Detection and Prevention Mechanism of Black Hole and Sybil Attack in Mobile Ad Hoc Network: A Review

Aparna Raj
Department of Electronics
and Communication Engineering,
Sagar Institute of
Science and Technology,Bhopal

Pankaj Kumar Vyas
Department of Electronics
and Communication Engineering,
Sagar Institute of Science and
Technology,Bhopal

ABSTRACT

Security is the major anxiety in mobile ad hoc network because of its characteristics such as lack of central coordination, dynamic topology; infrastructure less. In such network nodes can easily be in and out and each node has capability to route the packets.Ad hoc network is more susceptible to various kinds of threats such as black hole, Sybil attack, worm hole attack, denial of service attack, replay attack etc. Black hole attack advertises itself that has fresh shortest or optimum route to the destination and Sybil attack may engender false identities of number of additional nodes. For the detection and removal of these attack different author proposed various mechanisms. In this paper, we present the review of literature of an assortment of proposed mechanism of black hole and Sybil attack. We also discuss the pros and cons of proposed and implemented mechanism of different authors.

Keywords

MANET,Black hole attack, Security threats, dynamic

1. INTRODUCTION

Mobile Ad-Hoc Networks are self-governing and decentralized wireless systems. MANETs comprises of mobile nodes that are open in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance (PDA), MP3 player and personal computer that are contributing in the network and are mobile. These nodes can behave as host/router or both at the same time. They can form uninformed topologies depending on their connectivity with each other in the network. These nodes have the capacity to configure themselves and because of their self-configuration capability, they can be deployed immediatelydevoid of the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc.

Security in Mobile Ad-Hoc Network is the most significantapprehension for the basic functionality of network. The accessibility of network services, confidentiality and reliability of the data can be achieved by assuring that security issues have been met. MANETs repeatedlyundergo from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battlefield circumstances for the MANETs against the security threats. The MANETs work devoid of a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more susceptible to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication [1, 2]. Mobile nodes present surrounded by the range of wireless link can overhear and even contribute in the network. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to present secure communication and transmission, the engineers must understand dissimilar types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can undergo from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

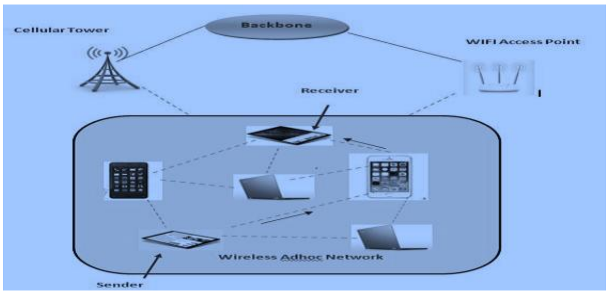


Figure 1: Architecture of Mobile Ad hoc Network

Black hole [3] and Sybil attack [4] is one of the more serious threats which may intercept the network.

Black hole is a kind of denial of service attack which broadcast itself that has optimum path to the destination while Sybil attack is the attack in which the identities of the node are subverted and large number of pseudonymous identities is produced to gain the access of the network. Lots of detection and prevention mechanism has been developed from such serious threat which we will discuss below. In this paper, we present the literature work about black hole and Sybil attack prevention and detection together with their advantages and disadvantages. The remaining section of the paper is organized as follows: In section II describe the overview of black hole and Sybil attack. Section III presents the related work about detection and prevention mechanism of both the attack. In Section IV describe detection mechanism of black hole and Sybil attack. Last section gives overall conclusion of the paper.

2. OVERVIEW OF BLACK HOLE AND SYBIL ATTACK

In this section of the paper we are describing the black hole and Sybil attack in mobile ad hoc network:

2.1 Black Hole Attack

A black hole attack is a kind of Denial of service attack in mobile ad hoc networks. In this attack, a malicious node sends [3] a fake RREP packet to the source node that has initiated a route discovery, in order to show itself as a destination node or an intermediate node to the actual destination node. In such a case the source node would send all of its data packets to the malicious node the malicious node then absorbs all the packets and drops them fully or sometimes partially. As a result source and destination node will not be able to communicate with each other.

