ISSN: 2321-7782 (Online)
Volume 2, Issue 4, April 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

A Review Paper on the Study of Attacks in MANET with Its Detection & Mitigation Schemes

Maulik H. Davda[1]
Researcher at M.Tech Computer Engineering Dept
R.K. University
Rajkot - India

Sheikh R. Javid[2]
Assistant Professor at M.Tech Computer Engineering Dept
R.K. University
Rajkot - India

Abstract: In mobile ad-hoc network (MANET) security is a challenging issue due to its open nature, infrastructure less property and mobility of nodes. In designing a new security mechanism for mobile ad hoc networks, one must consider the attacks variations as well as the characteristics of the attacks that could be launched against the ad hoc networks and existing detection and mitigation schemes.. The discussions of these four aspects are summarized in this paper. This paper also classifies several common attacks against the ad hoc networks routing protocols based upon the techniques that could be used by attackers to exploit routing messages.

Keywords: MANET, attack, Wormhole, Black hole, Gray hole, Jellyfish.

I. INTRODUCTION

A MANET is similar to a set of mobile hosts that fulfils primary networking purposes not having the help of a permanent structures and facilities. Nodes of an ad hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. Security in MANET is a required component for necessary network purposes like packet forwarding and routing: network operation can be easily put in danger if countermeasures are not embedded into basic network functions at the primary stages of their design. Unlike networks using dedicated nodes to support basic functions like packet forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This very difference is at centre of the security problems that are particular to ad hoc networks. As opposed to dedicated nodes of a traditional network, the nodes of an ad hoc network cannot be depending for the correct execution of serious network functions. However, similar to other networks, MANET also vulnerable to many security attacks. MANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself [1]. As people will be encouraged to use a secured network, it is important to provide MANET with reliable security mechanisms if we want to see this exciting technology become widely used in a next few years. Before the development of any security measure to secure mobile ad hoc networks, it is important to study the variety of attacks that might be related to such networks. With the knowledge of some common attack issues, researchers might have a better understanding of how mobile ad hoc networks could be threatened by the attackers, and thus might lead to the development of more reliable security measures in protecting them. The purpose of this study is to investigate some of the important issues that might be related to security attacks in mobile ad hoc networks and some of the existing detection and mitigation schemes. In Section II, we see how attacks against the ad hoc networks may vary depending upon in which environment the attacks are launched, what communication layer the attacks are targeting, and what level of ad hoc network mechanisms are targeted. After considering these three variations, it is also important to investigate the characteristics of attacks against the ad hoc networks. This topic explained in Section III. In this paper, we give a special attention to attacks that could be launched against the routing protocols [2]. We identified that most of the attacks against ad hoc networks routing protocols are actually launched by exploiting the routing messages, and further classify them based upon the techniques that could be used to exploit routing messages in Section IV. We conclude study and present future work in Section V.

II. Attacks Classification

A. *Mobile vs. wired attackers:*

Mobile attackers have the same capabilities as that of the other nodes of any particular ad hoc network. Having the same resource limitations, their capabilities to harm the networks operations gets also limited. For instance, with the limited transmitting capabilities and battery powers, mobile attackers could only jam the wireless links within its vicinity. They are not capable to launch the network jamming attacks to disrupt the whole networks operations. On the other hand, wired attackers are attackers that are capable of gaining access to the external resources such as the electricity. Since they have more resources, they could launch more severe attacks in the networks, such as jamming the whole networks or breaking expensive cryptography algorithms. Existence of the wired attackers in the ad hoc networks (especially in the open environment networks) is always possible as long as the wired attackers are able to locate themselves in the communication range and have access to the wired infrastructures.

B. *Passive vs. Active attacks:*

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur. Attacks which are in ad hoc networks can be mostly categorized into two groups:

Passive attacks: involve only eavesdropping of data

Active attacks: involve actions performed by attacker, such as replication, modification and deletion of communicated data.

1. *Passive Attack:* A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks contain traffic investigation, observation of insecure communications, decrypting weakly encrypted traffic, and capturing authentication information like passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks produce in the disclosure of information or data files to an attacker without the permission or awareness of the user.
2. *Active Attack:* In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information [3].

