A Detail Review of Routing Attacks in Mobile Ad Hoc Networks

Aarti Chauhan
M-Tech. Student
artianu1991@gmail.com
Department Of Computer Science
Shri Ram College of Engineering and Management,
,Palwal, Haryana, India

Puneet Rani
Asst. Prof.
Department Of Computer Science
Shri Ram College of Engineering and Management
Palwal, Haryana, India

Abstract— A MANET is an infrastructure –less type of ad-hoc network that consist of number of mobile nodes to make communication among nodes mobile establish dynamic path among one node to another via wireless network interfaces. In a MANET rating is a particularly challenging task as compared to other conventional network. Due to unique characteristics such as limited power, dynamic network topology and limited bandwidth. In the availability of malicious nodes , one of the main problems in MANET is to design the robust security to mitigating various type of routing attack difficult mechanism have been proposed using various cryptographic Techniques. In this paper we describe various ad hoc network security mechanism required to mitigate several type of attacks in rating protocols. To accomplish our goals e have done detail literature survey for collecting relevant information related to various security attacks with their mechanism. In our survey we focus on the results and related works from which provide secure protocol for MANET.

Keywords— MANET, Black-Hole Attack, Gray-Hole Attack, Jellyfish Attack, Rushing Attack, Worm Hole Attack

I. INTRODUCTION

A MANET is rapidly growing technology which is based on rapidly deployed network and self-organized. Due to its important features, MANET attracts various real world application areas where the networks topology changes very fast [2]. Nodes are interconnected through wireless interface. There is no fixed set of infrastructure and centralized administration in this type of networks. MANET is used different of applications such as search and rescue, emergency relief scenarios, public meeting, device network, disaster recovery, automatic battlefields and virtual classroom etc. The counter measures can be considered as function or features that reduce security vulnerabilities and attacks [14].

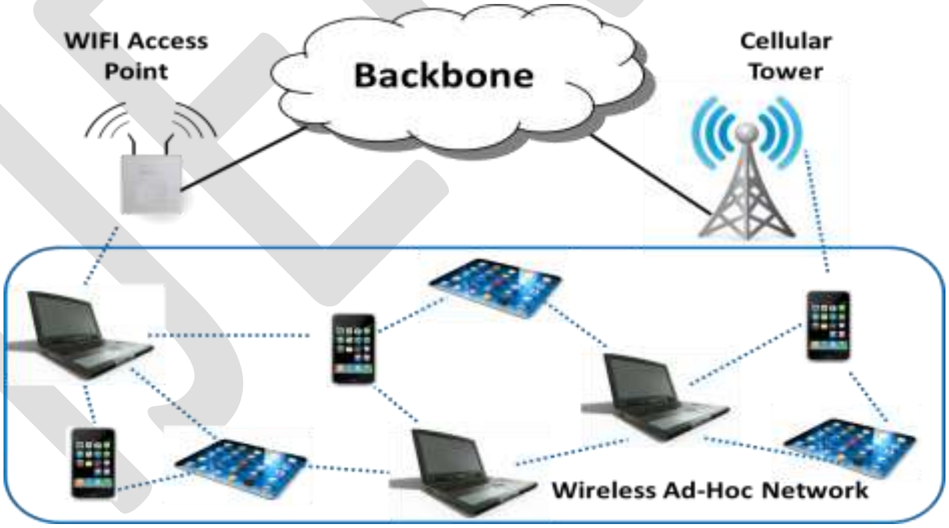

Figure: 1 Mobile Ad hoc Network

Malicious routing attacks can target the routing discovery or maintenance parts by not following the specification of routing protocols. Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and suppose that all nodes are well-behaved and trustworthy [6]. However in a hostile environment, a malicious node can launch Routing attacks to disrupt denial-of-service (DoS) attacks or routing operations to deny services to legitimate nodes [11].

