1-2 Skip List Approach for Efficient Security Checks in Wireless Mesh Networks

Hemraj Saini

Department of Computer Science & Engineering,
Jaypee University of Infromation Technology, Wakanaghat-173234 (INDIA)
(Email: hemraj1977@yahoo.co.in; hemraj.saini@juit.ac.in)

(Received Jan. 16, 2014; revised and accepted Mar. 27, 2014)

Abstract

In the fast growing era of the online business, Wireless Mesh Networks (WMNs) are playing a significance role to grow the economy of different countries. Therefore, it is essential to implement the efficient security measures or methods at the Wireless Mesh Gateway (GW) as it is only the place to enter the incoming traffic to the particular WMN. In the traditional solutions, the monotonically increased traffic at GW is handled by the help of “linear queue” data structure, which is not the efficient way for security analysis in the present criteria. Therefore, in the manuscript, it is replaced by another efficient data structure named “1-2 Skip List”. In addition, it has shown that detection of flooding or DoS like attacks are also easily possible by using 1-2 Skip List approach. A sufficient analysis is also provided for the proposed solution with performance analysis in the manuscript.

Keywords: Wireless Mesh Network, WLAN, Network Security, 1-2 Skip List

1 Introduction

In case of sparsely populated areas it is difficult and costly to use traditional communication networks. In such types of situation Wireless Mesh Network (WMN) plays an important role for communication and helps to grow the business there. In WMN a number of radio nodes are organized under mesh topology. WMN generally contains mesh client, mesh routers and mesh gateways. Laptops, cell phones, vehicles and other devices having wireless capability can be the part of a WMN. In WMN mesh routers are used to forward traffic to and from the mesh gateway which may, but need not, connect to the Internet. Every radio node creates its own mesh cloud having the rage up to its coverage area [1, 2, 3] and likely to be a single network. Mesh cloud can be accessed by the permission of the radio node which is working in coordination with other radio nodes to create radio network. A WMN preserves the properties of reliability that offers redundancy. Non operational mode of a mesh node doesn’t mean that rest of WMN is not in operation, the rest of the nodes can still communicate to each other. They can communicate directly or through other one or more intermediate mesh nodes. Figure 1 depicts a sample of WMN. A WMN can be implemented with various technologies such as 802.11, 802.15, 802.16, Cellular technology or combination of more than one type [4, 5, 6, 7, 8].

A talented purpose of WMN is the low cost extension of wireless local area network (WLAN) in a sparsely populated area. A WLAN links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider Internet. This gives users the mobility to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name. WLANs were once called LAWNs (for local area wireless network) by the Department of Defense. An application of WMN can be a pilot program to provide city workers in all different municipality of the city with wireless Internet. The traffic of all the access clients passes through the Mesh Gateway (GW) which causes a monotonically increase in the traffic [9, 10, 11]. Additionally, there is a great possibility of the malicious attack from the incoming traffic from the Internet. Therefore, it is heavily required to keep an eye over the incoming traffic. Another thing, the incoming traffic from the internet can be at high rate and hence an efficient data structure is to be used to synchronize it with the delivery speed at their respective destinations. In traditional implementation this data structure is either a linear array or a linear linked list [12, 13, 14]. These two data structures are having the scope of enhancement in the performance of the WMN as well as better security check process. In the manuscript, 1-2 skip list has been used for the purpose which leads the better results.

The paper is further organized into six more sections. Section-II is devoted to understand the concepts of skip list. Section-III discussed the usage of 1-2 skip list for temporary storage of incoming traffic. Section-IV provides the implementation of 1-2 skip list to detect DoS like attacks. Section-V explains about the performance analysis of proposed method and the section-VI provides the conclusion about the whole work.