C. *Inside vs. Outside Attacks:*

In an insider attack, an attacker has compromised or captured a node, thus gaining access to encryption and authentication keys. The primary method of detecting and mitigating insider attacks is to monitor the packet forwarding behavior among the nodes. In an outsider attack, attackers are supposed to have no knowledge of the keys that are used to encrypt and authentication. Preventing outside attackers from tampering with the data is accomplished by simply employing encryption and authentication schemes.

D. *Layered Attacks:*

Attacks can also be classified as per the layer at which the attack happens, as shown on the following table:

TABLE I
Layer Attacks

Layers	Attacks
Application Layer	Repudiation, Data corruption
Transport Layer	Session Hijacking, SYN Flooding
Network Layer	Gray Hole, Black Hole, Worm Hole, Byzantine, Sybil, Jellyfish, Rushing
Link Layer	Interception, Fabrication, Modification
Physical Layer	Jamming, sniffing

E. Data vs. Control Traffic Attacks:

Data traffic attack deals either in nodes dropping data packets passing through them or in delaying of forwarding of the data packets. Some types of attacks choose victim packets for dropping while some of them drop all of them irrespective of sender nodes. This may highly degrade the quality of service and increases end to end delay. This also causes significant loss of important data. In Control traffic attack, an attacker tries to gain access to a valid route by deliberately tampering routing messages. In another variation of this attack attacker first listens wireless traffic for control message and then it creates forged packet to gain access to the route next time when route request is again sent.

III. Active Attacks Against Routing Scheme

Routing is one of the most vital mechanisms in the ad hoc networks. Inappropriate and unconfident routing mechanisms will not only decrease the performance of ad hoc networks, but will also make such networks vulnerable to many security attacks. One of the basic elements in the routing mechanism is the routing message, which is used to establish and maintain relationships between nodes in the networks. The importance of the routing message has made it a main target by the attackers to launch attacks against the ad hoc networks. Attacks against the routing messages could be started in many types and may contain all the characteristics described in Section III. In this work, attacks against routing messages are classified based on the classification suggested by Stallings in [4]. In such classification, information or messages could be deviated from the normal operation flow using modification, interception, interruption or fabrication attacks. In a more severe case, attackers also might use any combination of these attacks to disrupt the normal information flow. As far as our concern, this study is the first to address security attacks against the ad hoc networks routing messages.

A. Modification

In a message modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks. Since nodes in the ad hoc networks are free to move and self-organize, relationships among nodes at some times might include the malicious nodes. These malicious nodes might exploit the sporadic relationships in the network to participate in the packet forwarding process, and later launch the message modification attacks. Examples of attacks that can be classified under the message modification attacks are packet misrouting and impersonation attacks.

1. *Packet misrouting attacks: In a packet misrouting attack, malicious nodes reroute traffic from their original path to make them reach the wrong destinations [5]. Attackers might misroute a packet to make it stay in the network longer than its lifetimes, thus render it to be dropped from the network. As a result, the source node needs to retransmit the lost packets and this will consume more bandwidth, as well as increasing the overhead in the networks.*

2. *Impersonation attacks:* The impersonation attacks, also called the spoofing attacks, are attacks where malicious node assumes the identity of another node in the networks [6]. By impersonating another node, attackers are able to receive routing messages that are directed to the nodes they faked. Impersonation attacks are possible in the ad hoc networks because most of the current ad hoc routing protocols do not authenticate the routing packets. As a result, malicious nodes might exploit this loophole to masquerade as another node by modifying the contents of the packets.

B. *Interception*

Attackers might launch the interception attacks to get an unauthorized access to the routing messages that are not intentionally sent to them. This kind of attack jeopardizes the integrity of the packets because such packets might be modified before being forwarded to the next hop. Besides, the intercepted packets might also be analyzed before passed to the destination thus violating the confidentiality. Examples of attacks that can be classified under the interception attacks are wormhole attacks, black hole attacks, and routing packet analysis attacks.