Table: 1 Different types of Attacks

Layer	Type of Attack
Application Layer	1. Repudiation attack, 2. Attacks by virus & worms
Transport Layer	1. TCP SYN attack (DOS in nature), 2. TCP session hijacking, 3. Jelly Fish attack
Network Layer	1. Flooding attack, 2. Route tracking, 3 Message Fabricate, modification, 4.Blackhole attack, 5.Wormhole attack, 6. Link spoofing attack
MAC Layer	1. Mac DOS (Denial of service) attack, 2. Traffic monitoring & analysis, 3. Bandwidth stealth, 4. MAC targeted attack, 5. WEP targeted attack
Physical Layer	1. Jamming attack (DOS in nature), 2. Stolen or compromised attack, 3. Malicious massage injecting, 4. Eavesdropping attack

II. Categories of Attacks: Attacks in MANET be divided into types are active attack and passive attack [12] .

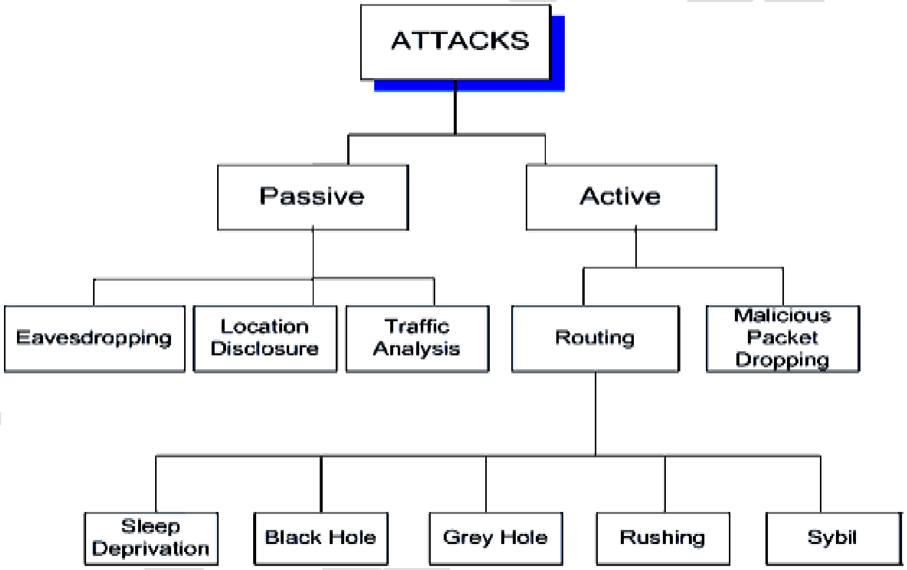

Figure: 2 Categories of Mobile Ad hoc Network Attacks

2.1 Active attack

The information which is routing through the nodes in MANET is altered by an attacker node. Attacker node also streams some false information in the network. Attacker node also do the task of RREQ (re request) though it is not an authenticated node so the other node rejecting its request due these RREQs the bandwidth is consumed and network is jammed [12].

Black hole attack: In black hole attack, a malicious node sends false routing information and claiming that it has an original route and causes other good nodes to route data packets through the malicious one [16]. All traffic will be routed through the attacker , and the attacker can misuse or discard the traffic .

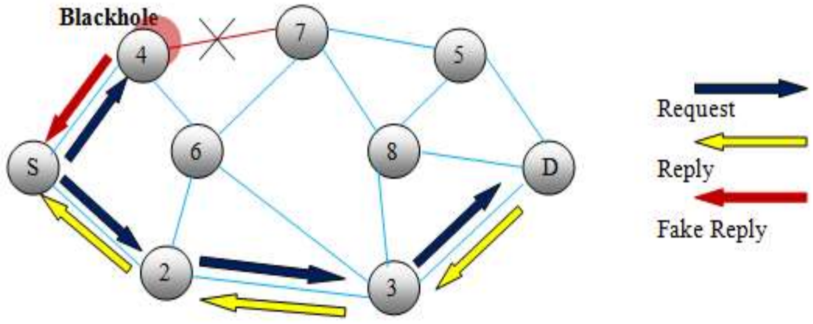

Figure: 3 Black Hole Attack

Worm hole attack: In Worm hole attack two malicious nodes make a tunnel b/w them. This tunnel is called worm hole. Wormhole attack is is additionally known as the tunneling attack. An attacker receives a packet at one point and tunnels it to another malicious node in the network. This way beginner assumes that he found the shortest path in the network. This tunnel between two colluding attackers is called the wormhole [1, 2, and 3]. The seriousness of this attack is that it can be launched against all communication that provide confidentiality and authenticate .