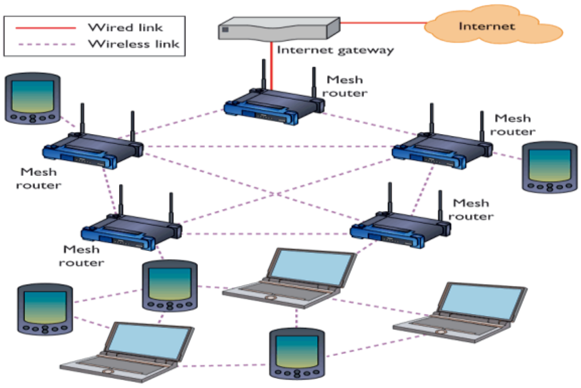


Figure 1: Wireless mesh network

2 Skip List

A skip list is a data structure for storing a sorted list of items using a hierarchy of linked lists that connect increasingly sparse subsequences of the items. These auxiliary lists allow item lookup with efficiency comparable to balanced binary search trees (that is, with number of probes proportional to log n instead of n).

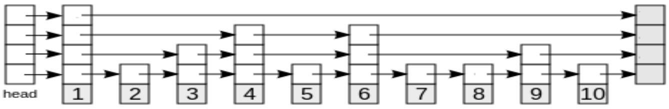


Figure 2: Skip list

Each link of the sparser lists skips over many items of the full list in one step, hence the structure's name as shown in Figure 2. These forward links may be added in a randomized way with a geometric / negative binomial distribution. Insert, search and delete operations are performed in logarithmic expected time. The links may also be added in a non-probabilistic way so as to guarantee amortized (rather than merely expected) logarithmic cost [15, 16].

A simple version of a skip list is called an 1-2 skip list, that has either 1 or 2 nodes of height h-1 between any two nodes of height h or more. This is depicted in Figure 3.

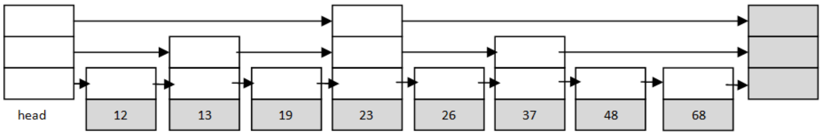


Figure 3: 1-2 Skip list

3 1-2 Skip List For Temporary Storage of Incoming Traffic

Incoming traffic at the mesh gateway (GW) node in Wireless Mesh Network (WMN) from the internet is continuously available. There are many number of access client nodes (ACNs) are existing in WMN and want to interact with the external points existing in the outer Internet. Therefore, the traffic can be increased monotonically at the GW node. To handle this incoming traffic it is required to temporarily store at the GW node by the use of some data structure. This data structure is generally storage queue which is less efficient to analyze the traffic for security check as the incoming traffic may contains malicious information. Therefore, we are proposing the usage of 1-2 skip list for temporary storage of incoming traffic. Incoming traffic stored in 1-2 skip list can be analyzed in a better way for security checks and increases the efficiency of the network. Let us consider a criteria where more than on DoS attacks are available in the incoming traffic from different source IPs. If the traffic is stored in a queue than it is difficult to analyze each packet for a particular time duration but 1-2 skip list make it easier. Assuming that there is incoming traffic from different source IPs and is recorded for a fixed time interval Δt shown as below in Table 1.

Table 1: Incoming packets from various source IPs in Δt time

Sr. No.	Source IP	No. Of Packets
1	IP1	10
2	IP1	20
3	IP2	12
4	IP3	13
5	IP1	23
6	IP2	34
7	IP3	27
8	IP4	24
9	IP3	15
10	IP2	31
11	IP1	15

1-2 skip list can be designed for Table 1 depicted in Figure 4. In Figure 3 every value is build by two atomic values i.e. source IP and number of packets in Δt time.