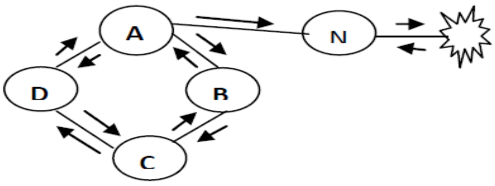
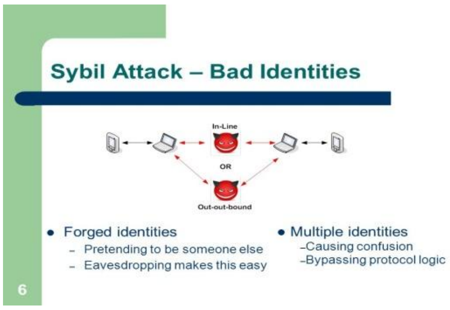


Figure 2.1: Black Hole attack by malicious node N

Consider the case in figure 2.1 where A is the source node D is the destination node and N is the malicious node here node A starts with the route discovery process then the node N advertises itself as having a valid shortest route to the destination, even though the route is false with the purpose of intercepting packets. Moreover a malicious node does not need to check its routing table when sending a false message; its response is more likely to reach the source node first. This makes the source node think that the route discovery process is complete, ignore all other reply messages and begin to send data packets. As a result, all the packets through the malicious node are simply absorbed discarded and then lost. The malicious node could be said to form a black hole in the network. Sometimes these malicious nodes cooperate with each other with the same aim of dropping packets these are known as cooperative Black Hole nodes and the attack is known as Cooperative Black Hole attack.

2.2 Sybil Attack

We argue that it is practically impossible, in a distributed computing environment, for initially unknown remote computing elements to present convincingly distinct identities. With no logically central, trusted authority to vouch for a one-to-one correspondence between entity and identity, it is always possible for an unfamiliar entityto present more than one identity, except under conditions that are not practically realizable for large-scale distributed systems. Peer-to-peer systems commonly rely on the existence of multiple, independent remote entities to mitigate the threat of hostile peers. Many systems replicate computational or storage tasks among several remote sites to protect against integrity violations (data loss). Others fragment tasks among several remote sites to protect against privacy violations (data leakage). In either case, exploiting the redundancy in the system requires the ability to determine whether two ostensibly different remote entities are actually different. If the local entity has no direct physical knowledge of remote entities, it perceives them only as informational abstractions that we call identities. The system must ensure that distinct identities refer to distinct entities; otherwise, when the local entity selects a subset of identities to redundantly perform a remote operation, it can be duped into selecting a single remote entity multiple times, thereby defeating the redundancy. We term the forging of multiple identities a Sybil attack on the system [4]. It is tempting to envision a system in which established identities vouch for other identities, so that an entity can accept new identities by trusting the collective assurance of multiple (presumably independent) signatories, analogous to the PGP web of trust for human entities. However, our results show that, in the absence of a trusted identification authority (or unrealistic assumptions about the resources available to an attacker), a Sybil attack can severely compromise the initial generation of identities, thereby undermining the chain of vouchers.


Sybil Attack – Bad Identities

- Forged identities
  - Pretending to be someone else
  - Eavesdropping makes this easy
- Multiple identities
  - Causing confusion
  - Bypassing protocol logic

6

Figure 2.2: Sybil attack –Bad Identities

3. LITERATURE SURVEY

So many researchers have proposed the security mechanism against attacks. The most recent research in field of Black hole and Sybil attack is discussed in this section.

3.1 Related Work

Author/ researchers	**Description**
Singh and Kumar [1]	Here this method is for detecting black-hole attack in mobile ad hoc networks, are extremely vulnerable to attacks compared to conventional wired networks due to its mobility and broadcast in nature. In this case black-hole attacks can be easily deployed by the adversary. To defend against this attack, they used an approach to detect whether there is present a black hole and a path (routing) recovery protocol to set up a correct path for the real destination. Their method has a remarkable advantage that it can be implemented with a slight modification in basic AODV protocol without much affecting the efficiency, throughput and end to end delay.
Baberwal and Bundele [4]	Presented a work a hybrid mechanism is presented that will perform the detection as well as the prevention to these kind of attacks. Their work was performed in two phases: first, sending of fake RREQ packet