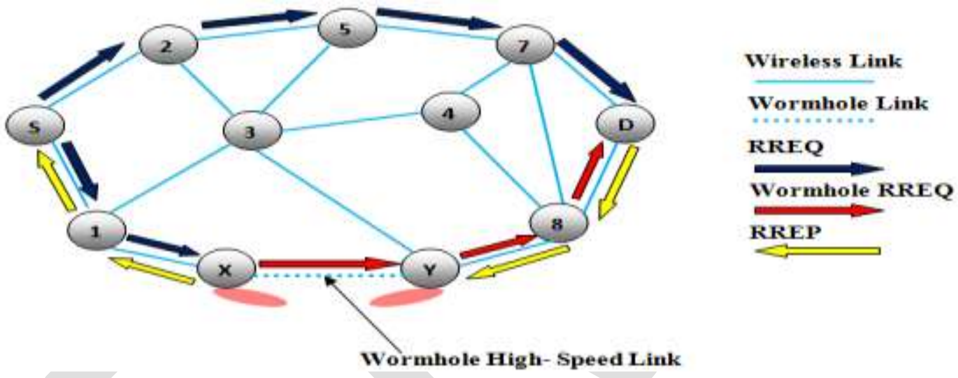

Figure: 4 Worm hole attack:

Spoofing: When a malicious node miss-present his identity, thus this manner it will alter the vision of sender and sender change the topology [1].

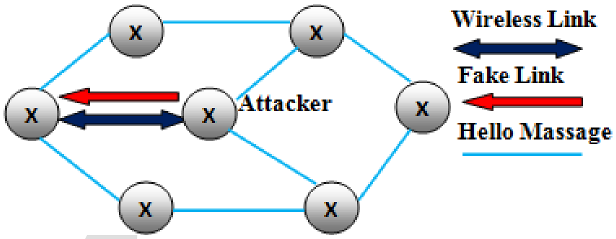

Figure: 5 Spoofing Attack

Rushing attack: In rushing attack, an attacker comes between the route of sender and receiver. When sender send packet to the receiver, then attacker intercept the packet and forward to receiver. Attacker performs duplicate suppression mechanism and then sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so that receiver will be busy continuously. This way, it reduces the efficiency of receiver [7].

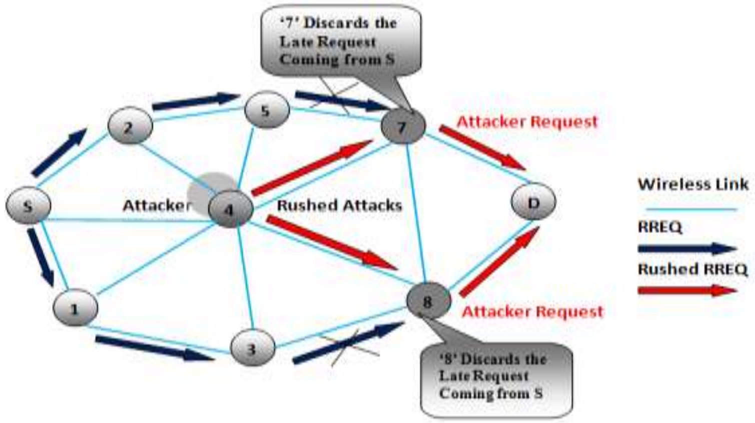

Figure: 6 Rushing Attack

Fabrication: When a malicious node generates the false routing message. This means malicious node generate the incorrect information about the route between devices [12].

