Using Merkle Tree to Mitigate Cooperative Black-hole Attack in Wireless Mesh Networks

Shree Om
Department of Computer Science
University of Botswana
Gaborone, Botswana

Mohammad Talib
Department of Computer Science
University of Botswana
Gaborone, Botswana

Abstract— **Security is always a major concern and a topic of hot discussion to users of Wireless Mesh Networks (WMNs). The open architecture of WMNs makes it very easy for malicious attackers to exploit the loopholes in the routing protocol. Cooperative Black-hole attack is a type of denial-of-service attack that sabotages the routing functions of the network layer in WMNs. In this paper we have focused on improving the security of one of the popular routing protocols among WMNs, Ad-hoc on demand distance vector (AODV) routing protocol and present a probable solution to this attack using Merkle hash tree.**

Keywords- WMN, MANET; Cooperative black-hole attack; AODV; Merkle tree; malicious; OWHF.

I. INTRODUCTION

A black-hole attack is a network layer denial-of-service (DoS) attack that exploits the route discovery process of on-demand routing protocols. The network layer of WMN defines how interconnected networks (inter-networks) function. The network layer is the one that is concerned with actually getting data from one computer to another even if it is on a remote network. It is at this layer that the transition really begins from the more abstract functions of the higher layers – which do not concern themselves as much with data delivery – into specific tasks required to get its data to the destination. Its job is to provide a best-efforts (i.e., not guaranteed) way to transport data-grams from source to destination, without regard to whether these machines are on the same network or whether there are other networks in between them. This whole communication is made possible through the use of Internet Protocol (IP). IP is the primary network protocol used on the internet. IP is a connectionless protocol. IP supports unique addressing for computers on a network. Most networks use the IP version 4 (IPv4) standard that features IP addresses four bytes (32 bits) in length. The newer IP version 6 (IPv6) standard features addresses 16 bytes (128 bits) in length. All in all, the point that we are trying to make here is that IP is the network layer protocol that holds the whole internet together and intruders love to interrupt the functions of this layer. You can imagine the seriousness of the damage caused if an intruder is able to sabotage the functions of this layer.

The aim of this paper is to reflect light on Cooperative Black-hole attack, a serious form of Black-hole attack and the challenges with its security mechanisms. Section II presents threats and attacks at network. Section III takes a look at Cooperative Black-hole attack, section IV presents related works against the attack and challenges, section V gives the problem statement, section VI, gives background on the hashing tree, section VI discusses a probable solution, section VIII highlights expected results and section IX discusses future work.

II. THREATS AND ATTACKS AT NETWORK LAYER

We expect a secured WMN to have accomplished objectives such as confidentiality, integrity, availability, authenticity, non-repudiation, authorization and anonymity. In this section, some of the most critical threats and attacks present at network layer are discussed.

A. *Black-hole attack:*

In this attack, the malicious node always replies positively to a route request from a source node although it may not have a valid route to the destination and will always be the first to reply to the route request message. Therefore, all the traffic from the source node will be directed toward the malicious node, which may drop all the packets, resulting in DoS [1].

B. *Wormhole attack:*

To launch this attack, an attacker connects two distant points in the network using a direct low latency communication link called the wormhole link. Once the wormhole-link is established, the attacker captures wireless transmission on one end, sends then through the wormhole link, and replays them at the other end [8]. Then the attacker starts dropping packets and cause network disruption. The attacker can also spy on the packets going through, use the information gained to launch new attacks, and thus compromise the security of the network.

C. *Sink-hole attack:*

In this attack, a malicious node can be made very attractive through the use of powerful transmitters and high-gain antennas to the surrounding nodes with respect to the routing algorithm [15].

D. *Sybil Attack:*

This attack is defined as a “malicious device illegitimately taking on multiple identities” [4]. This attack abuses the path diversity in the network used to increase the available bandwidth and reliability. The malicious node creates multiple identities in the network. The legitimate nodes, assuming these identities to be distinct network nodes, will add these identities in the list of distinct paths available to a particular destination thus including the malicious node on path of a data, which can affect packet transfer as well as drop them. But, Even if the malicious node does not launch any attack, the advantage of path diversity is diminished, resulting in degraded performance [15].