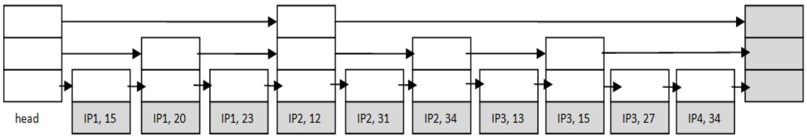


Figure 4: Corresponding 1-2 skip list for Table 1

4 Using 1-2 Skip List To Detect DoS Like Attack

Incoming traffic from the outer side will entered into the WMN from WG only therefore, either a queue of a 1-2 skip list is required to handle the incoming traffic. In the queue it is difficult to identify an IP which is continuously sending the packets beyond a threshold value during Δt time but 1-2 skip list can by tool to solve this problem.

1-2 skip list sorts all the incoming traffic with IP and number of packets shown in Figure 3 and hence it can be utilized to improve the performance. Identifying which IP is flowing maximum number of packets during Δt time, it can be checked with respect to the ***threshold value*** (threshold value can be different for different scenarios of the network and traffic management in network and can be adjusted by an adaptive way [17]). If it is beyond the threshold value, related IP can be categorized as the suspected IP and kept under supervision. If same property of this IP is repeated for 5 times (or fixed according to the application), it can be marked as attack carrying IP and security measures are to be taken over it. In this way Distributed Denial of Service Attacks (DoS) of flooding attacks can be easily detected and sorted out which is depicted in Figure 5 and Figure 6 in the form of flow chart and algorithm respectively.

5 PERFORMANCE ANALYSIS OF PROPOSED METHOD

Most common operations used over 1-2 skip list at GW node are search, insert and delete. Incoming traffic can be handled at GW node by using any one of linear queue, linear linked list and 1-2 skip list. Incoming traffic at GW node handled by linear queue allows search operation at cost O(logn) and insertion and deletion at the cost O(n). But in case of using linear linked list search is at the cost O(n) and insertion and deletion at the cost O(1).

In case of 1-2 skip list all the operations are optimized and performance increased. Search operation for 1-2 skip list is at the cost O(n) and updating operation have the cost O(logn). An experiment has been carried out in a constant computer network of seven (07) computer nodes. Results of the network statistics when queue is used and 1-2 skip list is used are shown in Table 2 and Table 3 respectively.

It is depicted in Figure 7 that there is no packet drop in case of 1-2 skip list implementations as it is dynamic but in case of queue implementation there are packet drops. Figure 8 depicts that there is no false positive detected in case of 1-2 skip list implementation as it will detect the attack only after a sufficient time supervision but in case of queue there are false positive detected as it will every time detect the attack if the incoming traffic goes beyond the threshold value.

