ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

A Simulation Based Security Evaluation through AODV against Black hole Attack in MANET Using Watchdog Module

N. Priya[1], S. Sri Gowtham[2]

Assistant Professor, Dept. of CSE, Bharath University, Chennai, Tamil Nadu, India[1,2]

ABSTRACT: Mobile Adhoc Network is an autonomous network used to form by create the nodes and establish the wireless connections dynamically, so that messages in that packets are going to sent from a sender to receiver. A number of routing protocols like Ad Hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), Destination-Sequenced Distance-Vector (DSDV) and Temporally Ordered Routing Algorithm (TORA) have been used. AODV is a prominent on-demand reactive routing protocol for mobile ad hoc networks. But in existing AODV, there is no security to against a well-known "Black Hole" attack. Black hole nodes are those malicious nodes that agree to forward packet to destination but do not forward packet intentionally. These black hole nodes activate in the network and degrade its performance. A watchdog mechanism is used to detect the blackhole nodes in a MANET. This method first detects a black hole attack and then gives a new route bypassing this node.Also in manet we activate the watchdog to improves its throughput and packet delivery ratio. We discuss the security attacks and two popular security techniques, Intrusion Detection System (IDS) and Watchdog and Path rater (WPR). The two techniques are evaluated using two measures, viz., Availability Factor (AF) and Integrity Factor(IF).We did simulations based security evaluation and intrusion prevention using the watchdog module based on above paramaters.Research is on going and also to indicate the possibilities to extend that.

KEYWORDS: AODV, Blackhole, MANET,Intrusion detection and prevention

I. INTRODUCTION

Mobile Adhoc Network (MANET) is popularly defined as a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. Unlike a wired network, nodes in an ad hoc network move freely, thus giving rise to frequent topology changes. MANETs can work independently or connected to the internet . Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks where, the structure of the network changes dynamically. In mobile ad-hoc networks where there is no infrastructure support and since a destination node might be out of range of a source node transmitting packets, a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. A base station can reach all mobile nodes without routing via broadcast in common wireless networks. , MANETs are formed on a continuous basis, to enhance its features through designing new algorithms and protocols.

II. OVERVIEW

A. MANET

A mobile node in a MANET has two functions, *viz*., as a host and a router. Communication of messages in packets is distributed among the nodes in a MANET; hence all nodes are Aco-operative and coordinations and there is no background network to control the operations. MANETs are formed in two layouts: single-hop and multi-hop. They differ in structure, im-plementation and the functionality cost. Formation of networks in MANET is a nonstop function of nodes and its topology and connectivity change quickly and continuously. These nodes can have access to a fixed infrastructure, as well. MANETs operate under different kinds of traffic that includes [1]: Peer-to-Peer when the communication occurs in one hop and steady traffic, Remote-to-Remote and stable route in a multi-hop network, so that

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

level of traffic depends on the stability of the route and dynamic traffic where the connectivity is poor. Another feature of MANET is that (i) its links fluctuate in capacity, (ii) network bandwidth is smaller than in fixed networks' and (iii) links are less stable. A multiple session [2] can be conducted in one end-to-end route. Moreover, the terminals in MANETs are light-weighted, so the algorithms that helps in carrying out the functions of the mobile nodes in MANET should be very effective to suit their low capabilities.

B. AODV

The AODV Routing protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets[3]. It employs destination sequence numbers to identify the most recent path. The major difference between AODV and Dynamic Source Routing (DSR) stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol, the source node floods the *RouteRequest* packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single *RouteRequest*.[4] The major difference between AODV and other on-demand routing protocols is that it uses a *destination sequence number*(DestSeqNum) to determine an up-to-date path to the destination. A node updates its path information only if the *DestSeqNum* of the current packet received is greater or equal than the last*DestSeqNum* stored at the node with smaller hopcount.[5] A RouteRequest carries souce*identifier* (SrcID),the *destinationidentifier* (DestID), *sourceseqnumber* (SrcSeqNum),the *destinationsequence number* (SrcSeqNum),the *destinationsequencenumber* (DestSeqNum), the *broadcast identifier* (BcastID), and the *time to live* (TTL) field. DestSeqNum indicates the freshness of the route that is accepted by the source. When an intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination. The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the RouteRequest packet.[6] If a RouteRequest is received multiple times, which is indicated by the BcastID-SrcID pair, the duplicate copies are discarded. All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send RouteReply packets to the source. Every intermediate node, while forwarding a RouteRequest, enters the previous node address and its BcastID. A timer is used to delete this entry in case a RouteReply is not received before the timer expires. This helps in storing an active path at the intermediate node as AODV does not employ source routing of data packets. When a node receives a RouteReply packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.[7]