A summary table has been drawn below that show the comparison of the above mentioned attacks based on the following properties:

1) *Type of attack:* Four types: Masquerade, Replay, Modify, and DoS attack [12].
2) *Type of attacker:* internal attacker or external attacker.
3) *Required knowledge:* The amount of information needed to be gathered or collected from the network in order to effectively perform the attack.
4) *Cost:* The cost of running an attack, not necessarily economic, but also measured in terms of resources or time requirements.
5) *Detectability:* An attack on the network layer or routing protocols is desired to be as less detectable as possible.

TABLE I. COMPARISON OF ATTACKS AT NETWORK LAYER

Attack	**Type of Attacker**	**Type of Attack**	**Required Knowledge**	**Cost**	**Detectability**
Black-hole	Insider	DoS	Low	Low	High
Wormhole	Insider & Outsider	Modify & Dos & Replay	High	High	Low
Sink-hole	Insider	Modify & DoS	Medium	Medium	Low
Sybil	Insider	Masquerade & DoS	Low	Medium	Low

As we see in the table, a black-hole attack will be favoured by most attackers because any attacker whose intentions are to bring down the whole network communication at a low cost with least amount of information about the network can carry out this attack. The detectability is surely higher than other attacks and that is why a more complex form of Black-hole attack called Cooperative Black-hole attack which is hard to detect, is being carried out by attackers. The next section takes a look in to this form of Black-hole attack.

III. Cooperative Black-Hole Attack

Since, WMNs share common features with the wireless ad-hoc networks, the routing protocols developed for MANETs can be applied to WMNs. In this paper, we focus on AODV and we explain operation of black-hole and cooperative black-hole attack by using AODV as an example protocol.

Black-hole attack is a type of active attack. These attacks involve some modification of the data stream or the creation of a false stream [12]. Figure 1 below show a simple scenario of this attack with one malicious node.

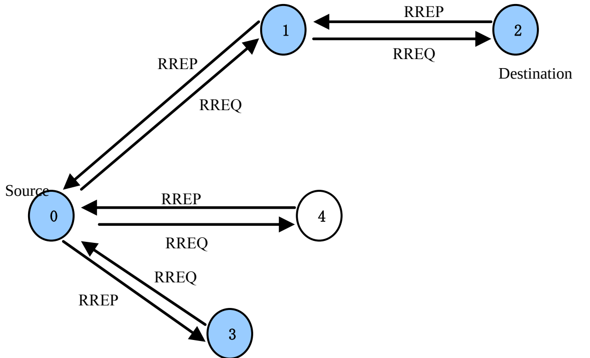
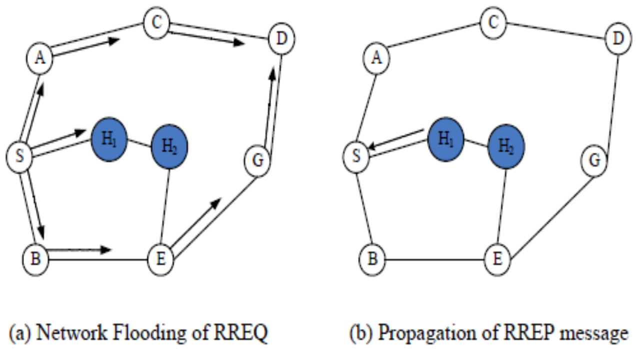


Figure 1. Black-hole attack in progress

The core functionality of WMNs is the routing capability and attackers take advantage of the shortcomings as the routing protocol has some loop holes. The AODV protocol is vulnerable to the well-known black hole attack. AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes. In case of multiple routes, a node selects the route with the highest sequence number. If multiple routes have the same sequence number, then the node chooses the route with the shortest hop count. A malicious node sends Route Reply (RREP) messages without checking its routing table for a fresh route to a destination. As shown in fig. 1 above, source node 0 broadcasts a Route Request (RREQ) message to discover a route for sending packets to destination node 2. A RREQ broadcast from node 0 is received by neighbouring nodes 1, 3 and 4. However, malicious node 4 sends a RREP message immediately without even having a route to destination node 2. A RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighbouring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them on.

A more complex form of the attack is a Co-operative Black Hole Attack where multiple malicious nodes collude together resulting in complete disruption of the routing and packet forwarding functionality of the network. For example, in figure 2, when multiple black hole nodes are acting in coordination with each other, the first black hole node H1 refers to one of its team-mates H2 as the next hop. According to the proposed methods in [3], the source node S sends a further request message to ask H2 if it has a routing to node H1 and a routing to destination node D. Because H2 is cooperating with H1, its further reply is “yes” to answer both the questions. So source node S starts passing the date packets. Unfortunately, in reality, the packets are abstracted by node H1 and the security of the network is compromised [10].