	for identification of malicious node, second, ensuring that the malicious node will never take part in routing in future
Pareek and Sharma [5]	Implemented the Sybil Attack using MAC address to detect the Sybil nodes in the network and also prevent it. Simulation tool used for the implementation is NS2.35. The comparative analysis is done using throughput and packet delivery ratio performance metrics.
Woungang et al. [16]	Proposed a novel scheme for Detecting Blackhole Attacks in MANETs (so-called DBA-DSR) is introduced. The BDA-DSR protocol detects and avoids the blackhole problem before the actual routing mechanism is started by using fake RREQ packets to catch the malicious nodes. Simulation results are provided, showed that the proposed DBA-DSR scheme outperforms DSR in terms of packet delivery ratio and network throughput, chosen as performance metrics, when blackhole nodes are presented in the network
Pooja et al. [6]	Here Hint-based Probabilistic routing protocol is used to propose a local utility function based scheme to detect black hole nodes. Then comparison of the network performance in the presence of a black hole and in the absence of black hole using different performance metrics like packet drop, packet delivered throughput and overhead ratio in the network
Siddiqua et al. [7]	Proposed a secure knowledge algorithm which aims to detect and prevent the black hole by considering the packet drop reasons in promiscuous mode. Existing AODV routing protocol is modified to detect and prevent the black hole attack The experiment results showed that our proposed algorithm secure the AODV against black hole attack in MANETs.
Karthika and Vanitha [8]	Proposed a probabilistic misbehavior detection scheme is highly desirable to assure the secure DTN routing as well as the establishment of the trust, among DTN nodes. A zone (routing zone) of a node is used to collect the node information within the range. In this protocol, it cannot achieve the packet delivery ratio, performance and data loss rate.
Singh and Singh [10]	Proposed a method in which broadcast synchronization (BS) and relative distance (RD) method of clock synchronization is used to prevent the black hole nodes. In this internal and external clock node compare with the threshold clock if both the clock time is greater than the threshold then it is found that the node is malicious. This method can easily detect and prevent the block-hole node.
Jain and Nigoti [9]	Proposed the Sybil Detection and Prevention (SDP) against Sybil attack. The property of this attack is to reply with every neighbors through multiple recognition (MR) value of itself i.e. fake identity, fake generated specification of itself in dynamic network. The SDP is able to find routes that deviates from these compromise nodes and provides secure path in between source to designation. The SDP has detected the malicious nodes and capture the malicious information of MR value generated in MANET. The better routing performance is devalued through performance parameters such as throughput and packets drop. The proposed scheme is improves throughput, minimizes data loss and provides secure routing
Liang Xiao et al. [17]	Proposed Channel-Based scheme for Sybil attacks Detection in Wireless Networks. To detect Sybil attacks analysis done on enhanced physical-layer authentication method, employing the spatial instability of radio channels in environments with rich scattering, as is ordinary in indoor and urban environments. A hypothesis test is build to detect Sybil clients for both narrowband and wideband wireless systems, like Wi-Fi and WiMax systems. Based on the existing channel estimation mechanisms, this method can be easily realized with low overhead
Piro et al. [21]	Showed that mobility can be used to enhance security. Specifically, showed that nodes that passively monitor the traffic in the network which can detect a Sybil attacker that uses a number of network identities simultaneously. We show through simulation that this detection can be done by a single node, or that multiple trusted nodes can join to improve the accuracy of detection. They then showed that although the detection mechanism will falsely identify groups of nodes traveling together as a Sybil attacker, we can extend the protocol to monitor collisions at the MAC level to differentiate

	between a single attacker spoofing many addresses and a group of nodes traveling in close proximity.
Kumar et al. [12]	Proposed system works considering the Certification Authority as one parameter and RSSI as the other parameter. The RSSI is used to form the cluster and to elect the cluster head. The CA's responsibility is given to the CH. Whenever huge variations occur in RSSI on neighbour's entry and exit behaviour, the Certification Authority comes into play. The CA checks the certification of a node. If it is not valid, its certificate is revoked otherwise it is free to communicate in the network
Shehzad et al. [11]	Proposed a novel mechanism that ensures the detection of both Simultaneous Sybil attack and Join and Leave Sybil attack in the network. The proposed mechanism handles both attacks individually by dividing proposed mechanism in two sections Hash Function Mechanism for detecting Simultaneous Sybil attack and Request Threshold validation Mechanism for join and leave Sybil attack. The proposed hash function mechanism for the detection of Sybil attack solves the drawback of lacking central authentication in the network. Request Threshold validation mechanism do not allow nodes to compromise its identity in the network
Wei Wei et al. [15]	Proposed the approach called Sybil defender for social network. This approach is based on performing a limited number of random walks within the social graphs. Conducting the experiment of the real world topologies, researchers claimed that this strategy is the most efficient and effective in order to identify the Sybil node and Sybil communities around the Sybil node. Also this strategy is useful in limiting the attacking edges in online social networks by relationship rating

