related work on flooding attacks. Section III describes the design of the proposed detection mechanism to mitigate flooding attacks. Section IV presents the experimental evaluation and performance results of the proposed detection mechanism. Finally, we conclude in Section V.

II. RELATED WORK

DWARD [1] autonomously detects and filters attack traffic from legitimate traffic by dropping the excess traffic by limiting the traffic rate to and from the victim thereby reducing the overload at the victim. But DWARD cannot detect attack traffic until connection buffer fills up thereby causing increased time delay to detect an attack and it causes more communication overhead. Sudip Misra *et al*. [2] proposed DLSR which uses the concept of Learning Automata (LA) and prevents the server being overloaded with excess amount of illegitimate traffic from crashing and keeps the server functioning. However DLSR cannot effectively differentiate valid user's IP address and spoofed user's IP address and it also causes excess time delay to detect and filter an attack. DARB [3] uses an active probing detection method and a TTL based rate-limit counteraction method to detect and filter SYN flooding attack traffic accurately and independently on the victim side. DARB consumes more amount of the victim's bandwidth and causes computation overhead for both detecting and counteracting methods. Patrick P.C. *et al*. [4] proposes an online early detection algorithm based on the statistical CUSUM method for detecting signalling attacks on wireless networks in a timely manner. This approach does not detect the attack traffic that has a spoofed IP address and causes signaling load on the control plane. This detection mechanism blocks all the traffic (both benign and malicious traffic) when the signaling load reaches a threshold. TVA [5] is a Traffic validation architecture which uses capabilities to discard unauthorized traffic floods on a single autonomous system. TVA achieves high throughput. The problem is TVA stores all capability information of each user on routers and a router with limited number of queues may not be able to protect all legitimate users. Haidar Safa et al. [6] proposed CDMS that is implemented at the edge routers of spoofed IP address' networks to defend the victim. CDMS also a communication protocol is used to encourage collaboration between various networks to protect each other. This mechanism is very efficient and it prevents the routers from being overloaded. However this mechanism causes time delay to detect and filter an attack. Supranamaya Ranjan et al. [7] proposed DDoS-Shield to detect the attack packets that overwhelm the system resources such as bandwidth. DDoS Shield consist of a suspicion assignment mechanism that examines requests belonging to every session (TCP,UDP,ICMP) and assigns suspicion values to sessions and a DDoS-resilient scheduler that schedules the sessions based on the values assigned to the sessions and decides which session to be forwarded and when. The scheduler also performs rate-limiting. DDoS shield improves victim's by consuming less memory for buffering requests and responses. However DDoS Shield consumes more processing time and cannot produce good throughput. Dimitris Geneiata et al. [8] proposed a two-part bloom filter based monitor to detect and filter flooding attacks against proxy servers. The monitor's main task is to record the state of any incoming session in 3 different filters and the filter is indexed through a hash function. This mechanism uses an alarming system to trigger an alarm and report if any entries in the filter exceed the threshold value. This mechanism is very efficient and cost-effective and causes reduced time delay to detect an attack. However, hashing of entries in the filters leads to computation overhead and more CPU utilization.

The existing approaches in the area of DoS were unable to effectively differentiate valid user's IP address and spoofed user's IP address. Once the attack is identified all traffic is blocked to reduce the load on the server thereby blocking legitimate traffic also. The buffer capacity in the router's queue is not enough to accumulate all legitimate traffic requests. Also to detect an attack, the system consumes more time. Due to these limitations in the existing approaches, it is necessary to frame a novel approach to mitigate DoS attack in wireless broadband networks.

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

To summarize, this paper addresses a novel flooding attack that takes place at the transport layer which is not addressed in existing detection schemes. It is observed that DoS attacks depend heavily on IP spoofing; therefore preventing IP spoofing might contribute to solving the problem. A common way for preventing IP spoofing is by using ingress and egress filters on firewalls. But it fails in wireless networks where legitimate packets could have topologically incorrect addresses. To combat this, a novel admission control mechanism is implemented at the victim network in order to make registration strong thereby preventing IP spoofing in the network. Once IP spoofing is prevented, the flooding attack can be banned effectively.