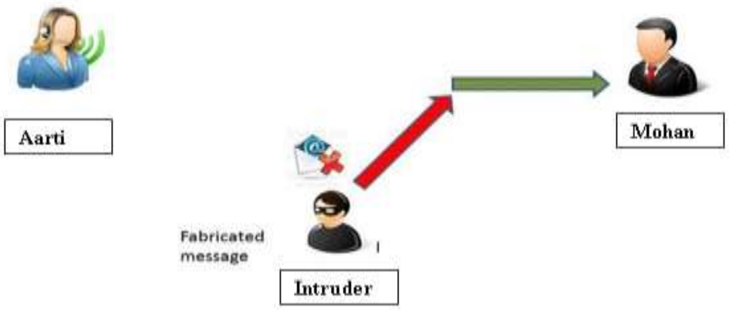

Figure: 7 Fabrication Attack

Modification: Malicious node performs some modification within the routing, in order that sender sends the message through the long route. This cause time delay and communication delay is occurred between sender and receiver [13].

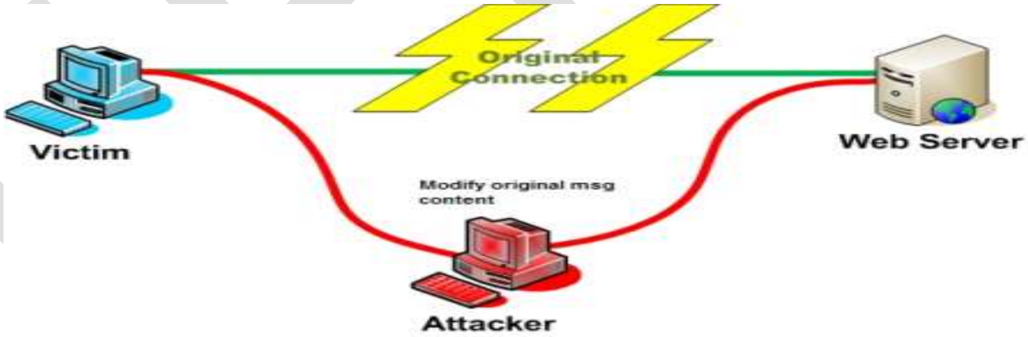

Figure: 8 Modification Attack

Denial of services: In this form of attack, malicious node causing the message to the node and consume the bandwidth of the network. The aim of malicious node is to be busy to the network node. This way, if a message from the authorized node will come, then receiver will not receive the message because he is busy and beginner should wait for the receiver response [14].

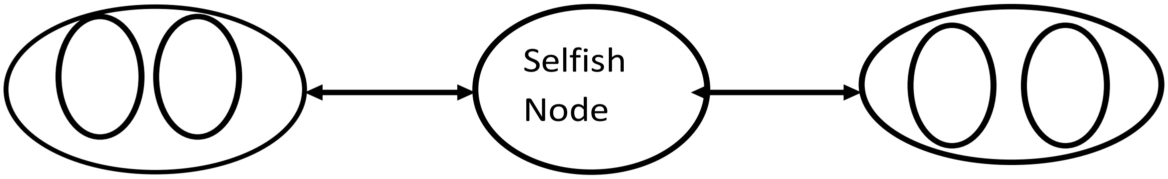

Figure: 9 Denial of Services Attack

Sinkhole Attack: It is a service attack that prevents the base station from obtaining complete and correct information [9]. In sinkhole attack, a compromised node tries to attract the data to it from his all neighboring node. Selective forwarding, modification or even dropping of data can be done by the sinkhole attack [11]