(a) Network Flooding of RREQ (b) Propagation of RREP message

Figure 2. Figure 2. Co-operative Black-hole attack [16]

IV. Related Works and Challenges

AODV does not incorporate any specific security mechanism, such as strong authentication. Therefore, there is no straightforward method to prevent mischievous behaviour of a node such as media access control (MAC) spoofing, IP spoofing, dropping packets, or altering the contents of the control packets.

Solutions have been proposed to mitigate black-hole nodes in [2, 3, 10]. However, the solution, which are designed for MANETs consider malicious nodes that work alone, i.e., each node is an attacker, and do not target attackers working in groups. For example, method proposed in [3] can help mitigate individual node attack because it requires the intermediate node to include information about the next hop to destination in the RREP packet. Then after the source node has received this packet, it sends a further route request (FREQ) to the next hop node asking if the node has route to the destination. Now, if this next hop node has been working together with the malicious node, then it will reply "yes" to the FREQ and the source node will transmit the packet to the malicious node that sent the first reply which is a black-hole node. A solution to defending cooperative black-hole attacks was proposed in [10] but no simulations or performance evaluations had been done. The methodology uses the concept of Data Routing Information (DRI) table and cross-checking further request (FREQ) and further reply (FREP). [14] have used the algorithm proposed by [10] and modified it slightly to improve the accuracy of preventing the attack and efficiency of the process and simulated the new modified algorithm. The solution has been proposed for MANETs which are usually mobile devices powered by battery. The maintenance of DRI increases overhead and cross-checking delays the communication process which in-turn drains more battery power. However [14] have compared their results with [3] and proved that their method is more efficient and accurate. Two authentication mechanism for identifying multiple black hole nodes cooperating as a group in MANETs is proposed by [16]. The mechanism is based on the assumption that no other authentication mechanism such as a Public Key Infrastructure (PKI) is present which is usually not practical in MANETs. The source node checks the RREP messages to determine the data packets to pass with the authentication mechanisms proposed in [16]. However, the question that arises is, how will this authentication mechanism be protected from malicious nodes that might forge the reply if the hash key of any node is to be disclosed to all nodes. In [13], authors propose an enhancement of the basic AODV routing protocol to combat the cooperative black hole attack in MANET. They use a structure, which they call fidelity table wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a black hole node and is eliminated. In their approach, they assume that nodes are already authenticated which is a little strong assumption. [2] present a solution to avoid single node and co-operative Black-hole attacks in a MANET based on the principle of Merkle tree. However, factors such as network density, nodes mobility and the number of black hole nodes which are determining factors in a solutions performance, in term of end to end delay and network load, were not considered.

V. Problem Statement

The state-of-the-art work is still insufficient for deploying sizeable WMNs because important aspects such as security still remain open problems. Cooperative black-hole attack is a severe denial-of-service attack routing protocol threat, accomplished by dropping packets, which can be easily employed against routing in Wireless Mesh Networks, and has the effect of making the destination node unreachable or downgrade communications in the network. The black holes are invisible and can only be detected by monitoring lost traffic. The emergence of new applications of WMNs necessitates the need for strong privacy protection and security mechanisms of WMNs. The AODV, our case study protocol, does not have any security mechanisms and malicious nodes can perform many attacks by taking advantage of the loopholes in the protocol. The next section proposes a solution to prevent Cooperative black-hole attack in hybrid WMNs.

A solution is proposed by [2] to black-hole and cooperative black-hole attack in MANETs based on the principle of Merkle tree but has challenges. Our solution uses its fundamentals and makes modifications to address these challenges and helps mitigate Cooperative black-hole attack in hybrid WMNs. Before we get in to the description of the solution, we would like to give a brief background of Merkle Tree.

VI. MERKLE TREE

Also called Merkle hash tree (MHT) is a binary tree relies on the properties of one way hash functions (OWHFs) [7]. A sample MHT is shown in figure 3.

