Avoidance of Black Hole Attack in Virtual Infrastructure for MANET

R. Kesavan
Research Scholar
St. Peter's University
Chennai

V. Thulasi Bai
Phd,Dean, R & D
Prathyusha Institute of Technology and Management, Chennai

ABSTRACT
A Mobile Ad-Hoc Network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on continual basis. Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. Virtual Infrastructure achieves reliable transmission in Mobile Ad Hoc Network. Black Hole Attack is the major problem to affect the Virtual Infrastructure. A black hole attack is a severe attack that can be easily employed against routing in mobile ad hoc networks. A black hole is a malicious node that falsely replies for any route requests without having active route to specified destination and drops all the receiving packets. In this paper, we give an algorithmic approach to focus on analyzing and improving the security of AODV, which is one of the popular routing protocols for MANET. Our aim is on ensuring the security against Black hole attack. The proposed solution is capable of detecting Black hole node(s) in the MANET at the beginning and a solution to discover a safe route detects cooperative black hole attack.

General Terms
Virtual Infrastructure, Vulnerabilities, Grouped Malicious Nodes

Keywords
Mobile Ad-Hoc network, AODV, Black Hole, Security, Routing.

1. INTRODUCTION
Today, people move and communicate a lot, in addition, they need new technologies, enabling them to quickly and easily retrieve various types of information and communicate with distant people. So, ad-hoc networks have emerged to meet these new needs. They are mobile radio networks without the aid of a fixed infrastructure or a centralized administration which allow them to be deployed easily as scalable.

MANETs have some special characteristic features such as unreliable wireless media (links) used for communication between hosts, constantly changing network topologies and memberships, limited bandwidth, battery, lifetime, and computation power of nodes etc. While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are absent or less severe in wired networks. MANETs are vulnerable to various types of attacks. These include passive eavesdropping, active interfering, impersonation, and denial-of-service. Intrusion prevention measures such as strong authentication and redundant transmission can be used to improve the security of an ad hoc network. However, these techniques can address only a subset of the threats. Moreover, they are costly to implement. The dynamic nature of ad hoc networks requires that prevention techniques should be complemented by detection techniques, which monitor security status of the network and identify malicious behavior. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes in a MANET may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. One of the most widely used routing protocols in MANETs is the *ad hoc on demand distance vector* (AODV) routing protocol [1]. It is a source initiated on-demand routing protocol. However, AODV is vulnerable to the well known black hole attack. In [2], the authors have assumed that the black hole nodes in a MANET do not work as a group and have proposed a solution to identify a single black hole. However, their proposed method cannot be applied to identify a cooperative black hole attack involving multiple malicious nodes. In this paper, a mechanism is proposed to identify multiple black hole nodes cooperating as a group in an ad hoc network. The proposed technique works with slightly modified AODV protocol and makes use of the *data routing information table* in addition to the cached and current routing table.

2. AODV ROUTING PROTOCOL
The Ad Hoc On-demand Distance Vector (AODV) routing protocol is an adaption of the DSDV protocol for dynamic link conditions [1][6]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with the routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route REPly) packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet.

Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules.

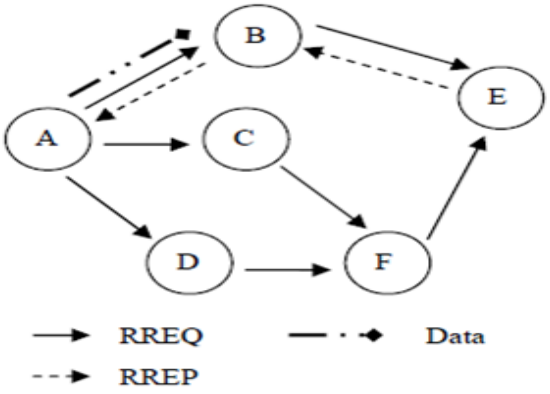

Fig 1: Propagation of RREQ & RREP from A to E

3. MANET VULNERABILITIES:

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

- Lack of Centralized Management
- Resource availability
- Scalability
- Cooperativeness
- Dynamic topology
- Limited power supply

4. SECURITY GOALS

Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self organizing manner. For these reasons, securing a mobile ad-hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

- Availability
- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Anonymity

5. SECURITY ATTACKS

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. [4]Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital / cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

5.1 Passive Attacks

Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected.