C. BLACKHOLE ATTACK

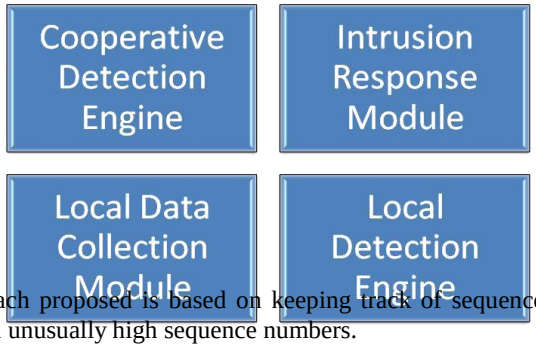
Black hole is one of the most serious attacks on a network layer, where a malicious node declares by itself that it has the shortest valid route to the targeted destination. When an another node trusts this node, and sends a message or packet to the malicious node, it either changes the contents before forwarding it or just drops it.[8] The black hole attack is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets.[9] In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have a fresh enough route to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination.[10] The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. Vulnerabilities of ad-hoc networks against black hole attacks are studied by different authors. Deng et.al. addresses the black hole problem and proposes a solution based on modification of the AODV protocol.[11] The authors propose to check the route through the next hop in the agreed upon path. This solution means that next hop information shall be added to the standard AODV header. Similar approach is adopted in where the nodes are asked to send their neighborhood sets once the route is established. In two solutions are proposed for detecting the black hole attack. in ad-hoc networks. First solution involves sending a ping packet to the destination to check the established route. If the acknowledgement does not arrive from the destination, presence of a black

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014



hole is deduced.[12] The other approach proposed is based on keeping track of sequence numbers as black holes usually temper with these sending packets with unusually high sequence numbers.

III.SECURITY TECHNIQUES

We discuss two effective techniques in MANETs in this section. Intrusion detection technique is a security violation detection scheme and watch-dog / pathrater is a security violation prevention technique.[13]

Intrusion detection technique: Intrusion detection System or (IDS) is a system that detects any abnormality in the network. A small chip or an electronic piece is attached to all devices protected by IDS. This technique is also used in wired networks; however that differs from an IDS in MANETs. This system can be applied on groups and individual nodes; however, it would be more efficient if it was implemented on a group of nodes an IDS applied to a MANET is illustrated.[14] Each node is capable of independent investigations, but they share and compare the information among them using an IDS agent implemented within each device, as mentioned before. Through this process, a node can obtain information about a wide range of the network, which will help in detecting any misbehaving in the network, tracing it and dealing with it before any node is harmed. Following Figure represents the internal structure of an IDS system. An IDS consists of four main modules.[15] The first module is the local data collection module. This module is responsible of gathering the information of the network and the surrounding entities that exists around a certain nod in the system.[16] The second module is the local detection engine that is responsible of analyzing the information that have collected by the local data collection module and recognizing any abnormality in the network[17].

This task can be done by observing the status of the network and report any suspicious changes. The third module is the cooperative detection engine, which become active when an abnormality is detected. It is responsible of sharing the information with the other nodes in the network, to compare this information and to identify the type of the intruder.[18] Once the intruder type is detected, the fourth module, which is intrusion response module, acts to protect the node through different ap-proaches depending on the type of the intrusion. This technique is effective in partially solving issues regarding decentralized management. However, IDS system con-sumes considerable power, which escalates threats due to limited
power supply.

Watchdog and path-rater: a watchdog and path-rater operation] in a MANET. These two techniques work in tandem to achieve prevention of a security violation and thus to provide a secure routing. Basically watchdog identifies misbehavior and path-rater rates nodes according to their reliability. Watchdog copies a packet and forwards it to a buffer, and then it sends the original packet to a node. After that, it snoops and checks if the node modified the packet[19]. If the packet forwarded without any modification, then the watchdog gets rid of the copy. In contrast, if the packet was modified, then the copy stays in the buffer for a certain time. If the time is out, the node will be marked as a suspicious node and if that behavior was repeated for a certain number of times, then the node is marked as malicious. After all of that, the information that the watchdog finds out go to the path-rater. The path-rater evaluates all the nodes that are in the same network that the path-rater's user is in and keeps these rates updated according to their behavior.[20] Then it chooses the best routes to use.