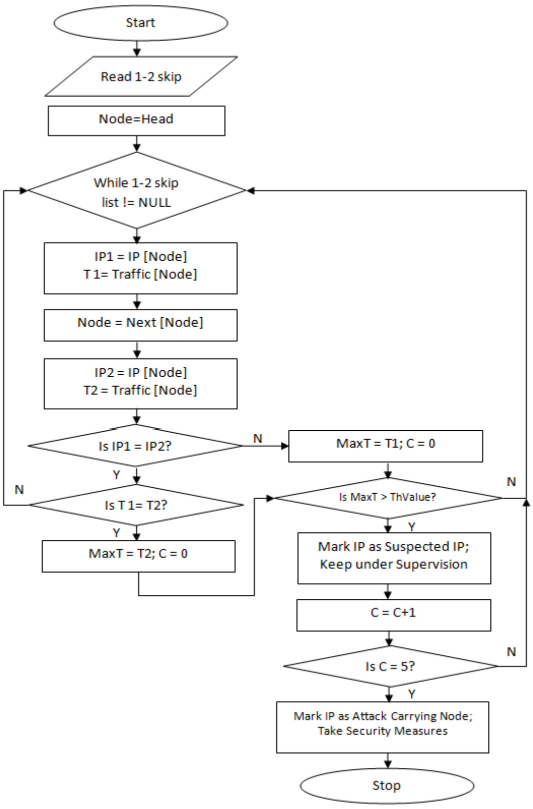
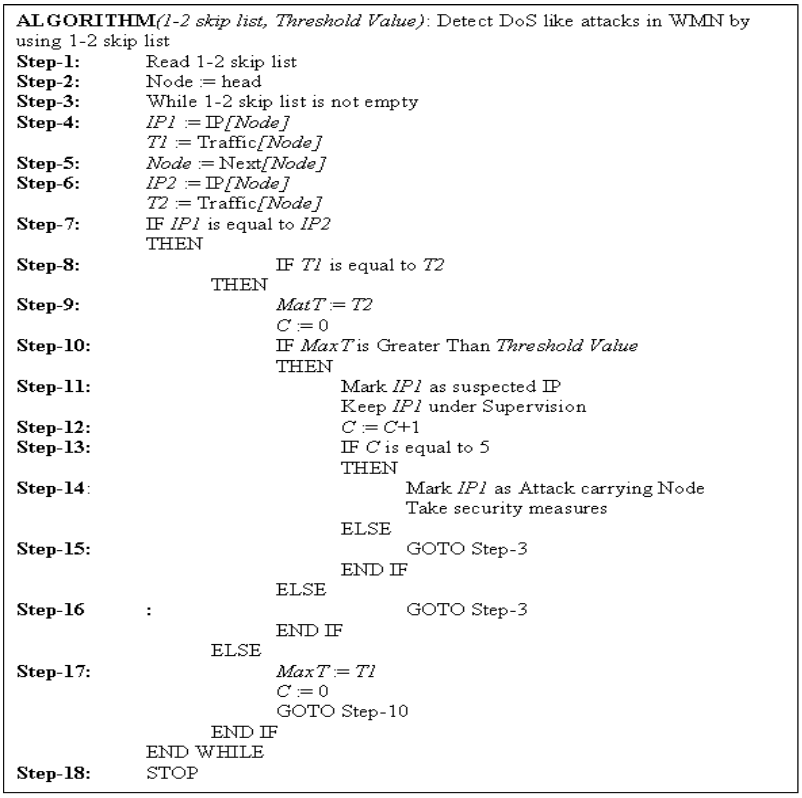


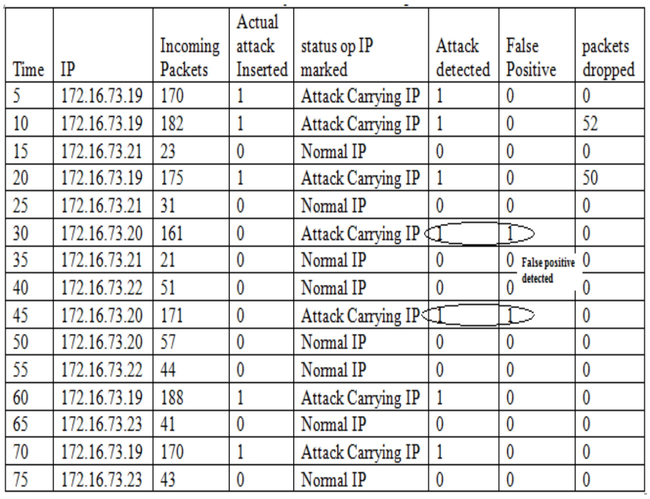
Figure 5: Flow chart to detect DoS like attacks in WMN by using 1-2 skip list



```
ALGORITHM(1-2 skip list, Threshold Value): Detect DoS like attacks in WMN by
using 1-2 skip list
Step-1:     Read 1-2 skip list
Step-2:     Node := head
Step-3:     While 1-2 skip list is not empty
Step-4:     IP1 := IP[Node]
            T1 := Traffic[Node]
Step-5:     Node := Next[Node]
Step-6:     IP2 := IP[Node]
            T2 := Traffic[Node]
Step-7:     IF IP1 is equal to IP2
            THEN
Step-8:                 IF T1 is equal to T2
                  THEN
Step-9:                 MatT := T2
                        C := 0
Step-10:                IF MaxT is Greater Than Threshold Value
                        THEN
Step-11:                      Mark IP1 as suspected IP
                              Keep IP1 under Supervision
Step-12:                      C := C+1
Step-13:                      IF C is equal to 5
                              THEN
Step-14:                            Mark IP1 as Attack carrying Node
                                    Take security measures
                              ELSE
Step-15:                            GOTO Step-3
                              END IF
                        ELSE
Step-16     :                       GOTO Step-3
                        END IF
                  ELSE
Step-17:                MaxT := T1
                        C := 0
                        GOTO Step-10
                  END IF
            END WHILE
Step-18:    STOP
```