5.2 Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. Active attacks can be internal or external.

5.2.1 External attacks are carried out by nodes that do not belong to the network.

5.2.2 Internal attacks are from compromised nodes that are part of the network.

Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication.

- Black hole.
- Gray hole
- Worm hole
- Jellyfish attack
- Spoofing.
- Sybil attack

6. GROUPED BLACK HOLE ATTACK

A Black Hole attack [2][8][20] is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. Co operative Black hole means the malicious nodes act in a group [18][19].

The Black Hole attack has two phases. In the first phase, the malicious node exploits the ad hoc routing protocol such as AODV to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the attacker node drops the intercepted packets without forwarding them. There is a more subtle form of this attack when an attacker node suppresses or modifies packets originating from some nodes, while leaving the data packets from other nodes unaffected. This makes it difficult for other nodes to detect the malicious node. In his work, however, a defense mechanism has been proposed against a cooperative black hole attack in a MANET that relies on AODV routing protocol.

Researchers [2] [7] [9] have proposed many solutions, which avoid the black hole attack in certain degree. However those methods only identify and eliminate a single black hole node [10]. And the case of multiple black hole nodes acting in coordination has not been addressed. As an example, consider the following scenario in figure 2.

Here node S is the source node and D is the destination node. Nodes 1 to 5 act as the intermediate nodes. Nodes 4 (B1) and 5 (B2) act as the cooperative Black holes. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole B1 reaches the source node, well ahead of the other RREPs, as it can be seen from the figure 2. Now on receiving the RREP from B1, the source starts transmitting the data packets. On the receipt of data packets, B1 simply drops them, instead of forwarding to the destination or B1 forwards all the data to B2. B2 simply drops it instead of forwarding to the destination. Thus the data packets get lost and hence never reach the intended destination

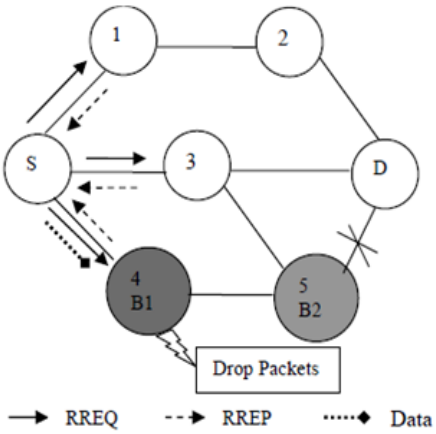

Fig 2: Black Hole Attack

7. RELATED WORK

A MANET is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. However, in [11],[1] many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security. The existing security solutions of wired networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks. In this paper, we have discussed current routing attacks in MANET.

Some solutions in [11,1,3] work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. In addition, some may require special hardware such as a GPS or a modification to the existing protocol. The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail.

M.A. Shurman [14] in his work proposed for source node to verify the authenticity of the node that initiates the RREP messages by finding more than one route to the destination, so that it can recognize the safe route to destination. This method can cause routing delay, since a node has to wait for a RREP packet to arrive from more than two nodes. Due to this, Dokurer [15] has proposed a solution based on ignoring the first established route to reduce adverse effects of Black hole attack. His assumption is based on the fact that the first RREP message that arrives at a node would normally come from a malicious node. Unfortunately, this method has some limitations. For instance, the second RREP message received at a source node may also come from malicious node if the real destination node is nearer to the source node than the malicious node. This method also does not address how to detect and isolate malicious node from the network [2]. Have proposed an algorithm to prevent black hole attacks in ad hoc networks. According to their algorithm, any node on receiving a RREP packet, cross checks with the next hop on the route to the destination from an alternate path. If the next hop either does not have a link to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. This technique does not work when the malicious nodes cooperate with each other. [16] has proposed for the source node to verify the RREP destination sequence number by analyzing the RREP messages which arrive within the predefined waiting period by using heuristic method. If sequence number is found to be exceptionally high, the sender of the respective RREP will be marked as malicious node. The major issue in this method is the latency time during the route discovery process since source node has to wait until waiting time period expires before routing table can be updated. In the event where there is no attack in the network, the node still suffers from the latency time.[18] presented an algorithm to prevent the co-operative black hole attacks in ad hoc network. The algorithm takes less time to complete, even when the network is under attack.

