ISSN No. 0976-5697

Volume 3, No. 2, March-April 2012

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Comparative analysis of Network layer threats & defense mechanisms of MANETs

Prof.Vrutik Shah*
Dept. of Computer Science
Indus Institute of Technology & Engg.
Ahmedabad, INDIA
vrutikshah@yahoo.com

Dr.Nilesh K. Modi
Prof. & Head Dept. of Computer Science
S.V. Institute of Computer Studies
Kadi, INDIA
drnileshmodi@yahoo.com

Abstract: Mobile ad hoc network (MANET) security has become the focus of vast research efforts. Motivated by the exclusive and substantial difficulties of providing security arising from the dynamic nature of MANETs, many security schemes have been proposed. Rather than trying to encompass the intact field of Ad Hoc security, this paper focuses on networks layer attacks. We perform a vulnerability analysis of protocol to identify unsolved threats to the algorithm, such as, blacks holes, wormholes, Modification, Sybil and rushing attacks. We then compare this vulnerability analysis to schemes that have been proposed to battle the identified threats . The comparison between various secure routing protocols has been made on the basis of security services and security attacks. From the survey it is fairly clear that Routing protocols are vulnerable to various network layer attacks. A multi defence secure routing protocol is still vital to fulfil the essential security services and provide solution against various attacks.

Keywords: MANETs; AODV; SAODV; security attack; Security Services.

I. INTRODUCTION

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information .Wireless networks have become increasingly popular in the past few decades, when they are being adapted to enable mobility and wireless devices became popular. Wireless ad-hoc network have many advantages like Low cost of deployment, Fast deployment, Dynamic Configuration. Networks that support the ad hoc architecture are typically called wireless ad hoc networks or mobile ad hoc networks [1]. Such networks are typically assumed to be self- forming and self healing, self-configured Routing in such networks is particularly challenging because typical routing protocols do not operate efficiently in the presence of frequent movements, intermittent connectivity, network splits and joins, network size. In typical routing protocols such events generate a large amount of overhead and require a significant amount of time to reach stability after some of those events.

Ad hoc wireless network routing protocols [2] can be classified into the three major categories wiz table driven routing protocol, reactive or on-demand driven routing protocol and hybrid routing based on the routing information update mechanism. In the table driven routing protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains. For example DSDV [3], STAR [4], OLSR 5], FSR, HSR and GSR. The Reactive or On-demand routing protocols do not maintain the network topology information. They obtain the necessary path when it is required, by using a connection establishment process. Hence these protocols do not exchange routing information periodically. For example DSR [8], AODV, ABR, SSA [11], FORP, The Hybrid routing protocols combine the best features of the above two categories. Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For example CEDAR, ZRP and ZHLS.

The above protocols do not endow with several security mechanism against essential security services such as authentication, confidentiality, integrity, authentication, non-repudiation and availability. These protocols are also vulnerable to various security attacks such as Rushing attack, Sybil attack, Black Hole attack, Wormhole attack,and Routing table poisoning attack. Many protocols have been introduced to offer basic security services and mitigate against security attacks. For example SAODV [16],SAR [17],A-SAODV [18], MS-AODV [19], RAODV [20], TAODV[21], ISAODV [22] and SecAODV [23], SRPM[24] , SecureAODV.

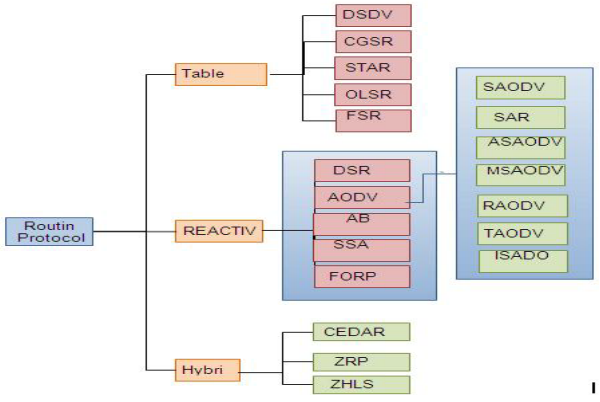

Figure 1: Classification of Routing Protocol

To secure the routing protocols in MANETs, researchers have considered the following security services: availability, confidentiality, integrity, authentication and non-repudiation