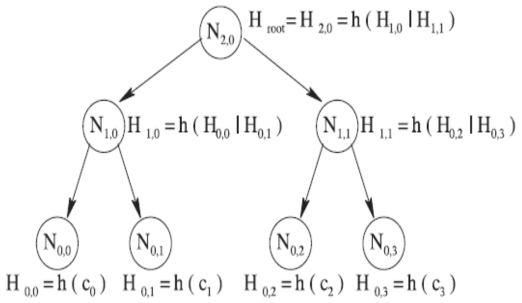


Figure 3. A sample MHT [7]

- N_{ij} denotes the nodes within the MHT where *i* and *j* represent, respectively, the *i*-th level and the *j*-th node.
- H_{ij} denotes the cryptographic variable.
- *h* denotes a one way hash function e.g. the function SHA-1 [6].
- | is the concatenation operator.
- Nodes at level 0 are called "leaves".
- Each leaf carries a given value e.g. $h(C_0)$, $h(C_1)$, $h(C_2)$ and $h(C_3)$ in Fig. 3.
- The value of an interior node (including the root) is a one-way hash function of the node's children values e.g. value of interior node $N_{1,0}$ is: $h(\ H_{0,0} \mid H_{0,1})$ which is the hashing result of the concatenation of values of children $N_{0,0}$ and $N_{0,1}$.

VII. The Proposed Solution

Table 3 contains the notations used to describe the solution.

TABLE II. NOTATIONS

Notation	Significance
IDi	Identity of node i.
Si	Secret generated by node i.
h	OWHF
|	Concatenation operator

In figure 4, we consider a piece of network made up of 4 nodes A, B, C and D. On this last, a Merkle tree is juxtaposed. We point out that our goal is to check that B and C conveys well, towards D, the traffic sent by A.

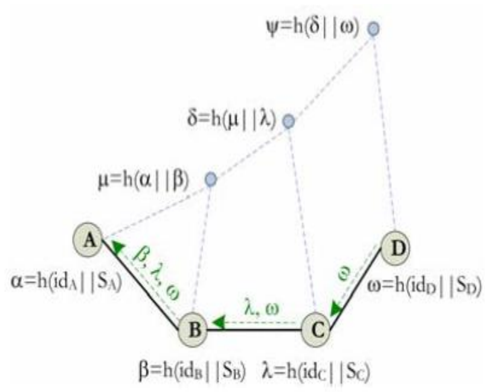


Figure 4. Basic principle of the solution [2].

Node A is source node and has the value ψ (value of the root of the Merkle tree). Each node *i* holds the value $h(id_i \mid S_i)$. So as per method proposed by [2], if A has to send data to D through B and C, in order to make sure that B and C are not cooperating as black hole nodes D sends ω (value held by D) to C, then C sends λ and ω to B which in turn sends β, λ and ω to A. A then recalculates ψ from α, β, λ and ω, then compares the result with the value ψ of already held, if equality, the route (A,B,C,D) is secured, otherwise, the route contains a black hole node.

Nodes B and C can cooperate to conduct black hole attack, this is easy if D communicates to C its secret S_D based on trust and since C is cooperating with B, it will pass the secret S_D to B so that it can calculate ω. [2] have not addressed this problem as how to protect the secret S_i from being compromised. This could create problems in dense network. Our solution adds to [2]. When A requests for a route to D, B being an attacker replies with the highest sequence number to A. According to AODV, A would discard other RREPs. Our solution looks to modify AODV such that it records the second best RREP from the node claiming to have a route to D. We assume that this node is safe. We call this node X. Node X has the value θ which is equal to $h(id_x \mid S_x)$. Since B already has β, λ and ω, it forwards all these values to A without any further communication with C (assumption). We introduce change of secret on the source and destination node whenever there is a request for the hash value. That means that when D sends ω to node X, it is a completely different value from the value of B. But B did not even communicate with C or D. Similarly, A would hold a new ψ and new α. Now, when A recalculates ψ from new α, β, λ and ω, then compares the result with the new value of ψ, it would be different but when A recalculates ψ from new α, θ and new ω and compares the result with the value ψ, they will be same. This would mark node B to be a malicious node and it will be black listed from future communication. At the same time a update will be sent with the packet to D through node X informing it of the malicious behavior of B. D will black list node C because it never received any RREQ from it because B never communicated with C which should not have been the case if both nodes were trusted.