8. THE PROPOSED ALGORITHM

In this, section the proposed mechanism for defending against a cooperative black hole attack is presented. The mechanism modifies the AODV protocol by introducing two concepts, (i) data routing information (DRI) table and (ii) cross checking.

8.1 *Data Routing Information*

In the proposed scheme, two bits of additional information are sent by the nodes that respond to the RREQ message of a source node during route discovery process. Each node maintains an additional data routing information (DRI) table. In the DRI table, the bit 1 stands for 'true' and the bit 0 stands for 'false'. The first bit 'From' stands for the information on routing data packet *from* the node (in the *Node* filed), while the second bit 'Through' stands for information on routing data packet through the node (in the *Node* field). a sample database maintained by node *4* is shown in Table 1. The entry 1 0 for node *3* implies that node *4* has routed data packets from *3*, but has not routed any data packets through *3* (before node *3* moved away from *4*). The entry 1 1 for node *6* implies that, node *4* has successfully routed data packets from and through node *6*. The entry 0 0 for node *B2* implies that, node *4* has not routed any data packets from or through *B2*.

Table-1 DRI Table for Node 4

Node ID	Data Routing Information	
	From	Through
3	1	0
6	1	1
B2	0	0
2	1	1

8.2 Cross Checking

The proposed scheme relies on reliable nodes (nodes through which source has routed data previously and knows them to be trustworthy) to transfer data packets. The modified AODV protocol and the algorithm for the proposed mechanism are depicted in Fig. 3. In the modified protocol, the source node (SN) broadcasts a RREQ message to discover a secure route to the destination node. The intermediate node (IN) that generates the RREP has to provide information regarding its next hop node (NHN) and its DRI entry for that NHN. Upon receiving the RREP message from IN, SN will check its own DRI table to see whether IN is its reliable node. If SN has used IN before for routing data packets, then IN is a reliable node for SN and SN starts routing data through IN. Otherwise, IN is unreliable and thus SN sends FRq message to NHN to check the identity of the IN, and asks NHN about the following information: (i) if IN has routed data packets through NHN, (ii) who is the current NHN's next hop to destination, and (iii) has the current NHN routed data through its own next hop. The NHN, in turn, responds with FRp

message including the following responses: (i) DRI entry for IN, (ii) the information about its (NHN's) next hop node, and (iii) the DRI entry for its (NHN's) next hop. Based on the FRp message from NHN, SN checks whether NHN is reliable or not. If SN has routed data through NHN before, NHN is reliable; otherwise, NHN is unreliable for SN. If NHN is reliable, then SN will check whether IN is a black hole or not. If the second bit of the DRI entry from the IN is equal to 1, i.e. IN has routed data *through* NHN, and the first bit of the DRI entry from the NHN is equal to 0 i.e. NHN has not routed data from IN, then IN is a black hole. If IN is not a black hole and NHN is a reliable node, then the route is secure, and SN will update its DRI entry for IN with 0 1, and starts routing data via IN. If IN is a black hole, then SN identifies all the nodes along the reverse path from IN to the node that generated the RREP as black hole nodes. Subsequently SN ignores any other RREP from the black holes and broadcasts the list of cooperative black holes in the network.