1. *Wormhole attacks [7]:* A compromised node in the ad hoc networks colludes with external attacker to create a shortcut in the networks. By creating this shortcut, they could trick the source node to win in the route discovery process and later launch the interception attacks. Packets from these two colluding attackers are usually transmitted using wired connection to create the fastest route from source to the destination node. [8][9] In addition, if the wormhole nodes consistently maintain the bogus routes, they could permanently deny other routes from being established. As a result, the intermediate nodes reside along that denied routes are unable to participate in the network operations.
2. *Black hole attacks: M*malicious nodes trick all their neighboring nodes to attract all the routing packets to them. As in the wormhole attacks, malicious nodes could launch the black hole attacks by advertising themselves to the neighboring nodes as having the most optimal route to the requested destinations[10][11][12]. However, unlike in the wormhole attacks where multiple attackers colluded to attack one neighboring node, in the black hole attacks, only one attacker is involved and it threatens all its neighboring nodes.
3. *Gray hole attacks:* A kind of the black hole attack, where the harmful node is not actually harmful initially, it turns into harmful soon after. This irregular behavior of malicious nodes prevents a trust based security solution from sensing them before they turn into malicious node. A gray hole may forward all the packets to certain nodes but may drop those packets coming from or destined to some specific nodes. In another variation of this attack, a node may behave maliciously for some time but later on it behaves normally. Sometimes, a node may combine the behaviour of attacks discussed above. Due to this uncertainty in behaviour of gray hole, this type of attacks are more difficult to detect/prevent compared to black hole attack. Like black holes, cooperative gray hole attacks may be possible against AODV. [13][14][15][16][17]
4. *Routing packet analysis attacks:* Since no disruptive action occurs, routing packet analysis could be classified as one of the passive attacks against the ad hoc networks. One way to launch this attack is by exploiting the promiscuous mode employed in the ad hoc network. In a promiscuous mode, if node A is the neighbour of both nodes B and C at a particular time, node A can always hear the transmissions between node B and node C. By exploiting this nature, node A is able to analyze the overheard packets transmitted between node B and node C. More explanation regarding the promiscuous mode in the ad hoc networks can be found in [17]. Besides, malicious nodes could also launch this attack by exploiting the nature in a multi hop routing. In multi hop routing, packets need to be forwarded through several intermediate nodes before reaching the actual destination. Malicious nodes might exploit this opportunity by locating themselves in any location along the route to participate in the message forwarding process and later launch the routing packet analysis attacks.

C. *Fabrication*

Instead of modifying or interrupting the existing routing packets in the networks, malicious nodes also could fabricate their own packets to cause chaos in the network operations. They could launch the message fabrication attacks by injecting huge packets into the networks such as in the sleep deprivation attacks. However, message fabrication attacks are not only launch by the malicious nodes. Such attacks also might come from the internal misbehaving nodes such as in the route salvaging attacks.

1. *Sleep deprivation attacks [18]:* This kind of attack is actually more specific to the mobile ad hoc networks. The aim is to drain off limited resources in the mobile ad hoc nodes (e.g. the battery powers), by constantly makes them busy processing unnecessary packets. In a routing protocol, sleep deprivation attacks might be launched by flooding the targeted node with unnecessary routing packets. For instance, attackers could flood any node in the networks by sending a huge number of route request (RREQ), route replies (RREP) or route error (RERR) packets to the targeted node. As a result, that particular node is unable to participate in the routing mechanisms and rendered unreachable by the other nodes in the networks.

2. *Route salvaging attacks:* Route salvaging attacks are launched by the greedy internal nodes in the networks. In a mobile ad hoc network, there is no guarantee that each transmitted packet will successfully reach the desired destination node [19]. Packets might not reach the destination node because of the natural network failures or might be under attacks by the adversaries. Therefore, to salvage their packets from such failures, misbehaving internal nodes might duplicate and retransmit their packets although no sending error messages received. The effects of the route salvaging attacks might be more severe if there are many greedy nodes in the networks. Besides draining off more resources in intermediate and destination nodes, this attack might also cause the consumption of unnecessary bandwidth.

D. *Interruption*

Interruption attacks are launched to deny routing messages from reaching the destination nodes. Adversaries could do this by either attacking the routing messages or attacking the mobile nodes in the networks. Actually, most of the attacks launched in the modification, interception, and fabrication attacks are aimed to interrupt the normal operations of the ad hoc networks. For instance, adversaries aiming to interrupt the availability service in the networks might destroy all paths to a particular victim node by using the message modification attacks. In a message fabrication attack, adversaries could overload the networks by injecting huge unnecessary packets. Examples of attacks that could be classified under the interruption attacks category are packet dropping attacks, flooding attacks, and lack of cooperation attacks.