Figure 6: Algorithm to detect DoS like attacks in WMN by using 1-2 skip list

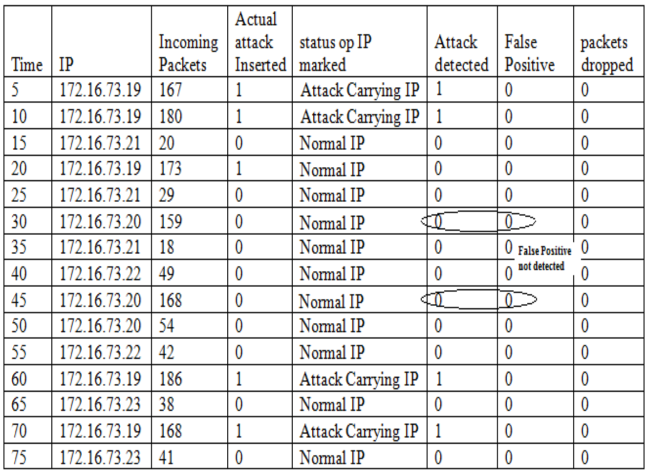
Table 2: Network Statistics in case of Queue and constant parameters of Network



Time	IP	Incoming Packets	Actual attack Inserted	status op IP marked	Attack detected	False Positive	packets dropped
5	172.16.73.19	170	1	Attack Carrying IP	1	0	0
10	172.16.73.19	182	1	Attack Carrying IP	1	0	52
15	172.16.73.21	23	0	Normal IP	0	0	0
20	172.16.73.19	175	1	Attack Carrying IP	1	0	50
25	172.16.73.21	31	0	Normal IP	0	0	0
30	172.16.73.20	161	0	Attack Carrying IP	1	1	0
35	172.16.73.21	21	0	Normal IP	0	0	0
40	172.16.73.22	51	0	Normal IP	0	0	0
45	172.16.73.20	171	0	Attack Carrying IP	1	1	0
50	172.16.73.20	57	0	Normal IP	0	0	0
55	172.16.73.22	44	0	Normal IP	0	0	0
60	172.16.73.19	188	1	Attack Carrying IP	1	0	0
65	172.16.73.23	41	0	Normal IP	0	0	0
70	172.16.73.19	170	1	Attack Carrying IP	1	0	0
75	172.16.73.23	43	0	Normal IP	0	0	0

False positive detected

Table 3: Network Statistics in case of 1-2 skip list and constant parameters of Network



Time	IP	Incoming Packets	Actual attack Inserted	status op IP marked	Attack detected	False Positive	packets dropped
5	172.16.73.19	167	1	Attack Carrying IP	1	0	0
10	172.16.73.19	180	1	Attack Carrying IP	1	0	0
15	172.16.73.21	20	0	Normal IP	0	0	0
20	172.16.73.19	173	1	Normal IP	0	0	0
25	172.16.73.21	29	0	Normal IP	0	0	0
30	172.16.73.20	159	0	Normal IP	0	0	0
35	172.16.73.21	18	0	Normal IP	0	0	0
40	172.16.73.22	49	0	Normal IP	0	0	0
45	172.16.73.20	168	0	Normal IP	0	0	0
50	172.16.73.20	54	0	Normal IP	0	0	0
55	172.16.73.22	42	0	Normal IP	0	0	0
60	172.16.73.19	186	1	Attack Carrying IP	1	0	0
65	172.16.73.23	38	0	Normal IP	0	0	0
70	172.16.73.19	168	1	Attack Carrying IP	1	0	0
75	172.16.73.23	41	0	Normal IP	0	0	0