III. PROPOSED METHODOLOGY

To prevent unauthorized access, every node whether stationary or mobile should be registered with the MA to join the network. The registration process is made effective such that attackers cannot spoof the valid user's IP address. Monitoring Agent (MA) plays the major role in this approach. All nodes must first register with the global MA to be a part of the network. All global MAs maintain a Host Profile Table (N1, N2….. Nn) of valid IP addresses as shown in Table 1. The Host Profile Table maintains a table with 3 fields: 1) host name 2) host address 3) privileged information about the host. The registration is done using the node's clock values. The registration is a 4-way handshake process and is described as follows: All Nodes first sends a join request message to join the MA. The MA asks the Nodes to send their privileged information to confirm their identity. The privileged information contains the following: 1) IP address of nodes, 2) MAC address of nodes, 3) Secret value (key) that changes in every TTL, 4) Clock value of nodes, T. The nodes prepare the privileged information and reply the HMAC value of this privileged information to the MA. The MA sends a successful reply message to the nodes. The successful reply message contains the hash of HMAC value of the following: 1) TTL (Time to Live), how long the privileged information is valid, 2) N, the total number of bytes that is allowed to and from each node.

$$N = \frac{B}{Nn}$$

where B is the total bandwidth allotted by the network and Nn is the total number of available nodes in a network.

The nodes after successful registration are allowed to transmit and receive only N bytes of data at a particular time. Nodes failing to transmit and receive less than or equal to N bytes of data are not allowed to be a part of the network.

Table 1 Router Information

Host Profile Table					
Host Name	IP Address	Privileged Information			
		IP	MAC	Secret	T

After successful registration, the Global MA informs the local MA (by sending the IP addresses of registered nodes) to allow traffic to and from the registered node. Now all nodes must periodically (10 seconds) send clock values (i.e. $T_1, T_2 \ldots T_n$) to their local MA when the nodes are available. The local MA checks these T values and computes the threshold as, $\Delta = T_1 - T_0$. The subsequent T values must be equal to the threshold. that is, Check whether T3-T2 = Δ. If not, check whether T4-T3 = Δ. If T4-T3 $\neq$ Δ then the MA never includes that node to be a part of the network and blocks all traffic to and from node1. This is shown in the algorithm below. The Local MA checks for each node whether $T_i - T_{i-1} = \Delta$. If so, then the local MA includes that node to be a part of the network. If $T_i - T_{i-1} \neq \Delta$, then the MA never includes that node to be a part of the network and blocks all traffic to and from that node. Consider a node that is unavailable at time t_2 and later at time t_3 it becomes available. When a node becomes available, that node should send the last T value when it was available (i.e.T_2) and the current T value (i.e.T_3) to the local MA. i.e. $T_{i-1}+T_i$ The local MA compares these T values (i.e. T_{i-1}) with those values in its table. If the T values (T_{i-1}) are valid, then the local MA grants privilege for that node to be a part of the network. Even if an attacker spoofs a node's IP address and act like that node, the attacker can be easily found; because the clock values of attacker's machine and the node's machine will not be the same. Only nodes within a network have synchronized clock values. There is a chance of authorized nodes being rejected by the MA and their traffic being blocked by the MA. In such case, the MA selects the rejected nodes from its table and asks those nodes to re-register with a new set of privileged information (derived from previous privileged information). If the node is still under attacker's hold, then the attacker cannot send a successful reply message. All local MAs will periodically send valid IP address report to the Global MA. The Global MA checks the report and removes those nodes, whose IP address is not listed in the valid IP address report from the network. MA includes the privileged information of all nodes and all networks in its table. After registration, the MA grants privilege for the nodes to be a part of the network. This privileged information is valid for TTL period. The length of TTL is 2^{32}. The clock value is a hash (T + Secret key). For every 10 seconds, the secret key value increments by 1-bit. The length of secret key is 32-bits and for every TTL, the secret key value changes when the privileged information changes.