D. WATCHDOG MECHANISAM

In pending packet table, each node keeps track of the packets, it sent. It contains a unique packet ID, the address of the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

next hop to which the packet was forwarded, address of the destination node, and an expiry time after which a still-existing packet in the buffer is considered not forwarder by the next hop[21].

E. Simulation Model

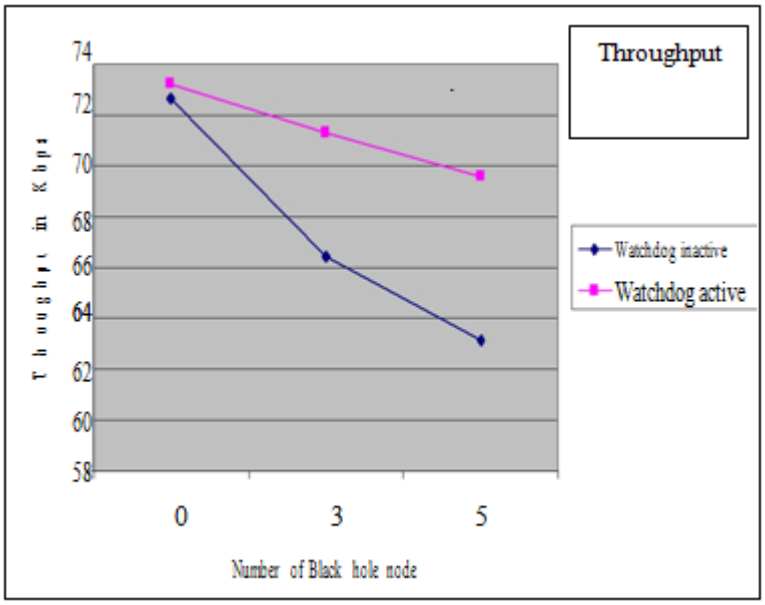
. We simulated a Uni-cast MANET using ns2 software. The simulation setting was an area of 2000m X 2000m and a random point way model with a node transmission range of 300 m were chosen. The experiments were repeated with two sets of 50 and 60 nodes and random partition attacks were induced using 0 to 10 malicious nodes in each set. We implemented algorithmic procedures for Intrusion detection system (IDS) and Watchdog and path rater (WPR). Availability and Integrity were used to evaluate the two security techniques. Availability factor (AF) and Integrity factor (IF) are the two proposed evaluation measures; *AF* is the ratio of the shortest distance between MANET sender and intended receiver to the actual distance between sender and intended receiver in MANET route. *IF* is the ratio of the number of error free packets in received message to the total number of packets in transmitted message.

Throughput*:* - It is the total number of received packet per unit time.Throughput = Total No. of packet received / Total traversing time

End-to-end delay*:* - This is defined as the delay between the time at which the data packet was originated at the source and the time it reaches the destination. Delay = Receiving time – Sending time

III. RESULTS AND DISCUSSIONS

In MANET first we calculate the normal mode behaviour for 5 nodes to calculate the throughput and end to end delay.if a black hole attack is affected the total throughput and delay.then we activate a watchdog it increases its throughput value.also try to reduce the blackhole effect.[22]