False Positive not detected

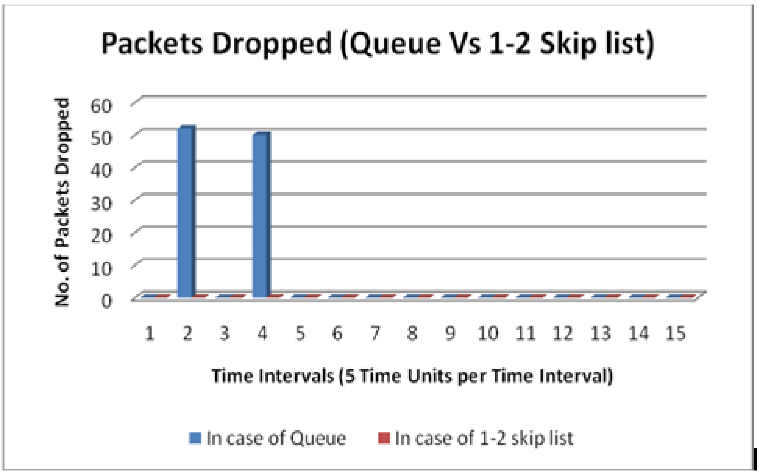


Figure 7: No of Packets dropped in Queue Vs 1-2 skip list implementation

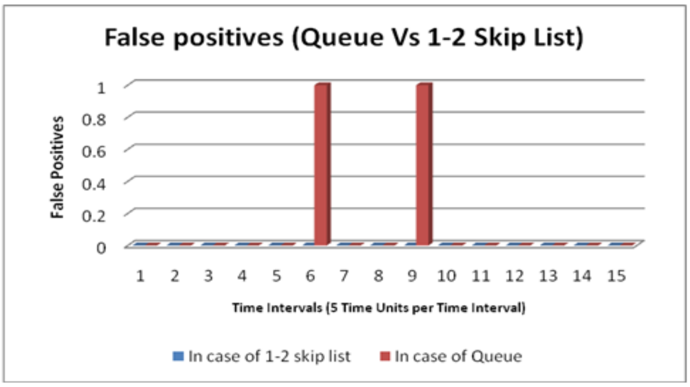


Figure 8: False Positives in Queue Vs 1-2 Skip List Implementation

6 CONCLUSION

In the current era, Ad Hoc computer Networks are having much importance in our day today life and Wireless Mesh Network is one of its types. The paper deals to explain WMN and the usage of 1-2 skip list to handle incoming traffic at Wireless Mesh Gateway node. It also explains that 1-2 skip list in place of linear queue is better to detect flooding or DoS type of attacks with an efficient manner. An appropriate and sufficient analysis with results is also provided in its support.

References

[1] Saini H., Sharma L. K., Panda T. C., and Pratihari H. N., “Extended Cell Planning for Capacity Expansion and Power Optimization by Using MEMETIC Algorithm,” *International Journal of Wireless Networks and Broadband Technology (IJWNBT)*, vol-2, Issue-2, pp. 36-46, 2012.

[2] Sharma L. K., Saini H., Panda T.C., and Pratihari H. N., “Taxonomy of Cell Planning,” *International Journal on reviews on Computing*, vol. 3, Issue-3, pp. 66-74, 2010.

[3] Cheng K. and Dasgupta P., “Weighted Voting Game Based Multi-Robot Team Formation for Distributed Area Coverage,” *in Proceedings of the 3rd International Symposium on Practical Cognitive Agents and Robots (PCAR '10)*. ACM, New York, NY, USA, pp. 9-15, 2010.

[4] Saini H., Sharma K. D., Dadheech P., and Panda T. C., “Enhanced 4-way Handshake Process in IEEE802.11i with Cookies,” *International Journal of Information & Network Security (IJINS)*, vol.2, No.3, pp. 229-238, 2013.