The steps below give a rough idea of how the solution will work assuming node D has already shared its secret with node C and node C has forwarded is secret to node B along with secret of node D.

Step 1: Source node A sends RREQ for destination D.
Step 2: Source node A updates its value of ψ and generates new secret for itself.
Step 3: Intermediate node B sends RREP with highest sequence number.
Step 4: Node A stores this information.
Step 5: RREP from node X is received after RREP from node B.
Step 6: Instead of discarding this RREP, node A temporarily stores this information
Step 7: In order to prove legitimacy, node B and node X have to send the hash values including that of destination D.
Step 8: Node X requests for ω from node D.
Step 9: Node D generates new secret, recalculates new ω and passes it to node X.
Step 10: Node X passes θ and new ω to node A.
Step 11: Node B passes β, λ and old ω (calculated on the basis of secret of D sent by node C).
Step 12: Node A recalculates two values of ψ, ψ1 based on values from node B and ψ2 based on values from node X.

Step 13: Node A compares ψ1 and ψ2 to already held new value ψ.
Step 14: Node A discovers ψ1 is not the same as new ψ.
Step 15: Node A black lists node B.
Step 16: Node A sends packet to node X to be delivered to node D with attached information about node B.
Step 17: Node D receives packet.
Step 18: Node D black lists node B.
Step 19: Node D black lists node C based on assumption that node B was able to calculate ω because node C must have shared secret with node B, hence making node C an untrusted node.
Step 20: Node D sends acknowledgement (ACK) packet to node A including information about untrustful behaviour of node C.
Step 21: Node A updates its list of black listed nodes and adds node C to it.

VIII. Expected Results

The method would successfully identify the colluding malicious nodes and when compared with other proposed methods would have

- Better packet delivery ratio (PDR) – the number of packets generated by the sources vs. the number of packets received at the destination.
- Reduced detection time - This is the time to detect the network, which has a black hole attack, measured by the attack detection time minus the traffic start time [14].
- Better average end-to-end delay - this is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver and includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc [9]. It is measured in milliseconds.
- Reduced routing overhead – ratio of number of control packets generated to the data packets transmitted.

IX. Future Work

In this paper we have studied the routing security issues of WMNs, described the Cooperative black hole attack that can be mounted against a WMN and proposed a possible solution for it in the AODV protocol. The proposed solution can be applied to identify multiple black hole nodes cooperating with each other in a hybrid WMN. As future work, we intend to develop concrete algorithms and simulations to analyze the performance of the proposed solution based on network density, nodes mobility and the number of black hole nodes.