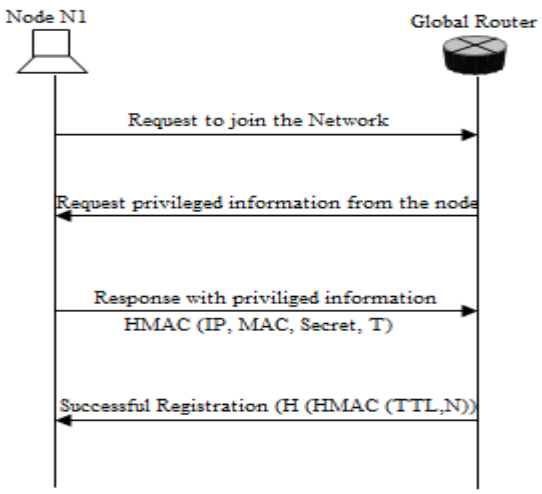

Fig. 4. Registration for nodes within a network

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

After TTL expires, the privileged information becomes invalid and all nodes and networks must re-register with the MA. This re-registration is done using previous privileged information.

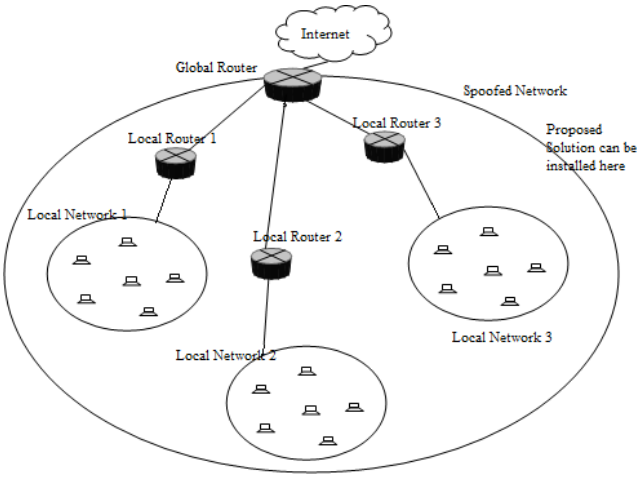

Fig.5. Network Topology in which proposed solution is implemented

IV. EXPERIMENTAL AND PERFORMANCE RESULTS

We have used the NS-2 network simulator for carrying out simulations. The network nodes are arranged in a mesh topology, the global monitoring agent (gateway router) receives packets from other networks, the local monitoring agent (local routers) receives packets from the source nodes in the network. The network contains 20% Local monitoring agents. The following performance metrics are used to measure the effectiveness of the proposed defense mechanism over existing techniques.

1) Time delay (TTD): It is the time taken for nodes to register with the monitoring agent and the time taken for the monitoring agent to detect an attacker.
2) False positive ratio (FPR): It is the percentage of number of legitimate nodes wrongly detected as attack nodes out of the total number of legitimate nodes in the network.
3) Rate of change of delta: The rate at which the delta value changes over time.