3.2 Performance parameter

There are various measuring parameter in Mobile ad hoc network which is used for performance measurement of the network in which some of them we are describing below:

- **Routing overhead:** How many routing packets for route discovery and route maintenance need to be sent so as to propagate the data packets.
- **Average Delay:** Represents average end-to-end delay and indicates how long it took for a packet to travel from the source to the application layer of the destination.
- **Throughput:** This metric represents the total number of bits forwarded to higher layers per second. It is measured in bps
- **Packet Delivery Ratio:** The ratio between the amount of incoming data packets and actually received data packets.

4. DETECTION MECHANISM OF BLACK HOLE AND SYBIL ATTACK

This section describes different black hole and Sybil attack detection technique:

4.1 Black Hole Detection Mechanism:

A. Next Hop Information Based Method

In this method Ad-hoc On-Demand Distance Vector (AODV) and proposed a solution for black holes attacks used. They discussed a protocol that needs the intermediate nodes to send RREP message along with the next hop information. When the source node get this information, it sends a FREQ to the next hop to verify that the replied node (i.e. the node that just sent back the RREP packet) a route to the destination. When the next hop receives a FREQ, it sends a FREP which includes the check result to the source node. Based on information in FurtherReply, the source node judges the validity of the route. This approach helps to know the reliability of the replied node [19]. In this protocol, the RREP control packet is modified to attach the information about next hop. Since, the source node will again send RREQ to the node specified as next hop in the received RREP, this exercise not only increases the routing overhead but also end-to-end delay. In addition, the intermediate node requires to send RREP message twice for a single route request. This method could prevent individual black hole attacks but cannot avoid cooperative attacks, where the next hop node cooperate with the replied node in malicious activity and reply with "yes " for FREQ sent by source node to it and the source node will trust on next hop and send data within the replied node.

B. Exponential Trust based mechanism:

This mechanism [20] is based on the Exponential Trust Based Mechanism. In their proposed method one factor is defined to calculate the number of packets dropped at each node and named it as Streak counter and also trust factor is maintained at each node. The trust factor decreases at each consecutive packet drop and with the help of this malicious node is detected.

C. Distributed Cooperative Mechanism (DCM): distributed and cooperative mechanism (DCM) method is used to solve the collaborative black hole attacks[21]. Since, nodes works cooperatively, they can detect, investigate, and mitigate multiple black hole attacks. The DCM has four phases: In the local data collection phase, each node in the network constructs and maintains an estimation table. Information of overhearing packets is evaluated by each node to find out whether there is any malicious node. If there is one doubtful node, the detect node enters to the local detection phase to identify whether there is possible black hole. The initial detection node sends a check packet to ask the cooperative node. If it receives the positive inspection value, the doubtful node is regarded as a normal node. Otherwise the initial detection node runs the cooperative detection procedure, and deals with broadcasting and notifying all one-hop neighbors to participate in the decision making process. The network traffic is increased because the notify step utilizes broadcasting, Therefore, a constrained broadcasting algorithm is run to limit the notification range within a fixed hop count. A threshold say thr contains the maximum hop count range of cooperative detection message. Lastly, the global reaction phase is executed to set up a notification system to send warning messages to the whole network. Global reaction phase contains some reaction modes. Role of first reaction mode is to notify all nodes in the network, but it might waste lots of communication overhead. Each node maintains its own black hole list and arranges its data transmission route in other mode, however there is a chance to exploit this route by malicious nodes and requires more operation time. In the simulation outcome, the notification delivery ratio is from 64.12 (thr = 1) to 92.93% (thr = 3) when different threshold values are used. On Comparing with the popular AODV routing protocol in MANET, the result shows that DCM has a higher data delivery ratio and detection rate even if there are multiple black hole nodes. Even though the control overhead can be reduced by using distributed design method, DCM still wastes few overhead inevitably.