II. SECURITY GOALS & ATTACK CLASSIFICATION

In mobile ad hoc networks, all networking functions, such as routing and packet forwarding, are performed by the nodes themselves in a self-organizing manner. For this reason, such networks have increased vulnerability and securing a mobile ad hoc network is very challenging. The following attributes are important issues related to mobile ad hoc networks[7.10].

a. ***Availability****:* Ensures survivability despite Denial Of Service attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

b. ***Confidentiality****:* Ensures certain information is never disclosed to unauthorized entities. Basically, there are these types of attacks on privacy in MANETs: Packet Tracing Attack, Packet Counting Attack, Timing Attack, TTL Attack.

c. ***Integrity****:* Message being transmitted is never corrupted. Authentication: Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

d. ***Non-repudiation*** Ensures that the origin of a message cannot deny having sent the message.

There are two sources of attacks related to node misbehavior in mobile ad hoc networks. The first is external attacker, in which unauthenticated attackers can replay old routing information or inject false routing information to partition the network or increase the network load. The second is internal attack, which comes from the compromised nodes inside the network. Since compromised nodes can be authenticated, internal attacks are usually much harder to detect and can create severe damage.

Misbehave nodes in mobile ad hoc networks are classified into two types: faulty/malicious nodes and selfish nodes. Faulty nodes refer to the nodes that are faulty and cannot follow a protocol, and malicious nodes are intentionally malicious and try to attack the network. The security problem caused by faulty/malicious nodes is extremely important in security sensitive applications. Selfish nodes are economically rational nodes whose objective is to maximize their own welfare. They will be the dominant type of nodes in a civilian ad hoc network. Although selfish nodes do not intend to attack the network, such selfish behaviors are also very harmful to mobile ad hoc network, which is highly dependent on the cooperation of all available nodes.

Although passive (eavesdropping) attacks are also possible in mobile ad hoc networks, they can easily be controlled by using cryptographic mechanisms. Active attacks, which are more damaging, cannot be defended by only applying cryptography mechanism

III. ROUTING PROTOCOL:AODV

AODV [1,9] discovers routes on an as needed basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers.

An important feature of AODV is the maintenance of timer-based states in each node, regarding utilization of individual routing table entries. A routing table entry is expired if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs. Route error propagation in AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves.

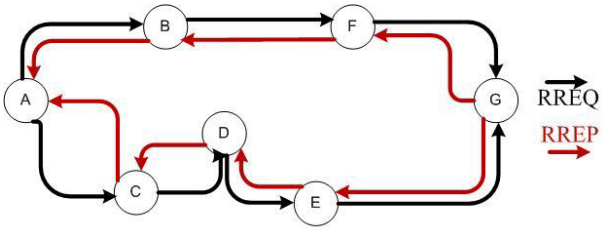

Figure 2: AODV Route Discovery

A. AODV Vulnerabilities[1,6,9]:

AODV has no security mechanism and is vulnerable to several kind of attacks that manipulate routing mechanisms like Route disturbance, Route incursion, Node isolation, Resource Depletion.

a. ***Route Disturbance:*** Malicious node broadcasts faked RERR causing other nodes to delete routes from routing table, using large destination sequence number will cause new RREQ to appear decayed and be ignored. This will cause Disrupting routing tables and breaking links.

b. ***Route incursion*****:** Malicious node attracts routes to itself by forging hop count or destination sequence number in RREP to make route appear shorter or fresher, and packets may now be intercepted or dropped.

c. ***Node isolation***: Attempting to isolate a node from communication with the rest of the network. Malicious node attracts route through hop count or sequence number in RREP, as well Malicious node impersonates destination node by sending RREP with forged destination in response to RREQ.

d. ***Resource depletion*****:** The aim of this attack is to consume power and processing energy from the involving nodes and to overflow the network with false routing packets to consume all the available network bandwidth with unconnected traffic.

A typical Denial of Service attack that attempts to use up network resources. Flooding the network with RREQs or RERRs to use up resources, to send junk data packets. Consequently AODV is vulnerable to atomic and composite attacks

IV. COMPARISONS ON BASIC SECURITY SERVICES

The table I provide a comparison on basic security servicessuch as Confidentiality, Integrity, Authentications, Nonrepudiation and Availability.