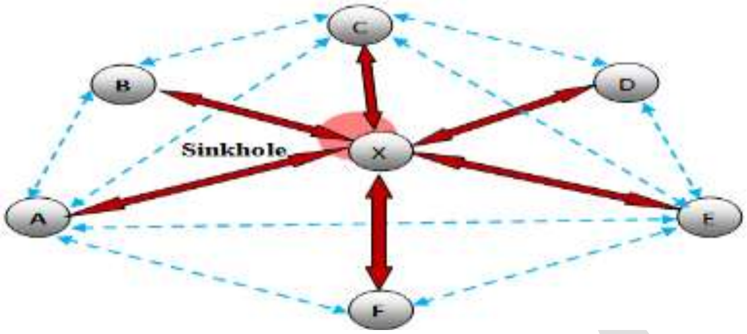

Figure: 10 Sinkhole Attack

Sybil Attacks: Sybil attack refers to the multiple copies of malicious nodes. It may be happen, if the malicious node shares its secret key with different malicious nodes. This manner the amount of inflated within the network and therefore the chance of the attack is additionally inflated.. If we have a tendency to use the multipath routing, then the possibility of choosing a path within the network, those contain the malicious node will be inflated [1, 2, 3].

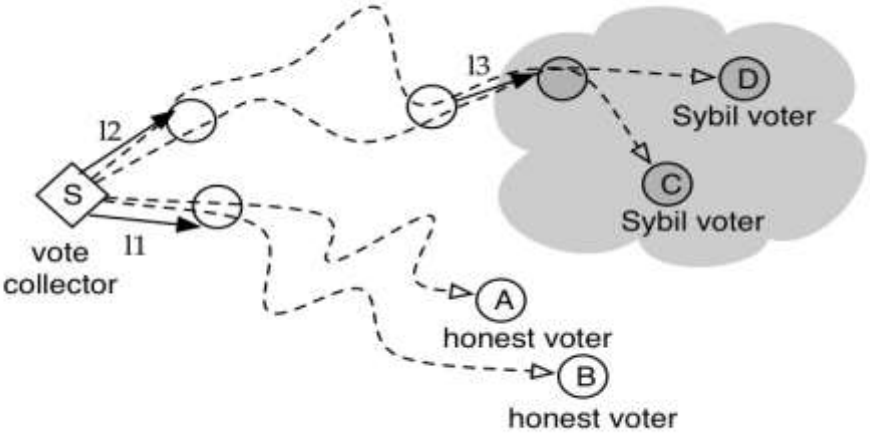

Figure: 11 Sybil Attack

Gray Hole Attack: A grey hole attack (GH) [24] is a special case of the BH attack, in which an intruder first captures the routes, i.e. becomes part of the routes in the network (as with the BH attack), and then drops packets selectively. For example, the intruder may drop packets from specific source nodes, or it may drop packets probabilistically or drop packets in some other specific pattern. As we noted above, BH and GH attacks are different in nature from packet dropping attacks, where the attacker simply fails to forward packets for some reason. BH and GH attacks on the other hand comprise two tasks: the attacker first captures routes and then either drops all packets (BH attack) or some packets (GH attack).