References

[1] I. Aad, P. J. Hubaux, W. E. Knightly, “Impact of denial-of-service attacks on ad-hoc networks,” IEEE/ACM Trans. Net. USA, vol. 16, iss. 4, pp. 791-802, August 2008.
[2] A. Baddache, A. Belmehdi, “Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks,” Int. J. of Comp. Sc. and Info. Sec. (IJCSIS). USA, vol. 7, iss. 1, pp. 10-16, January 2010.
[3] H. Deng, W. Li, P. D. Agarwal, “Routing security in wireless ad-hoc networks,” IEEE Comm. Mag. USA, vol. 40, iss. 10, pp. 70-75, December 2002
[4] M. Imani, M. E. Rajabi, M. Taheri, M. Naderi, “Vulnerabilities in network layer at WMN,” Int. Conf. on Ed. and Net. Tech. China, pp. 487-492, June 2010.
[5] J. Yin, S. Madria, “A hierarchical secure routing protocol against black hole,” IEEE Int. Conf. on Sensor Net., Ubiquitous, and Trustworthy Computing. Taiwan, vol. 1, pp. 376-383, June 2006.
[6] R. C. Merkle, “A certified digital signature,” Advances in Crypt. (CRYPTO89) USA, pp 218-238, August 1989.
[7] L. J. Munoz, J. Forne, O. Esparaza, M. Soriano, “Certificate revocation system implementation based on the Merkle hash tree,” Int. J. of Info. Sec. Heidelberg, vol. 2, iss. 2, pp. 110-124, January 2004.
[8] F. Nait-Abdesselam, B. Bensaou, T. Taleb, “Detecting and avoiding wormhole attacks in wireless ad-hoc networks,” IEEE Comm. Mag. Canada, vol. 4, iss. 64, pp. 127-133, April 2008.
[9] S. S. Ramaswami, S Upadhyaya, “Smart handling of colluding black hole attacks in MANETs and wireless sensor networks using multipath routing,” IEEE workshop on Info. Assurance. USA, pp. 253-260, July 2006.
[10] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, K. Nygard, “Prevention of cooperative black hole attack in wireless ad hoc networks,” Int. Conf. on Wireless Net. USA, vol. 1, pp. 570-575, June 2003.
[11] S. M. Siddiqui, S. C. Hong, “Security issues in wireless mesh networks,” IEEE Inter. Conf. on Multimedia and Ubiquitous Eng. (MUE'07). South Korea, vol. 1, pp. 717-722, April 2007.
[12] W. Stallings, Network security essentials: Applications and Standards. New Jersey, USA: Prentice Hall, 2003
[13] L. Tamilselvan, V. Sankarnarayanan, “Prevention of blackhole attack in MANET,” Int. Conf. on Wireless Broadband and Ultra Wideband Comms. Australia, vol. 2, pp. 21, April 2007.
[14] H. Weerasinghe, H. Fu, “Preventing cooperative black hole attacks in mobile ad hoc networks: simulation implementation and evaluation,” Future Gen. Comm. and Networking (FGCN). South Korea, pp. 362-367, December 2007.
[15] V. Zhang, J. Zheng, H. Hu, Security in wireless mesh networks. Florida, USA: Auerbach Publications, 2009
[16] M. Zhao, J. Zhou, “Cooperative black hole attack prevention for mobile ad hoc networks,” IEEC '09 Proceedings of the 2009 Int. Symp. on Info. Engg. and Elec. Commerce. USA, vol. 1, pp. 26-30, May 2009
[17] Bhakthavathsalam, R., Shashikumar, R., Kiran, V., & Manjunath, Y. R. (2010). Analysis and Enhancement of BWR Mechanism in MAC 802 . 16 for WiMAX Networks. International Journal of Advanced Computer Science and Applications - IJACSA, 1(5), 35-42.
[18] Prasad, D. (2011). A Reliable Security Model Irrespective of Energy Constraints in Wireless Sensor Networks. International Journal of Advanced Computer Science and Applications - IJACSA, 2(4), 20-29.
[19] Jaigirdar, F. T. (2011). Grid Approximation Based Inductive Charger Deployment Technique in Wireless Sensor Networks. International Journal of Advanced Computer Science and Applications - IJACSA, 2(1).

Authors Profile

Shree Om received his B.Sc. degree in computer engineering from University of South Alabama, USA in 2007. He is currently pursuing M.Sc. in Information Systems at University of Botswana, Botswana. His research interests are in the networking field particularly in mesh networking. He has attended several workshops conferences locally and internationally.

Professor Mohammad Talib has, presently, been associated with the Computer Science Department of the University of Botswana and has also been an adjunct professor at a couple of Universities in the United States. He has worked at a number of universities all across the globe in different capacities besides India where he remained the Head of the Department of Computer Science. He has an excellent industrial relevance and has worked as Software Engineer in the Silicon Valley at California for a significant period of time. He has been a Consultant for several software development companies and handled various small and big projects all across the world. He was conferred upon a degree of the Doctor of Philosophy (Ph.D.) in computer science & Engineering with specialization in computer vision from the prestigious University of Lucknow in India with Certificate of Honor. Besides PhD, he is also flanked by an M.S. in Computer Science, M.Sc. in Statistics and a PG Diploma in Computing. He has supervised over a dozen Master and four PhD students in different areas of Computer Science, Business and IT. His research areas include Bio informatics, Computer Vision, and Robotics. Presently, he is working on a two way interactive video communication through the virtual screen with the essence of smell. He has about eighty research papers published in different world class journals and conferences besides a book. He is also credited with over 300 publications including (under)graduate project reports, thesis, extension articles, study guides, edited research papers, books, etc. besides a minimum of 50 Industrial training supervision reports all across the world. He has chaired and remained member of various Academic Councils, Board of Studies, Academic and Advisory Boards, Examination Committees, Moderation and Evaluation Committees worldwide. He is the Member of the Editorial Board of about a dozen International Journals. He has also been associated with a number of international computer societies, associations, forums, conferences etc. in various capacities. He is conferred upon an honorary doctorate in computer science and engineering by the Yorker International University, USA