Table I. AODV Variant Protocol Mapping to Security Services

Protocol	*ARAN*	*SAODV*	*A-SAODV*	*MS-AODV*	*RAODV*	*TAODV*	*ISAODV*	*SAR*
Type	**Reactive**	**Reactive**	**Reactive**	**Reactive**	**Reactive**	**Reactive**	**Reactive**	**Reactive**
Encryption Algorithm	**Asymmetric**	**Asymmetric**	**Asymmetric**	**Asymmetric**	**Asymmetric**	**Asymmetric**	**Asymmetric**	**Asymmetric**
MANET Protocol	**AODV/DSR**	**AODV**	**AODV**	**AODV**	**AODV**	**AODV**	**AODV**	**AODV**
Synchronization	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**N**
Central Trust Authority	**CA**	**CA**	**CA**	**NOT**	**NOT**	**NOT**	**NOT**	**CA/KDC**
Authentication	**Yes**	**Yes**	**Yes**	**NO**	**Yes**	**Yes**	**Yes**	**No**
Confidentiality	**Yes**	**NO**	**NO**	**NO**	**NO**	**NO**	**Yes**	**Yes**
Integrity	**Yes**	**Yes**	**Yes**	**NO**	**Yes**	**Yes**	**Yes**	**Yes**
Availability	**No**	**No**	**No**	**No**	**No**	**No**	**No**	**No**

V. NETWORK LAYER ATTACKS & DEFENSE MECHANISMS

A. Black Hole Attack:

Black hole[1,2,10,29,30] is a type of routing attack where a malicious node advertise itself as having the shortest path to all nodes in the environment by sending fake route reply as depicted in figIII. By doing this, the malicious node can withdraw the traffic from the source node. AODV is vulnerable to the classic "Blackhole" attack defined for on-demand networks[15]. A composite and protocol non-compliant attack, the malicious node replies to every route request with a route reply, then drops the data packets. Grey Hole attacks are designed to defeat trust-based mechanisms. The attacking node does not act maliciously for an initial period to gain trust before be- ginning to misbehave[29] .

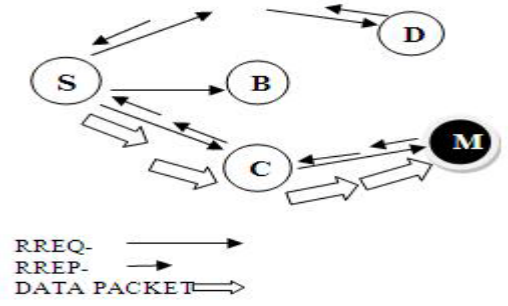

Figure. 3: Black hole attacks in MANETs

a. Defense Mechanism Proposed:

a) A DPRAODV (Detection, Prevention and Reactive AODV) [2] is designed as a countermeasure to the blackhole attack. HASH Function based Two authentication mechanisms the Message Authentication Code (MAC) and the Pseudo Random Function (PRF) , proposed to identify multiple black holes cooperating with each other. Wait and check the replies mechanism is also proposed to find a safe route for packets.

b) TOGBAD a new centralized approach, using topology graphs to identify nodes attempting to create a black hole. In this, use well-established techniques to gain knowledge about the network topology and use this knowledge to perform plausibility checks of the routing information propagated by the nodes in the network. In this approach, we have to consider a node generating fake routing information as malicious.

c) Security-aware ad hoc routing protocol (SAR) [17] can be used to defend against blackhole attacks. The security-aware ad hoc routing protocol is based on on-demand protocols, such as AODV or DSR. In SAR, a security metric is added into the RREQ packet, and a different route discovery procedure is used. Intermediate nodes receive an RREQ packet with a particular security metric or trust level. At intermediate nodes, if the security metric or trust

level is satisfied, the node will process the RREQ packet, and it will propagate to its neighbors using controlled flooding. Otherwise, the RREQ is dropped.

B. WormHole Attack:

Attacker records a packet[1,10,14,15] at one location in the network, tunnels the packet to another location, then replays it there Packets may be replayed from the far end of the wormhole as depicted in fig IV. Puts attacker in a controlling position.