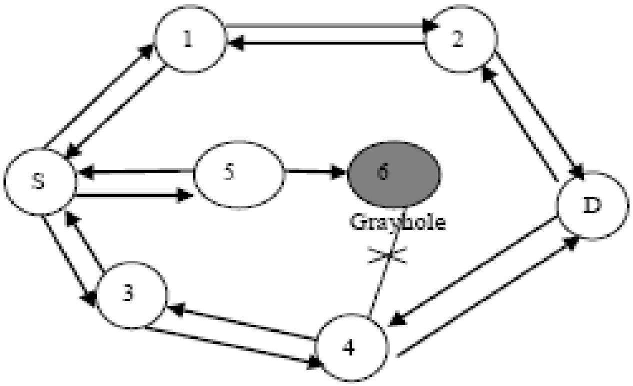

Figure: 12 Gray Hole Attack

Table: 2 Different Approaches for attacks

S. No.	Approaches	Type of Detection	Problems
1.	Packet Forwarding Misbehavior	Single Black Hole	Falsely Accusing
2	Dynamic Anomaly Detection	Single Black hole	High False Alarm Rate
3	Core Maintenance of Allocation Table Approach	Collaborative black hole	Time delay
4	Neighborhood-Based Approach	Single Black Hole	High False Positive
5	Bluff- Based Approach	Single Black Hole	More Time Delay
6	Authentication & Sequence No Based	Single Black Hole	Limited sequence No
7	REACT(Hash Based Defending)	Single Black Hole	Resource consumption & Identification delay
8	Random two-hop ACK	Single Black Hole	Less Efficient
9	DPRAODV	Single Black Hole	Time delay & Normalized Overhead

Table: 3 Related Work

Author	Attack	Solution	Remarks
Cerri. D Politec di Milan, Ghioni A	Blackhole Attack	SAODV	Requires heavyweight asymmetric cryptographic algorithm

Seung Yi, Prasad Naldurg, Robin Kravets [20]	Replay Attacks	SAR	Require excessive encrypting and decrypting at each hop. Discovered route may not be shortest path
Davide Cerri and Alessandro Ghioni	DOS, Man in the Middle Attack	Adoptive SAODV	Routing Overhead and High Processing Power, Time delay in establishing routes
Bridget, Brain Neil, Elizabeth Royer, Clay Shields	Active Attacks	ARAN	Cannot defend against authenticated Selfish nodes
Chu-Hsing Lin,Tunghai Univ, Taipei,Wei-Shen Lai,Yen-Lin Huang; Mei- Chun Chou [21]	Wormhole attack	SEAD	It doesn't provide a way to prevent an attacker from tampering with "next hop" columns. Instead, it relies on doing neighbor authentication, which is bad.

III. Passive Attack: In passive attack there is not any alteration within the message that is transmitted. There is an attacker (intermediated node) between sender & receiver that reads the message. This intermediate attacker node is additionally doing the task of network observance to analyze which kind of communication is goes on. The name of some passive attacks is Eavesdropping, traffic analysis, and Monitoring [11].

a. Eavesdropping: Eavesdropping is a passive attack, that occurred within the mobile ad-hoc network. The aim of eavesdropping is to find some secret or confidential information that should be kept secret during the communication. This confidential information may be privet or public key of sender or receiver or any password [17].

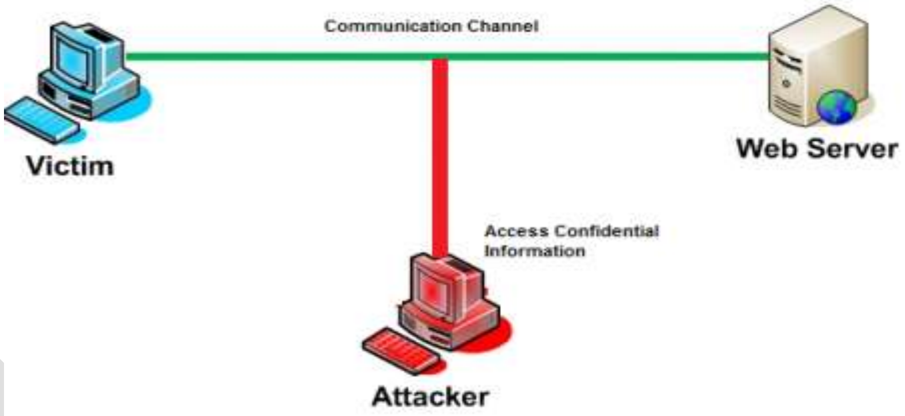

Figure: Eavesdropping

b. Traffic analysis: In this type of attack, an attacker tries to sense the communication path between the sender and receiver. This way attacker found the amount of data which is travel between the route of sender and receiver. There is no alteration in data by the traffic analysis [17].

c. Monitoring: Monitoring is a passive attack in which attacker can see the confidential data, but he cannot change the data or cannot modify the data [23].