SN: Source Node, **IN:** Intermediate Node, **FRq:** Further Request, **DN:** Destination Node, **NHN:** Next Hop Node **FRp:** Further Reply

Reliable Node: The node through which the SN has routed data, **DRI:** Data Routing Information

ID: Identity of the node

```
1   SN broadcasts RREQ
2   SN receivesRREP
3   IF (RREP is from DN or a reliable node) {
4           Route data packets (Secure Route)
5         }
6 ELSE {
7           Do {
8 Send FRq and ID of IN to NHN
9 Receive FRp, NHN of current NHN, DRI entry for NHN's
        next hop, DRI entry for current IN
10 IF (NHN is a reliable node) {
11 Check IN for black hole using DRI entry
12 IF (IN is not a black hole)
13 Route data packets (Secure Route)
14 ELSE {
15          Insecure Route
16          IN is a black hole
17 All the nodes along the reverse path from IN to the node that
   generated RREP are black holes
18                  }    } ELSE
19          Current IN = NHN
20      } While (IN is NOT a reliable node)      }
```

Algorithm for Detection of Grouped Malicious Node to Avoid Black hole Attack

As an example, node *B1* responds to source node *S* with RREP message, it provides its next hop node *B2* and DRI for the next hop (i.e. if *B1* has routed data packets through *B2*). Here the black hole node (*B1*) lies about using the path by replying with the DRI value equal to 0 1. Upon receiving RREP message from *B1*, the source node *S* checks its own DRI table to see whether *B1* is a reliable node. Since *S* has never sent any data through *B1* before, *B1* is not a reliable node to *S*. Therefore, *S* sends FRq to *B2* via alternative path *S-2-4-B2* and asks *B2* about three things: (i) whether *B2* has routed any data from *B1*, (ii) who is *B2*'s next hop, and (iii) whether *B2* has routed data packets through *B2*'s next hop. Since *B2* is maliciously collaborating with *B1*, it replies positively to all the three queries and gives node *6* (chosen randomly) as its next hop. When the source node contacts node *6* via alternative path *S-2- 4-6* to cross check the validity of the claims of node *B2*, node *6* responds negatively. Since node *6* has neither a route to node *B2* nor it has received data packets from node *B2*, the DRI value corresponding to *B2* as stored in node *6* is 0 as shown in Fig. 3. Based on this information, node *S* can infer that *B2* is a black hole node. If node *B1* really had routed data packets through node *B2* before, it should have validated the node (*B2*) before sending it. Now, since node *B2* is invalidated through node *6*, the source node *S* infers that node *B1* is maliciously cooperating with node *B2*. Hence both nodes *B1* and *B2* are marked as black hole nodes and this information is propagated throughout leading to the revocation of their certificates. Subsequently *S* discards any further responses from *B1* or *B2* and looks from a valid alternative route to *D*.

The process of cross checking the intermediate nodes is a one-time procedure which should be affordable for the purpose of security. The cost of crosschecking the nodes can be minimized by allowing the nodes to share the DRI table of their trusted nodes with each other.

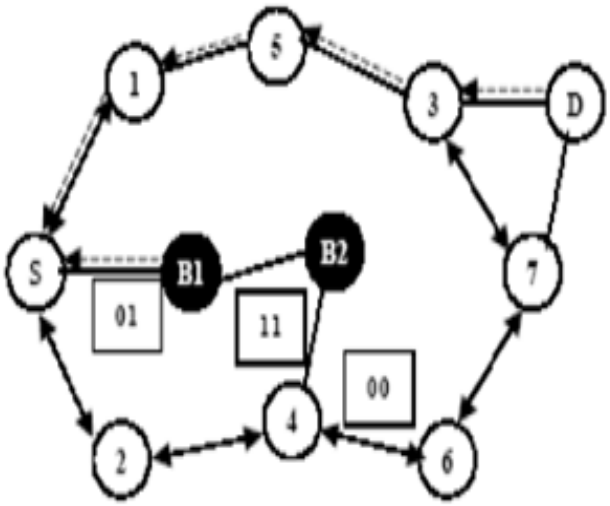

Fig 3. Detection of Grouped Malicious node in the Network

9. SIMULATIONS

The experiments for the evaluation of the proposed scheme have been carried out using the network simulator *ns-2*. The 802.11 MAC layer implemented in ns-2 is used for simulation. An improved version of random waypoint model is used as the model of node mobility [13].