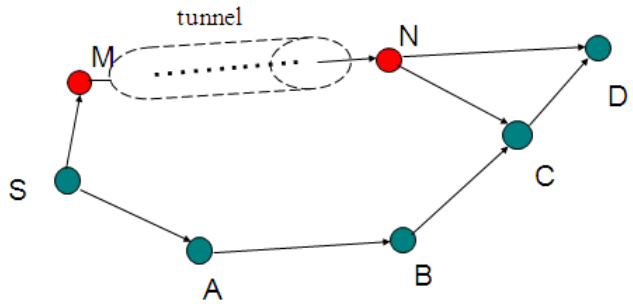

Figure 4:Wormhole Attack

a. Wormhole Defense Mechanism:

Packet leashes [24]: A packet leash is a technique to prevent wormholes by restricting the maximum allowed transmission distance of a packet . These may be geographic or temporal. A geographic packet leash requires nodes to know their own location, and incorporate this information (cryptograph- ically protected) into packets. This allows the distance from sender to receiver to be established. Temporal packet leashes require nodes to have tightly synchronized clocks. The packet creation time is included with the packet (en- crypted), and this allows the receiver to estimate the dis- tance a packet has traveled by examining the time the packet has been in transit. Of course, there is nothing to prevent a malicious authenticated node falsifying time stamps to make transit times appear shorter than they actually are.

A cluster based counter-measure is proposed as countermeasure for the wormhole attack. Wormhole Attack Prevention (WAP) without using specialized hardware is proposed to prevent the wormhole attack. A TrueLink mechanism is proposed which is a timing based countermeasure to the wormhole attack. A packet leash protocol [6,24] is designed as a countermeasure to the wormhole attack. The SECTOR mechanism is proposed to detect wormholes without the need of clock synchronization.

Directional antennas[28]: Directional antennas are also proposed as a countermeasure against wormhole attacks. This approach does not require either location information or clock synchronization, and is more efficient with energy Directional antennas are also proposed to prevent wormhole attacks.

C. Rushing Attack:

Rushing attack [1,10,12], the attacker simply forwards all control packets (but not data packets) received at one node (the attacker) to another node in the network as depicted in Fig V. The rushing attacker may employ a wormhole to rush packets. This attack impacts more on reactive routing protocol.

The protocol defenses it by using randomized selection of route request message. Every node is expected to collect a threshold number of route requests.

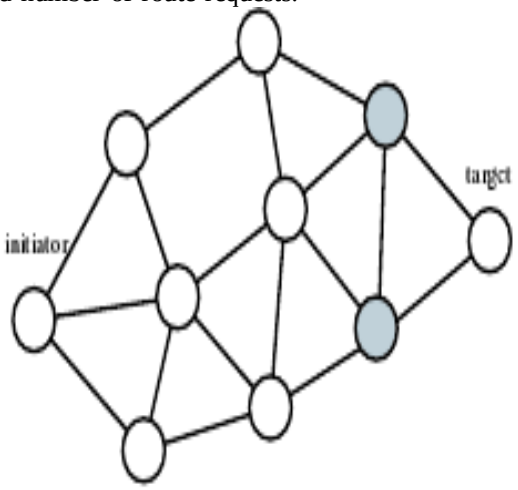

Figure 5: Rushing Attacks

a. Defnese Mechanism:

Randomizing RREQ rebroadcast A solution for countering rushing attacks has been pro- posed in. To prevent rushing attacks through a node using higher power transmissions or out of band links to skip nodes, a secure neighbour detection protocol ensures that nodes will not forward RREQs from nodes that are not their neighbours. To deal with rushing attacks that employ the cutting of backoff times involves removal of the mechanism that only forwards the first RREQ received. Instead, the RREQ to be forwarded is selected randomly, meaning RREQs that arrive earlier (with low latency) are only slightly more likely to be forwarded. In response to a rushing attack preventing a route being found, re-initiating route discovery allows another chance at finding a valid route. Unfortunately, this would also mean that even if there is no threat, there would still be a chance of taking a non-optimal route, leading to some inefficiency.

D. Sybil Attack:

The Sybil attack[1.10] assumed that every physical device has only one radio and device is incapable of simultaneously transmitting and receiving on more than one channel. The node allocates a channel to each of its neighbors to verify if any of its neighbors are Sybil identities. The neighboring node is expected to transmit a message on the allocated channel. The verifier node then picks random channels for listening. If no message is heard on the channel selected then the corresponding node identity is assured to be a Sybil identity

a. Defense Mechanism:

- ***a)*** A multifactor authentication framework is proposed that extends the cryptographic link, binding an entity to a physical node device. ARAN[12,26] can be used to defend against impersonation and repudiation attacks.
- ***b)*** A robust Sybil attack detection framework[27] is proposed for MANETs based on cooperative

monitoring of network activities. In this mechanism, we do not require designated and honest monitors to perform the Sybil attack detection. Each mobile node in the network observes packets passing through it and periodically exchanges its observations in order to determine the presence of an attack. Malicious nodes fabricating false observations will be detected and rendered ineffective.