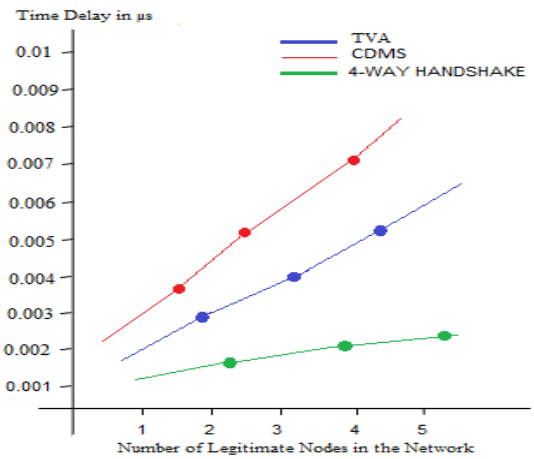

Fig.6. Time delay vs. Network Size

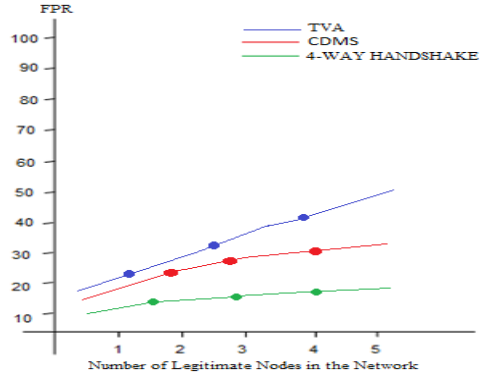

Fig. 7. False Positive Ratio vs. Network Size

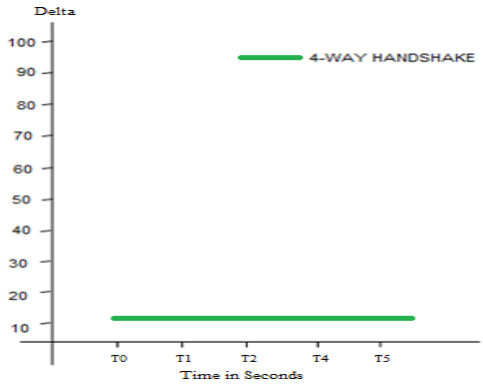

Fig. 8. Rate of Change of Delta

The simulation results show that the registration process is done without much delay and the attack nodes are detected within a short period in the proposed scheme when compared to TVA and CDMS as shown in fig. 6. As the network size increases the false positive ratio decreases in the proposed scheme when compared to TVA and CDMS as shown in fig. 7. The rate of change of delta value is proved to be constant over time and it is shown in fig. 8.

V. CONCLUSION

In this paper we have clearly stated half-open connection flooding and full-open connection flooding attack that occurs at the transport layer and how it affects the performance of the network. We have also described an efficient method to prevent such flooding attack by introducing 4-way handshake registration mechanism. The implementation results and performance analysis show that this method is more effective and accurate over the existing defense mechanisms. In future this mechanism can also be used to prevent a lot of attacks in broadband wireless networks.

REFERENCES

[1] Jelena Mirkovic, Peter Reiher, "D-WARD: A Source-end Defense Against Flooding Denial-of-service Attacks," IEEE Transactions On Dependable And Secure Computing, Vol. 2, No. 3, July - September 2005.

[2] Sudip Misra, P. Venkata Krishna, Kiran Isaac Abraham, Navin Sasikumar, S. Fredun, "An Adaptive Learning Routing Protocol For The Prevention Of Distributed Denial Of Service Attacks In Wireless Mesh Networks," Acm Journal Of Computers & Mathematics With Applications, Vol. 60, Issue 2, July 2010.