Performances of the three protocols are evaluated:

(i) Standard AODV protocol,

(ii) AODV with two malicious nodes cooperating in a black hole attack,

(iii) AODV with the proposed algorithm. The scenarios developed to carry out the tests use two parameters:

(i) the mobility of the nodes and (ii) the number of active connections in the network. Every point in the graph is an average of the values obtained after the experiment is repeated five times.

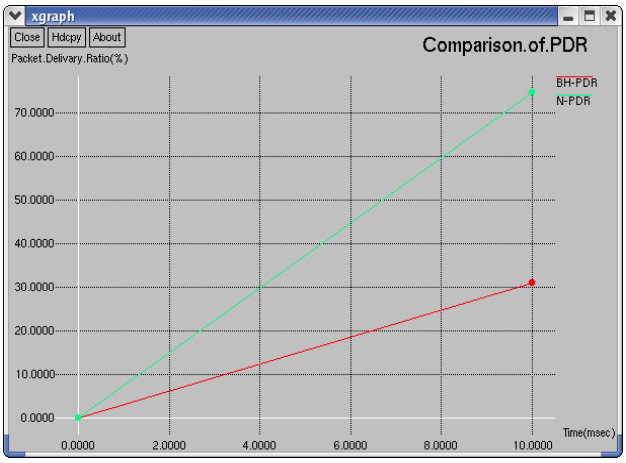

Fig. 4 Graph for Packet Delivery Ratio(PDR)
Y Axis: PDR (%)
X Axis: Time (m/sec)

In Fig. 4, packet delivery ratio is plotted against the Time (m/sec). It is observed that AODV performs better for lower node mobility rates. The delivery rate starts dropping with increasing mobility of the nodes. The performance of the network significantly reduces when AODV is under the cooperative black hole attack, and when the mobility of the nodes in the network increases. This behavior of the protocol is expected due to the following reason. With increasing mobility of the nodes the topology of the network changes faster, resulting in frequent route request generation. This gives an opportunity to a malicious node to send more false RREP packets. AODV under black hole attack exhibits a decrease in delivery ratio to 38%. The proposed algorithm increases the delivery ratio to 55%, resulting in an average improvement of 17%.

10. CONCLUSION

In this paper, cooperative black hole attack has been described in detail. A security protocol has been proposed that can be utilized to identify multiple black hole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the black hole nodes. The proposed scheme has been evaluated by implementing it in the network simulator *ns-2*, and the results demonstrate the effectiveness of the mechanism. As a future scope of work, the proposed security mechanism may be extended so that it can defend against other attacks like resource consumption attack and packet dropping attack. Adapting the protocol for efficiently defending against *gray hole* attack- an attack where some nodes switch their states from black hole to honest intermittently and vice versa, is also an interesting future work.

11. REFERENCES

[1]. C. Perkins, E. Belding-Royer, and S. Das,(2003) "Ad-hoc on-demand distance vector (AODV) routing", Internet Draft, RFC 3561, July.

[2] H. Deng, H. Li, and D. Agarval,(2002) "Routing security in wireless ad hoc networks", *IEEE Communications Magazine*, Vol. 40, No. 10.

[3]L.Tamilselvan, and V. Sankaranarayanan, (2008) "Prevention of cooperative black hole attack in manet", Journal of Networks, Vol. 3 (5),pp.13-20.

[4] Z. Karakehayov,(2005) "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Wksp. Real-WorldWireless Sensor Networks, June 20–21.

[5] S. Desilva, and R. V. Boppana,(2005) "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA.

[6]Yih-Chun, Adrian Perrig, David B. Johnson,(2002) "Ariadne: A secure On-Demand Routing Protocol for AdHocNetworks",parrow.ece.cmu.edu/~adrian/projects /secure routing/ariadne.pdf.