E. Modification Attack:

Modify the protocol fields of control messages Compromise the integrity of routing computation Cause network traffic to be dropped, redirected to a different destination or take a longer route.

a. Defense Mechanism:

A new key management scheme is implemented in NTP protocol, since Node Transition Probability (NTP) [25] based algorithm provides maximum utilization of bandwidth during heavy traffic with less overhead. NTP determines stable routes using received power, but the packet delivery cannot be guaranteed since it is a non secured protocol. The proposal detects the modification, impersonation attacks and TTL attacks and, avoids the effects of malicious node and determines appropriate measures to discard such malicious nodes in dynamic condition.AODV and Variants are not able to defense against modification attack.

VI. SUMMARY

We make a summary of all the attackers on mobile ad hoc network routing protocols. Table II illustrates the different types of attacks, their description and results.

Table II Types of Attacks, Results

Type of attacks	***Description***	***Results***
Modification	Modify the routing message	acquire control of the route
Fabrication	Generate false routing messages	acquire control of the route
Tunneling attack	Colluding, take advantage of "tunnels"	acquire control of the route
DoS attack	Floods irrelevant data, resource consuming	
Sybil attack	Colluding, forging of multiple identities	acquire control of the route
Rushing attack	Rushing routing message	acquire control of the route

We make a summary of all the attackers on mobile ad hoc network routing protocols. Table III illustrates the different types of attacks, Proposed Solutions in literatures.

TABLE 3. Comparative study based on various security attacks and Solutions

Attacks/Solutions	*ADRPRAODV*	*TOGBAD*	*SAR*	*Packet Leashes*	*Directional Antennas*	*Randomized RREQs*	*Multifactor Auth.*	*Node Transition probability(NTP)*	*Intrusion Detection Schemes*	*Cooperative Monitoring*
Wom hole			**Y**	**Y**						
Black hole	**Y**	**Y**								
DOS Attacks									**Y**	
Byzantine										
Sybil Attack							**Y**			**Y**
Modification Attack								**Y**		
Rushing Attack						**Y**				

Y: Considerable Reduce Risk

VII. CONCULSION

Secure Routing is one of the most basic and important tasks in MANETs. This paper reviewed various secure routing protocols based on AODV. From the comparative studies it is quite clear that these protocols are vulnerable to various routing attacks.

It has been observed none of secure routing protocol provides the availability service. Two protocols ISAODV and SAR provide the Confidentiality, Integrity, Authentications, Nonrepudiation. Only one protocol MSAODV does not provide any basic security services.

All the secure protocols provides the protection against replay and routing table poisoning attack but does not provide the protection against black-hole attack, blackmail attack, rushing attack and DoS. Only RAODV provides the protection against black-hole attack, wormhole attack, rushing attack.

In concise, there is no exclusively mechanism which can provide fundamental security services and protection against various security attacks. So, there is a requirement of a multifence mechanism which can provide basic security services as well mitigate against various security attacks.

VIII. REFERENCES

[1]. Farooq anjum and Petros Mouchtaris, "Security for wireless ad hoc networks," John Wily, 2007.

[2]. Payal N. Raj and Prashant B. Swades, "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET" , IJCSI International Journal of Computer Science Issues, Vol. 2, 2009 ISSN (Online):1694-0784 ISSN (Print): 1694-0814.

[3]. C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-SequencedDistance-vector-Routing (DSDV) for Mobile Computers," SIGCOMMUK, pages 234-244, 1994.

[4]. J.J. Garcia-Luna-Aceves and M. Spohn, "Source-Tree Routing in Wireless Networks," Proceedings of IEEE ICNP, Pages 273-282, October 1999.

[5]. T. Clausen and P. Jacquet, eds, "Optimized Link State Routing Protocol(OLSR)," IETF RFC 3626, October 2003.

[6]. Abbas, Y. ; Mazhar, N. "Vulnerability assessment of AODV and SAODV routing protocols against network routing attacks and performance comparisons " Wireless Advanced (WiAd), 2011 Page(s): 36 – 41 June 2011

[7]. H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vol. 40, pp. 70-75, 2002

[8]. D. Johnson and D. Maltz., "Dynamic source routing in ad-hoc wireless networks routing protocols," In Mobile Computing, pages 153-181. Kluwer Academic Publishers, 1996

[9]. C.E.Perkins and E.M.Royer, "Ad hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Workshop of Mobile Comp. Sys. and Apps., pages 90-100, Feb. 1999

[10]. S. A. Razak, S. M. Furnell, and P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols," 2004.