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

[3] Patrick P.C. Lee A, Tian Bu B, Thomas Woob, "On The Detection of Signaling DoS Attacks on 3G/WiMax Wireless Networks," Elsevier Journal on Computer Networks 53 2601–2616, 2009.
[4] Xiaowei Yang, Wetherall, D. Anderson, T. IEEE/ACM Transactions on Networking, Vol. 16 , Issue 6, December 2008.
[5] Haidar Safa, Mohamad Chouman, Hassan Artail, Marcel Karam, "A collaborative defense mechanism against SYN flooding attacks in IP networks," Elsevier Journal of Network and Computer Applications, Volume 31 Issue 4, November 2008.
[6] Dimitris Geneiatakis, Nikos Vrakas, Costas Lambrinoudakis, "Utilizing bloom filters for detecting flooding attacks against SIP based services," Elsevier Journal of Computers & Security, Volume 28, Issue 7, October 2009, Pages 578-591.
[7] Bin Xiaoa, Wei Chenb, Yanxiang Hec, "An autonomous defense against SYN flooding attacks: Detect and throttle attacks at the victim side independently," Elsevier Journal of Parallel and Distributed Computing, Volume 68 (2008), Pages 456 – 470.
[8] P.Ferguson and D.Senie, "Network ingress filtering: Defeating denial of service attacks that employ IP source address spoofing," Internet RFC 2827, 2000.
[9] Suman Jana And Sneha K. Kasera, "On Fast And Accurate Detection Of Unauthorized Wireless Access Points Using Clock Skews," Ieee Transactions On Mobile Computing, Vol. 9, No. 3, March 2010.
[10] J.Ioannidis and S. Bellovin, "Implementing pushback: Router-based defense against DoS attacks," in Proc. NDSS, 2002.
[11] I.B. Mopari, S.G. Pukale, M.L. Dhore, Detection of DDoS attack and defense against IP spoofing, in: Proceedings of the International Conference on Advances in Computing, Communication and Control, ICAC3'09, January 23_24, 2009, Mumbai, Maharashtra, India, pp. 489_493.
[12] Amey Shevtekar, Karunakar Anantharam, And Nirwan Ansari, "Low Rate Tcp Denial-of-service Attack Detection At Edge Routers," Ieee Communications Letters, Vol. 9, No. 4, April 2005.
[13] Supranamaya Ranjan, Member, Ieee, Ram Swaminathan, Mustafa Uysal, Antonio Nucci, Senior Member, Ieee, And Edward Knightly, Senior Member, Ieee, "Ddos-shield: Ddos-resilient Scheduling To Counter Application Layer Attacks," IEEE/ACM Transactions on Networking, Vol. 17, No. 1, February 2009.
[14] CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks, CERT CC, http://www.cert.org/advisories/CA-1996-21.html, 1996.
[15] Nikhil Saxena, Mieso Denko, Dilip Banerji, "A hierarchical architecture for detecting selfish behaviour in community wireless mesh networks," Elsevier Journal of Computer Communications, 2010.

I. Diana Jeba Jingle is the Assistant Professor of Loyola Institute of Technology and Sciences, India. She reveived her Bachelor of Engineering degree in Information Technology from Sun College of Engineering and Technology, Anna University, India in 2006. She received her Master of Engineering degree in Computer Science from Francis Xavier Engineering College, Anna University, India in 2008. Her research interests lie in the area of Wireless Networks, Mobile Ad-hoc Networks and network security and specifically focus on denial-of-service characterization, detection and defense, IP spoofing defense. She is a member of CSI.

Elijah Blessing Rajsingh is the Professor and Director for the Department of Computer Science and Engineering of Karunya University, India. He received his Master of Engineering degree with Distinction from the College of Engineering, Anna University, India. He received the Ph. D degree in Information and Communication Engineering from College of Engineering, Anna University, India in 2005, focusing on Security in Wired and Wireless Networks. He is the member of IEEE. He has very strong research background in the areas of Network Security, Mobile Computing, Wireless & Ad hoc Networks, Parallel and Distributed Computing. He is an Associate Editor for International Journal of Computers & Applications, Acta Press, Canada and member of the editorial review board for International Journal of Cases in E Commerce as well as for Information Resources Management Journal, Idea Group Publishers, USA. He is the recognized guide for Ph.D students of Karunya University and is guiding students in their doctoral programme. He has published a number of papers in international journals and conferences.

P. Mano Paul is the Assistant Professor of Loyola Institute of Technology and Sciences, India. His Bachelor of Engineering degree in Computer Science is from Noorul Islam College of Engineering, M.S. University, India in 2002. He received his Master of Engineering degree in Computer Science from M.S. University, India in 2005. His research interests lie in the area of Cyber security, Wireless Networks and Network Security and specifically focus on malware simulation, detection and defense.

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