IV. 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 [23]:* 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.

4. Worm Hole Attack *[13]:* 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.

5. Rushing Attack: (I) SEDYMO [15]: 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 [16]: 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 [16]: 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.

V. CONCLUSION

We have tried to categorize the various varieties of unintentional security attacks only supported on their characteristics to significantly cut back the mitigation amount. By transportation the attacks under these two broad categories the complicacy of naming additionally reduces. We have also kept a close look on the prevailing algorithms required 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 a lot of powerfully bind them into these categories and to ably design more powerful algorithm in mitigating information.

REFERENCES:

[1]. Karan Singh, Rama Shankar Yadav and Ranvijay, "A Review Paper on Ad-Hoc Network Security, International Journal of Computer Science and Security", Volume (1): Issue (1) 2010

[2]. J. Nafeesa Begum, K.Kumar and Dr.V.Sumathy, "Multilevel Access Control in a MANET for a Defense Messaging system using Elliptic Curve Cryptography", International Journal of Computer Science and Security, Volume (4): Issue (2) 2012

[3]. Jun Jiang and Symeon Papavassiliou, "Detecting Network Attacks in the Internet via Statistical Network Traffic Normality Prediction", Journal of Network and Systems Management, Vol. 12, No. 1, March 2004

[4]. T.V.P.Sundararajan , Dr.A.Shanmugam, "Performance Analysis of Selfish Node Aware Routing Protocol for Mobile Ad Hoc Networks**"**, ICGST-CNIR Journal, Volume 9, Issue 1, July 2009

[5]. Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010

[6]. Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, DAWWSEN: "A Defense Mechanism Against Wormhole Attacks In Wireless Sensor Networks", International Conference on Innovations in Information Technology (IIT'05), 2005

[7]. Mehdi Kargar and Mohammad Ghodsi, "Truthful and Secure Routing in Ad Hoc Networks with Malicious and Selfish Nodes", International Journal of Security and its Applications Vol. 3, No. 1, January, 2009

[8]. B.Revathi, D.Geetha, "A Survey of Cooperative Black and Gray hole Attack in MANET" International Journal of Computer Science and Management Research Vol 1 Issue 2 September 2012.

[9]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magazine, vol. 40, no. 10, October 2002.

[10]. Vishnu K, and Amos J .Paul," Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks." International Journal of Computer Applications 2010, Volume 1-No.22, pp.38-42.

[11]. Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[12]. Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehaviour in Mobile Ad-Hoc networks", Journal of Internet Engineering, 2:1, 2008.

[13]. Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehaviour in Mobile Ad-Hoc Networks Centre for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

[14]. H. Weerasinghe and H. Fu. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In Future generation communication and networking (fgcn 2007), volume 2, pages 362–367. IEEE, 2007.

[15]. H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato. A dynamic anomaly detection scheme for aodv- based mobile ad hoc networks. Vehicular Technology, IEEE Transactions on, 58(5):2471 –2481, jun 2009.

[16]. Sarita Choudhary, Kriti Sachdeva. Discovering a Secure Path in MANET by Avoiding Black/Gray Holes. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-3, August 2012.

[17]. Sun B, Guan Y, Chen J, Pooch UW, "Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[18]. Al-Shurman M, Yoo S-M, Park S , " Black Hole Attack in Mobile Ad Hoc Networks". 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.

[19]. Prof. Sanjeev Sharma, Rajshree, Ravi Prakash, Vivek , "Bluff-Probe Based Black Hole Node Detection and prevention", IEEE International Advance Computing Conference (IACC 2009), 7 March 2009.

[20]. Djenouri D, Badache N (2008) Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6

[21]. Wang W, Bhargava B, Linderman M (2009) Defending against Collaborative Packet Drop Attacks on MANETs. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009

[22]. Kozma W, Lazos L (2009) REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009

[23]. 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.

[24]. 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.

[25]. 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

[26]. 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

[27]. 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

[28]. 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

[29]. 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

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

[31]. 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

[32]. 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

[33]. 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.

[34]. 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

[35]. 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