[11]. R.Dube, C.D.Rais, K.Y. Wang and S.K. Tripathi, "Signal Stability- Based Adaptive Routing for Ad Hoc Mobile Networks," IEEE Personal Communications Magazine, Pages 36 -45, February 1997.

[12]. 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, pp. 38-47, 2004.

[13]. R Alekha Kumar Mishra and Bibhu Dutta Sahoo, "A Modified Adaptive-Saodv Prototype For Performance Enhancement In Manet," In International Journal Of Computer Applications In Engineering,chnology And Sciences (Ij-Ca-Ets), Volume 1 : Issue 2 ,Page: 443, April '09 – September '09.

[14]. Mahajan, M. Natu, and A. Sethi, "Analysis of Wormhole Intrusion Attacks in MANETS",In Proceeding of Military Communications Conference, 2008. MILCOM 2008. IEEE, Pages:1-7, ISBN: 978-1-4244-2676-8

[15]. Y. Hu, A. Perrig, and D. B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, 2006, Vol. 24, No. 2, Pages: 370-380.

[16]. Manel Guerrero Zapata, "Secure Ad hoc On-Demand Distance Vector(SAODV) Routing," draft-guerrero-manet-saodv-06.txt, September 5, 2006.

[17]. R. Kravets, S. Yi, and P. Naldurg, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks," In ACM Symp. On Mobile Ad Hoc Networking and Computing, 2001

[18]. Khan and K.K. Loo, "SRPM Analysis in the Presence of Sinkhole attack in Hybrid Wireless Mesh Networks," In International Journal of Research and Reviews in Ad Hoc Networks Vol. 1, No. 1, March 2011.

[19]. Tamanna Afroze, Saikat Sarkar, Aminul Islam and Asikur Rahman, "More Stable Ad-hoc On-Demand Distance Vector Routing Protocol," In978–1–4244–2800–7/09/$25.00 ©2009 IEEE.

[20]. Sandhya Khurana, Neelima Gupta and Nagender Aneja, "Reliable Ad- hoc On-demand Distance Vector Routing Protocol," In Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06) 0 -7695-2552-0/06

$20.00 © 2006 IEEE.

[21]. Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu, "A Trust Model BasedRouting Protocol for Secure Ad Hoc Networks," In IEEEAC, 0-7803-8155-6 © 2004 IEEE.

[22]. Seyed Amin Hosseini Seno, Rahmat Budiarto andTat-CheeWan, "A Secure Mobile Ad hoc Network Based on Distributed Certificate Authority," In King Fahd University of Petroleum and Minerals 2010,15 January 2011.

[23]. Suman Deswal and Sukhbir Singh, "Implementation of Routing Security Aspects in AODV," In International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010.

[24]. Y. Hu, A Perrig, and D. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks." Proc. of IEEE INFORCOM, 2002.

[25]. Vaithiyanathan, Gracelin Sheeba.R, Edna Elizabeth. N, Dr.S.Radha, "A Novel method for Detection and Elimination of Modification Attack and TTL attack in NTP based routing algorithm ", 2010 International Conference on Recent Trends in Information, Telecommunication and Computing 978-0-7695-3975-1/10 $25.00 © 2010 IEEE

[26]. K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002

[27]. Muhammad Zeshan, Shoab A.Khan, Ahmad Raza Cheema, Attique Ahmed," Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks", 2008International Seminar on Future Information Technology and Management Engineering 978-0-7695-3480-0/08

$25.00 © 2008 IEEE

[28]. L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", Proc. of Networks and Distributed System Security Symposium (NDSS), 2004

[29]. C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775

[30]. Y.F.Alem, Z.C.Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",2nd International Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May,2010

Short Bio Data for the Author

Vrutik Shah was born in India in 1980; He is a Ph.D scholar in Computer Science He received his MCA degree in Computer Science and Application. His research interest includes security in wireless networks, Ad- Hoc networks, and network protocols. This work is a part of Ph.D Program from KARPAGAM University, Coimbatore, INDIA.

Dr. **Nilesh Modi** received his MCA from Hemchandracharya North Gujarat University in 2002, and his Ph.D. in computer science from Bhavnagar University in 2006. He is currently a Professor and Head of Department at SVICS,Kadi,