[5] Zhou Y., Wang Y., Ma J., Jia J., and Wang F., “A Low-latency GTS Strategy in IEEE802.15.4 for Industrial Applications,” *IEEE 2nd International Conference on Future Generation Communication and Networking*, pp. 411-414, 2008.

[6] IEEE 802.16 Working Group on Broadband Wireless Access. *http://wirelessman.org*

[7] Singh V. and Sharma V., “Efficient and fair scheduling of uplink and downlink in IEEE 802.16 OFDMA networks.” *Wireless Communications and Networking Conference, IEEE WCNC*, 2006.

[8] Cicconetti C., Lenzini L., Mingozzi E., and Eklund C., “Quality of service support in IEEE 802.16 networks. *IEEE Network*”, vol. 20, pp. 50-55, 2006.

[9] Cordero J. A., Yi J., and Clausen T., “Optimization of jitter configuration for reactive route discovery in wireless mesh networks,” *International Symposium on Modeling & Optimization in Mobile, Ad Hoc & Wireless Networks (WiOpt)*, 2013 11th, pp. 452- 459, 2013.

[10] Ahmed I, Mohammed A., and Alnuweiri H., “On the fairness of resource allocation in wireless mesh networks: a survey,” *Wirel. Netw.* 19, 6, pp. 1451-1468, 2013.

[11] Akyildiz I. F., Wang X. D., and Wang W. L., “Wireless Mesh Networks: A Survey,” *Computer Networks*, vol. 47, No. 4, pp. 445-487, 2005

[12] Nandiraju N.S., Nandiraju D. S., Cavalcanti D., Agrawal D.P., “A Novel Queue Management Mechanism for Improving Performance of Multihop Flows in IEEE 802.11s based Mesh Networks Performance,” *25th IEEE International on Computing, and Communications (IPCCC 2006)*, pp.161-168, 2006.

[13] Garcia-Luna-Aceves J.J., Menchaca-Mendez, and R. STORM, “A Framework for Integrated Routing, Scheduling, and Traffic Management in Ad Hoc Networks,” *IEEE Transactions on Mobile Computing*, vol. 11, No. 8, AUGUST 2012.

[14] Nandiraju N.S., Nandiraju D.S., Santhanam L., and Agrawal D.P., “A Cache Based Traffic Regulator for Improving Performance in WEEE 802.11s based Mesh Networks,” *IEEE Conference on Radio and Wireless Symposium*, pp. 293-296, 2007.

[15] Wikipedia, Skip-List, Retrieved on: Jan, 2014), Available at: *http://en.wikipedia.org/wiki/Skip_list*.

[16] William Pugh, “Skip lists: a probabilistic alternative to balanced trees,” *Communications of the ACM*, 33(6), pp. 668–676, 1990.

[17] Kim, Y. H., Lee, S.K., Koh, J. G., “Enhanced Synchronizing Packet Coalescing Mechanism for Improving Energy Efficiency in Ethernet Switch,” *International Journal of Smart Home*, vol. 7, No. 3, May, 2013.

Hemraj Saini received his PhD in Computer Science from Utkal University, Vani Vihar, Bhubaneswar (ODISHA), M.Tech. degree in Information Technology from the Punjabi University, Patiala, Punjab and B.Tech. in Computer Science & Engineering from National Institute of Technology, Hamirpur (H.P.). Since 1999, he has been actively engaged in Research, Teaching and academic Development activities. Currently he is attached with the Department of Computer Science & Engineering / ICT of Jaypee University of Information Technology, Wakanaghat INDIA. His main professional interests are in Cyber Defense, Software Testing, Enterprise Application Integration, Image processing and Intelligent Techniques. He has played an important role for organizing various National and International Conferences successfully funded by DST, Govt. of India, New Delhi, CSIR, Govt. of India, New Delhi and AICTE, Govt. of India, New Delhi. In addition to it he has published more than 45 research articles in various National/International Journal/Conferences of repute.