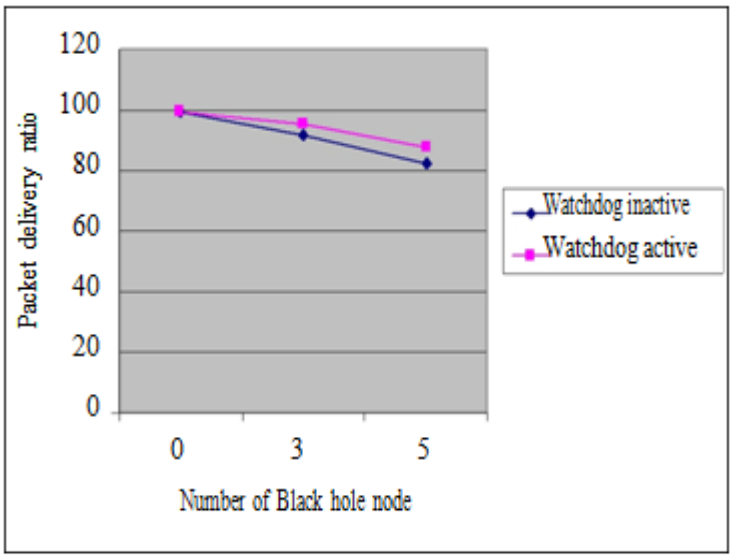
10.15680/ijircce.2014.0212096

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

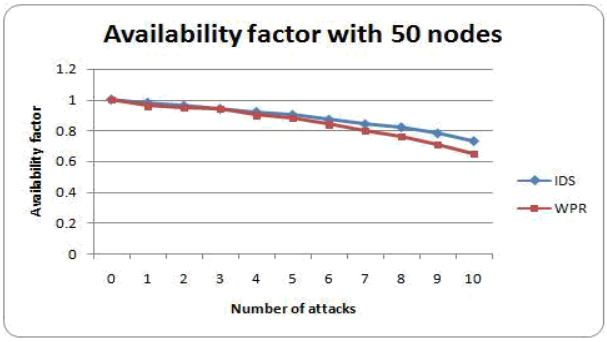
International Journal of Innovative Research in Computer and Communication Engineering

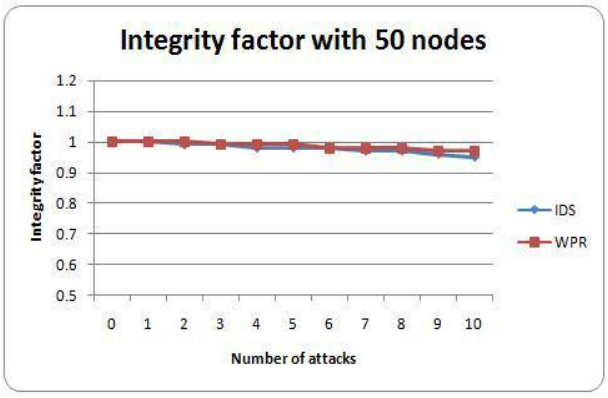
(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014



Figures indicate plots of Integrity factors of the security techniques (IDS and WPR) for a total number of 50 and 60 nodes in the domain, respectively. We observe that there is no significant difference in numerical performance factor. A more precise observation leads to a finding that WPR has a better IF measure than IDS in the simulated sets of attacks





IV. CONCLUSION

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Here discussed elaborately about several security attacks on MANETS, following brief discussions on the features, challenges in MANET implementation and some applications. Two more popular security detection and prevention tech-niques, namely Intrusion Detection system (IDS) and Watch-dog and Path rater (WPR) were considered for evaluations using two well defined security measures. The two measures that were considered were Availability factor and Integrity factor. Throughput and packet delivery ratio was calculated for existing AODV running for different scenarios having 0, 3 and 5 black hole nodes.Using same simulation parameter modified AODV was tested on above-mentioned networks having 0, 3 and 5 black hole nodes, for both watchdog active and inactive mode. The experimental results show that when the black hole nodes is increased up to 6% of total network nodes then in the presence of watchdog active throughput increases up to 3% to 8% for different scenarios. It is beneficial to adopt a particular security technique that suits an application requirement. Performance of security techniques to other types of attacks need to be further studied, which is our ongoing current work. We have also considered a Uni-cast MANET, whereas a multi-cast MANET is of equal practical relevance.