1. *Packet dropping attacks:* Direct interruption to the routing messages could be done by using the packet dropping attacks. In a standard packet dropping attack, an adversary collaborates as usual in the route discovery process and launches the constant packet dropping attacks if it is included as one of the intermediate nodes. In addition, instead of constantly dropping all the packets, adversaries might vary their techniques using random, selective, or periodic packet dropping attacks to help their interrupting behaviour remain concealed [20][21][22].

2. *Flooding attacks:* Adversaries also might interrupt the normal operations in the packet forwarding process by flooding the targeted destination nodes with huge unnecessary packets. Nodes under the flooding attacks are unable to receive or forward any packet thus all the packets directed to them will be discarded from network [23] [24].

3. *Lack of cooperation attacks:* Lack of cooperation from the internal nodes to participate in the network operations can also be seen as an attempt to launch a refusal of service attack. In such attacks, internal nodes are discouraged to cooperate in the network operations that did not benefit them because participating in such operations will drain off their resources. Misbehaving internal nodes might use different strategies to save their limited resources. They might refuse to forward the other node’s packets, not send back the route error report to the sender when failing to forward packets, or might turn off their devices when not sending any packet in the networks.

IV. Detection and Mitigation Scheme

A. *Intrusion Detection*

The mobile nodes are independent and there movement is not controlled by the system. So the nodes can easily be captured & compromised. The architecture of wireless network also has no physical obstacles, so attacks can come from any directions.

Adversaries can exploit the decentralized management, by breaking the cooperative algorithm. To tackle this situation different IDS are available, such like:

1. *Standalone IDS:* Every node has its own IDS agent, which monitor the node only, if any threat has been detected then it can take protection locally & since there is no cooperation between nodes then all decisions are based on information collected by nodes. This method is not so proficient.
2. *Cooperative IDS:* Wireless ad hoc network is distributed in nature so the detection & response mechanism must be in two phase. Local & Global detection. Every node has IDS agent that detect attacks locally and cooperates with other nodes inside network and inform globally. Significantly, this distributed-cooperative IDS technology mush more stable than standalone IDS and more stable form flat, cluster based network configuration. [25][26]
3. *Hierarchical IDS:* Here also every node has its own IDS agent. Collection of nodes form cluster. Every cluster has a special node know as cluster head.IDS agent for cluster head in responsible for both local & global Intrusion detection. Layered architecture in wireless ad hoc network can be protected by this approach. Another alternative distributed solution called spontaneous watchdog. Fast sensor ad hoc network without divide them into clusters, some powerful independent, spontaneous nodes are created, known as watchdog, which monitors the communication with their neighbors[27][28].
4. *Zone based IDS:* The local IDS agent used in Zone based Intrusion detection system (ZBIDS).Zone can be formed by geographic partitions. Every node has its two identities, INTRA ZONE and INTERZONE & can be determined by Zone ID. By forwarding HELLO Message, inter and intra zone nodes are determined. A node may change its role by the nature of mobility. [29][30][31]

B. *Mitigation technique*

Mitigation technique in ad hoc network guarantees to protect from the attacks, security threats and vulnerabilities, like The Multipath Routing can be effective way to mitigate selective forwarding. Different mitigation techniques for attacks are:

1. *Black-Hole Attack:* [28] (I) Collecting multiple RREP messages (from more than two nodes) and thus hoping multiple redundant paths to the destination node and then buffering the packets until a safe route is found. (ii) Maintaining a table in each node with previous sequence number in increasing order. Each node before forwarding packets increases the sequence number. The sender node broadcasts RREQ to its neighbors and once this RREQ reaches the destination, it replies with a RREP with last packet sequence number. If the intermediate node finds that RREP contains a wrong sequence number, it understands that somewhere something went wrong.
2. *Gray-Hole Attack: Mitigated by priority protocols schemes [32]. Whenever a node enters in a Mobile Ad Hoc network IP allocation is the first step in which the node will get its IP along with initial priority and we have adopted the technique of Prime DHCP [25]. Neighbor Discovery is the second step of the proposed scheme. New node will send the HELLO packets to its neighbors and discover the identity of the neighbors along with their priority. Authentication is the next step of the scheme in which it will broadcast information about its existence and exchange keys with the neighbors according to the scheme HEAP [26] which is a hop-by-hop authentication protocol. HEAP authenticates packets at every hop by using a modified HMAC based algorithm along with two keys and drops any packets that originate from outsides.*
3. *Jellyfish Attack: (I) 2ACK [33]:* The basic idea of the 2ACK scheme is that, when a node forwards a data packet successfully over the next hop, the destination node of the next-hop link will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully. Such a 2ACK transmission takes place for only a fraction of data packets, but not for all. (ii) Credit based systems [28]: This

approach provides incentives for successful transmission of some kind of token or credit which the node might use when it starts sending its own packet. (iii) Reputation based scheme: Here individual nodes collectively detect misbehaving nodes (such as CONFIDANT). [42][43]

4. *Worm Hole Attack [44] [45] [46]:* (I) Geographical leashes & temporal leashes: A leash is added to each packet in order to restrict the distance the packets are allowed to travel. A leash is associated with each hop. Thus, each transmission of a packet requires a new leash. A geographical leash is intended to limit the distance between the transmitter and the receiver of a packet. A temporal leash provides an upper bound on the lifetime of a packet. [47] (II) using directional antenna: Using directional antenna restricts the direction of signal propagation through air. This is one of the crude ways of limiting packet dispersion.

5. *Rushing Attack:* (I) SEDYMO [35]: Secured Dynamic MANET On-Demand is similar to DYMO but it dictates intermediate node must add routing information while broadcasting the routing messages and no intermediate node should delete any routing information from previous sender while broadcasting. It also incorporates hash chains and digital signature to protect the identity. (ii) SRDP [34]: Secure Route Discovery Protocol is security enhanced Dynamic Source routing (DSR) protocol. (iii) SND [31]: Secure Neighbor Detection is another method of verifying each neighbor's identity within a maximum transmission range.

6. *Cache Poisoning Attack:* (I) SAODV [36]: Secure AODV is an extension to AODV protocol that adds each node to exchange signed routing messages. Each node has its own public key which it uses to sign routing messages. Also SAODV uses hop count as a metric for shortest-route as AODV and uses hash chains to secure hop count information in route messages. (ii) SNRP [38]: Secure Neighbor Routing protocol uses security enhanced Neighbor Lookup Protocol (NLP) to secure MANET routing. Newly added node uses public key to participate in MANET.

7. *Sybil Attack:* One way of mitigating this attack is maintaining a chain of trust, so single identity is generated by a hierarchical structure which may be hard to fake. Another approach would be based on signal strength [39] [40] [41].

V. Conclusion

We have tried to categorize the different types of ad hoc security attacks solely based on their characteristics to considerably reduce the mitigation period. By bringing the attacks under these two broad categories the complicacy of naming also reduces. We have also kept a close look on the existing algorithms needed to mitigate the attacks and have tried to bind the attacks into categories according to that. Some attacks have characteristics which makes them unsuitable to be categorized into these categories, so they have been kept away from this topic of discussion for the time being. Further study is in progress to find out more common characteristics of the attacks to more strongly bind them into these categories and to ably design more powerful algorithm in mitigating data.

References

1. Mohammad Al-Sherman, Song-Moo You, Black Hole Attack in Mobile Ad Hoc Networks, ACM-SE 42 Proceedings of the 42nd annual southeast regional conference
2. Songhai Lu,Lingyan Jia,Kwok-Yan Lam,Longxuan Li, SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack, International Conference on Computational Intelligence and Security, 2009
3. Piyush Agrawal and R. K. Ghosh: Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks www.stanford.edu/~piyushag/docs/icuimc08.pdf
4. W. Stallings, Cryptography and network security, Principles and practice, 2nd ed., Prentice Hall, Inc, 1999, pp. 6-9.
5. S. Rajavaram, H. Shah, V. Shanbhag, J. Undercoffer, and A. Joshi, "Neighborhood Watch: An Intrusion Detection and Response Protocol for Mobile Ad Hoc Networks," Student Research Conference, University of Maryland at Baltimore County (UMBC), May 3, 2002.
6. A. Burg, "Ad hoc networks specific attacks," Technische Universität München, Institut für Informatik, Seminar Paper, Seminar Ad Hoc Networking: concept, applications, and security, Nov., 2003.
7. Johnny Wong, Xia Wang ,An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks, Computer Software and Applications Conference, Annual International ,:July 2007

8. Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala: A Review of Current Routing Attacks in Mobile Ad Hoc Networks http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/Volum e2/Issue3/IJCSS-41.pdf

9. Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah: MANET Routing Protocols and Wormhole Attack against AODV http://paper.ijcsns.org/07_book/201004/20100403.pdf

10. Songbai Lu,Lingyan Jia,Kwok-Yan Lam,Longxuan Li, SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack, International Conference on Computational Intelligence and Security, 2009

11. Sheenu Sharma, Roopam Gupta: Simulation Study of BLACK HOLE Attack In MOBILE AD HOC NETWORKS http://jestec.taylors.edu.my/Vol%204%20Issue%202%20June%20 09/Vol_4_2_243-250_Sheenu%20Sharma.pdf

12. Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedroil : Black Hole Attack Injection in Ad hoc Networks www.ece.cmu.edu/~koopman/dsn08/fastabs/dsn08fastabs_ruiz.pdf

13. Piyush Agrawal and R. K. Ghosh: Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks www.stanford.edu/~piyushag/docs/icuimc08.pdf

14. M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar,Jaydip Sen: A mechanism for detection of Gray Hole Attack in Mobile Ad Hoc Networks , Proceedings of the 6th International Conference on Information, Communications and Signal Processing (ICICS '07), Singapore, December 2010

15. Vishnu K, Amos J Paul: Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks www.ijcaonline.org/journal/number22/pxc387679.pdf

16. Vishnu K Amos J Paul , Detection and Removal of Cooperative Black/Gray hole attack in Mobile AdHoc Networks ,International Journal of Computer Applications, Number 22 - Article 8,2010 , www.ijcaonline.org/archives/number22/445-679

17. Sukla Banerjee : Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks

18. Rainer Falk, Hans-Joachim Hof, "Fighting Insomnia: A Secure Wake-Up Scheme for Wireless Sensor Networks" , The International Conference on Emerging Security Information, Systems, and Technologies, June 2009

19. S. Y. Ni, Y. C. Tseng, Y. S. Chen, and J. P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in Proc. of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp. 151-162, Aug. 15-19, 1999.

20. Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies," in Proc. of The 23rd International Conference on Distributed Computing Systems (ICDCS), pp. 478-489, May 19-22, 2003.

21. Salmin Sultana,Elisa Bertino,Mohamed Shehab , "A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks", International Conference on Distributed Computing Systems Workshops, June 2011

22. Shoab A. Khan,Muhammad Zeshan,Attique Ahmed,Ahmad Raza Cheema, "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks",International Seminar on Future Information Technology and Management Engineering, November 2008

23. Chris Karlof, David Wagner, Secure routing in wireless sensor networks: attacks and countermeasures , Ad Hoc Networks 1 (2003)

24. Joaquin Garcia-Alfaro, Gimer Cervera, Michel Barbeau, Evangelos Kranakis , "Mitigation of Flooding Disruption Attacks in Hierarchical OLSR Networks" , Annual Conference on Communication Networks and Services Research, May 2011

25. International Journal of Computer Applications (0975 – 8887) Volume 8– No.9, October 2010, Comparative study of Distributed Intrusion Detection in Ad-hoc Networks,

26. SECURITY FOR WIRELESS AD HOC NETWORKS, Farooq Anjum and Petros Mouchtaris, Published by John Wiley & Sons, Inc., Hoboken, New Jersey

27. Zhihong Qian,Yinan Li , "Mobile Agents-Based Intrusion Detection System for Mobile Ad Hoc Networks", International Conference on Innovative Computing and Communication and Asia-Pacific Conference on Information Technology and Ocean Engineering, January 2010