[7] Junhai luo; Mingyu Fan,(2008) "Research on trust model based on game theory in mobile ad-hoc networks, Journal of Computer Research and Development", Vol 45, No.10, pp1704-1710

[8] Yi-Chun Hu, Adrian Perrig,(2004) "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, 1540-7993/04/$20.00 © 2004 IEEE.

[9] Satoshi Kurosawa, "Hidehisa Nakayama and Nei Kato et al,(2008) "Detecting black hole attack on AODV based mobile ad hoc networks by dynamic learning method, International Journal of Network Security", pp.338-346

[10] Makki, Shamila, Pissinou, Nikki; Huang, Hui,(2004)," Solution to the black hole problem in mobile ad-hoc network, 5th World Wireless Congress", pp. 508-512

[11] Lidong zhou, Zygmunt J. Haas(1999), "Securing Ad Hoc Networks", IEEE network, special issue on network security, Vol.13, no.6.

[12] Sukla Banerjee(2008) "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science San Francisco, USA

[13] S. Bansal and M. Baker,(2003) "OCEAN: Observation based cooperation enforcement in ad hoc networks", *Technical Report*, Stanford University.

[14] M. A. Shurman, S. M. Yoo, and S. Park,(2004) "Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE˝04), pp.

[15] Dokurer, Semih.(2006) "Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, AtılımUniversity.

[16] N. H. Mistry, D. C. Jinwala and M. A. Zaveri,(2009) "MOSAODV: Solution to Secure AODV against Blackhole Attack ", (IJCNS) International Journal of Computer and Network Security, Vol. 1, No. 3.

[17] Piyush Agrawal, R. K. Ghosh, Sajal K. Das,(2008), Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference onUbiquitous information management and communication, Pages 310-314, Suwon, Korea.

[18] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard,(2003) "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", www.cs.ndsu.nodak.edu/~nygard/research BlackHoleMANET.pdf .

[19] Bracha Hod,(2005) "Cooperative and Reliable Packet-Forwarding On Top of AODV", www.cs.huji.ac.il/~dolev/pubs/reliable-aodv.pdf.

[20] Chen Hongsong, Ji Zhenzhou and Hu Mingzeng, (2006) "A Novel Security Agent Scheme for Aodv Routing Protocol Based on Thread State Transition". Asian Journal of Information Technology, 5 (1) : 54-60.

12. AUTHOR PROFILE

R. Kesavan is Assistant Professor of Department of Computer Applications, Jaya Engineering College, Chennai, India. He received his Bachelor's degree in Computer Science from Bharathidasan University, Trichy, Master of Science in Computer Science form Bharathidasan Uniersity, Master of Philosophy from Manonmaniam Sundaranar University, Thirunelveli, Tamilnadu, India. Master of Technology in Computer Science and Engineering from Dr. M G R University, Chennai. He has been in teaching profession for the last 10 years. His research area is Mobile Ad Hoc Network . He authored many papers in National / International conference proceedings. He is a life member of Indian Society for Technical Education, New Delhi.

Dr.V. Thulasi Bai is Professor and Dean of Electronics and Communication Engineering Department, Prathyusha Institute of Technology and Management, Chennai, India. She received her Bachelor's degree in Electronics and Communication Engineering from Madurai Kamaraj University, Madurai, and Master's in Electronics and Control from Birla Institute of Technology and Science (BITS), Pilani, Rajasthan, India and Doctorate from Satayabama University Chennai. She has been awarded Young Scientist Award by Department of Science and Technology, Govt of India under FAST TRACK SCHEME for young scientists. She has been in teaching profession for the past 20 years. Her research interests include broadband networks, mobile communication and telemedicine. She is a Member of many professional societies. She has authored well over 60 papers in reputed journals/conference proceedings. She is a life Fellow/Member of many professional societies such as IETE, IEEE, IsfTeH, TSI and BES