REFERENCES

1. J.-Z. Sun, “Mobile ad hoc networking: An essential technology for pervasive computing,” in Proceedings of International Conferences on info-tech and Info-net, 2001, pp. 316–321.
2. C. de Morais Cordeiro and D. Agrawal, “Mobile ad hoc networking,” Center for Distributed and Mobile Computing, ECECS, University of Cincinnati, 2002.
3. Kaliyamurthie K.P., Parameswari D., Udayakumar R., "QOS aware privacy preserving location monitoring in wireless sensor network", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4648-4652.
4. S. Yu, Y. Zhang, C. Song, and K. Chen, “A security architecture for mobile ad hoc networks,” in 18th Asia-Pacific Advanced Network Meeting, Cairns, 2004.
5. J. Karlsson, “Rotuing security in mobile ad-hoc (manet) networks,” International Research Seminar on Network Security and Next Generation Networks, Arcada University of Applied Sciences, September 2009.
6. Maitha Salem Al Mazrouei and Dr Sundaravalli Narayanaswami, FBCS” Mobile Adhoc Networks: A Simulation based Security Evaluation and Intrusion Prevention” 6th International Conference on Internet Technology and Secured Transactions, 2011
7. Irshad, W. Noshairwan, M. Shafiq, S. Khurram, E. Irshad, and M. Usman, “Security enhancement in manet authentication by checking the crl status of servers,” International Journal of Advanced Science and Technology, pp. 91–98, 2007.
8. R. H. Jhaveri, A. D. Patel, J. D. Parmar, and B. I. Shah, “Manet routing protocols and wormhole attack against aodv,” IJCSNS International Journal of Computer Science and Network Security, vol. 10, no. 4, pp. 12–18, April 2010.
9. Kanika Lakhani ,Himani bathla, Rajesh Yadav” A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET” IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010
10. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad-hoc networks: Challenges and solutions,” IEEE Wireless Communications, vol. 11, no. 1, pp. 38–47, 2004.
http://www.isi.edu/nsnam/ns/.-05.txt March 2000
11. Lidong Zhou, Zygmunt J.Hass, “Securing Ad Hoc Networks”, IEEE Special Issue on Network Security, vol-13, pp 24-30 Nov-Dec 1999
12. P.Ning and K.Sum, “How to misuse AODV: A case study of insider attack against mobile ad hoc routing protocol”, Tech Rep, TR- 2003-07, CS Department, NC University, April 2003
13. Sharmila D., Muthusamy P., "Removal of heavy metal from industrial effluent using bio adsorbents (Camellia sinensis)", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 5(2) (2013) pp.10-13.
14. L.Venkatraman and D.P. Agrawal, “Strategies for Enhancing Routing Security in Protocols for Mobile Ad Hoc Networks”, IEEE Network Magazine, vol. 13, no-6, Nov 1999
15. S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in
Proceedings of MOBICOM, Boston MA USA, pp 255-265 2000.
16. Udayakumar R., Khanaa V., Saravanan T., Saritha G., "Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 16(12) (2013) pp.1781-1785.
17. David B.Johnson and Dravid A. Maltz, “Dynamic Source routing in ad hoc wireless networks”,
Technical report, Carneigie Mellon University, 1996
18. M. Abolhasan, T. Wysocki, and Eryk Dutkiewicz, “A review of routing protocol for mobile ad hoc networks”, Technical report, University of Wollongong, 2003
19. Kalaiselvi V.S., Prabhu K., Ramesh M., Venkatesan V., "The association of serum osteocalcin with the bone mineral density in post menopausal women",Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 7(5) (2013) pp.814-816.
20. X. Hong, Kaixin Xu, and Mario Gerla, “Scalable routing protocols for mobile ad hoc networks”, IEEE Network Magazine, pp11-21, July-Aug 2002
21. Jayalakshmi T., Krishnamoorthy P., Kumar G.R., Sivamani P., "The microbiological quality of fruit containing soft drinks from Chennai", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 3(6) (2011) pp. 626-630.
22. V.D.Park and M.S.Corson, “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks,” Proc. INFOCOM, Apr-1997.
23. P.JENNIFER, DR. A. MUTHU KUMARAVEL, Comparative Analysis of advanced Face Recognition Techniques, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, pp 4917-4923 Vol. 2, Issue 7, July 2014

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

24 Dr.R.Udayakumar, Computer Simulation of Polyamidoamine Dendrimers and Their Complexes with Cisplatin Molecules in Water Environment, International Journal of Innovative Research in Computer and Communication, ISSN(Online): 2320-9801,pp 3729,25-30, Vol. 2, Issue 4, April 2014

25. DR.A.Muthu kumaravel, Mr. Kannan Subramanian, Collaborative Filtering Based On Search Engine Logs, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online): 2320-9801,pp 2432-2436, Vol. 2, Issue 1, January 2014

26 Dr.A.Muthu Kumaravel, Mining User Profile Using Clustering FromSearch Engine Logs, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online): 2320-9801,pp 4774-4778, Vol. 2, Issue 6, June 2014

27. P.Kavitha, Web Data High Quality Search - No User Profiling, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online):2320-9801,pp 2025-2030, Volume 1, Issue 9, November 2013