28. Ze Li,Haiying Shen , "ARM: An Account-Based Hierarchical Reputation Management System for Wireless Ad Hoc Networks", International Conference on Distributed Computing Systems Workshops, June 2008

29. Alert Aggregation in Mobile Ad Hoc Networks, by Bo Sun, Kui Wu, Udo W. PoochWiSE'03, September 19, 2003, San Diego, California, USA. Copyright 2003 ACM 1-58113-769-9/03/0009

30. Guorui Li,Yingfang Fu,Jingsha He , "A Distributed Intrusion Detection Scheme for Mobile Ad Hoc Networks", Annual International Computer Software and Applications Conference, July 2007

31. Xiaoxin Wu,Elisa Bertino , "An Analysis Study on Zone-Based Anonymous Communication in Mobile Ad Hoc Networks", IEEE Transactions on Dependable and Secure Computing , October 2007

32. A Priority Based Protocol for Mitigating Different Attacks in Mobile Ad hoc Networks by Himadri Nath Saha, Debika Bhattacharyya & P. K. Banerjee, International Journal of Computer Science & CommunicationVol. 1, No. 2, July-December2010, pp. 299-302.

33. Zhaoyu Liu, AnthonyW. Joy, Robert A. Thompson,Department of Software and Information Systems,University of North Carolina at Charlotte,{zhliu, awjoy, rthompso}@uncc.edu, "A Dynamic Trust Model for Mobile Ad Hoc Networks" , 10th IEEE International Workshop

34. Jihye Kim and Gene Tsudik, Computer Science Department, University of California, Irvine, {jihyek, gts}@ics.uci.edu, "SRDP: Securing Route Discovery in DSR" , Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05)

35. Helena Rif`a-Pous and Jordi Herrera-Joancomart, Universitat Oberta de Catalunya, Rambla del Poblenou, Spain, {hrifa,jherreraj}@uoc.edu, "Secure Dynamic MANET On-demand (SEDYMO) Routing Protocol", Fifth Annual Conference on Communication Networks and Services Research(CNSR'07)

36. Manel Guerrero Zapata: "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing" September 2006 http://people.ac.upc.edu/guerrero/saodv.html

37. International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October2009 1793-8201, Secure Routing Techniques for MANETs, Dr. Harsh Sadawarti and Anuj K. Gupta, Member, IAENG

38. Ajay Jadhav and Eric E. Johnson, Senior Member, IEEE, "Secure Neighborhood Routing Protocol" , MILCOM 2006 , October 2006

39. D. Llewellyn-Jones,M. Merabti,S. Abbas , "Signal Strength Based Sybil Attack Detection in Wireless Ad Hoc Networks", International Conference on Developments in eSystems Engineering, December 2009
40. John Brooke,Saorsh Hashmi , "Towards Sybil Resistant Authentication in Mobile Ad Hoc Networks", The International Conference on Emerging Security Information, Systems, and Technologies, July 2010
41. Gilles Guette,Bertrand Ducourthial , "On the Sybil attack detection in VANET", IEEE International Conference on Mobile Adhoc and Sensor Systems Conference , October 2007
42. N. Bhalaji, A. R. Sivaramkrishnan, Sinchan Banerjee, V. Sundar, and A. Shanmugam, "Trust Enhanced Dynamic Source Routing Protocol for Adhoc Networks", World Academy of Science, Engineering and Technology 49 2009
43. Jean-Yves Le Boudec,Sonja Buchegger , "Performance analysis of the CONFIDANT protocol" , Proceedings of the third ACM international symposium on Mobile ad hoc networking & computing (MobiHoc '02)
44. Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, June 2008
45. Maria Gorlatova, Peter Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano , "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis" MILCOM , October 2006
46. Stephen Mark Glass, Vallipuram Muthukkumarasamy, Marius Portmann , "Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks", International Conference on Advanced Information Networking and Applications, May 2009
47. C.E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” Proc. ACM SIGCOMM,1994

AUTHOR(S) PROFILE

Maulik H. Davda, Received the BE degree in Computer Science and Engineering from Gujarat Technological Univesity and Pursing M.Tech degree in Computer Engineering from RK University.

Sheikh R. Javid, Assistant professor at RK University in Computer Engineering Department, Specialist in Networking and Electronics.