D. DRI Table and Cross Checking Scheme :The data routing information (DRI) table and cross checking technique to identify the cooperative black hole nodes, and used modified Ad-hoc On-demand Distance Vector (AODV) routing protocol to build up this methodology [22,23]. All nodes need to have an extra DRI table, in which 1 represents for true and 0 for false. The table has two entries, “From” to have the information on routing data packet from the node and “Through” to have the information on routing data packet through the node.

Table 1

Node_ID	Routing_Information	
	From	**Through**
2	0	0
6	1	1

As shown in Table 1, the entry 1 1 means that node 1 has routed data packet from or through node 6 successfully, and the entry of 0 0 means that node 1 has not routed any data packets from or through node 2. The course of action of proposed solution is described as follows. The source node sends Route Request (RREQ) message to each node and wait for Route Reply (RREP) message. Then it sends packets to the node which replies the Route Request (RREP) packet. The intermediate node then sends next hop node (NHN) information and DRI table to the source node (SN). Now source node cross checks its own table and the DRI table received from the intermediate node to verify the IN’s honesty. After that, source node sends the further request (FREQ) message to IN’s next-hop-node for gathering its routing information, including the current NHN, the NHN’s Data Routing Information (DRI) table and its own DRI table. Lastly, the SN compares the above details by cross checking to judge the malicious nodes in the routing path. Authors proposed a detection method to mitigate the multiple black hole problems and the collaborative attacks, and showed the simulation result in [Paper_3_37]. The simulation result shows that the performance of this solution is almost 50% better than other solutions. However, it wastes 5 to 8% communication overhead, and increases the packet loss percentage very slightly as a delay to secure route discovery.

4.2 Sybil Attack Detection Mechanism

A. Authentication and Public Key Mechanism

Detecting Sybil attacks based on this approach have been a focal point of many research works. It is an understandable that using authentication mechanism and keys are the best and only approach that can fully eliminate Sybil attacks [24]. But since Public Key Infrastructure is heavy and could be complex solution, it is difficult to implement and sometimes considered unrealistic approach towards the detection of Sybil attacks n Vehicular ad hoc networks. More time is consumed and message size is significantly increased Public key encryption or message authentication systems which intern increases the memory requirement for such approach.

B. Foot Printing Mechanism

This is another proposed mechanism [24] for the detection of Sybil attacks in vehicular ad hoc networks based on using the authorized event messages as vehicle trajectory by preserving the privacy of vehicles in the network. The detection mechanism is carried out by the vehicle and the road side unit which act as a conversation holder by transmitting the messages among the vehicles.

C. Certificate Issuing Mechanism

This way is used to detect the Sybil entities is issuing certificate to the vehicles. In this approach [24] researches propose to issue the timestamp certificate to the vehicle whenever they pass by a road side unit. This approach does not involve any use of the public key infrastructure and only road side unit are able to generate and issue the certificates. The vehicle after gaining the timestamp certificate can use this for authentication purposes and also to obtains new certificates form the next road side unit.

D. Hash Key Mechanism

Each individual node detects Sybil attackers by validating the Hash received alongwith message by neighbor, message can be keep alive messages, data transmissions and routing requests or replies [17]. Afterreceiving message node gets Hash of sender and compares it with the previous Hash received in Hello message for the validation of its identity. If Identity or Hash differs to that of Hash received along with hello message than node is nominated as Sybil and node is blocked from any communication. Thus Hash mechanism detects Simultaneous Sybil attack that tries to obtain multiple identities for incorporating storage, bandwidth or computation of network resources.

5. CONCLUSION

In wireless ad hoc network security is the key issues because of its dynamic and lack of centralization. In such network, nodes may gets compromised from various security threats in which black hole and Sybil attack is one of them. Black hole attack broadcast itself that it has shortest route to the destination while Sybil attack makes multiple identities to confound other nodes and diminish the trust of legal nodes in the network. In this paper we present some literature study of the black hole and Sybil attack detection mechanism.

We also discuss some mechanism for detection of black hole and Sybil but some approaches are less efficient to mitigate these attack so in future work design such mechanism which efficiently detect and prevent it to harm the network and also reduces the computation time of the system and less complex to design.

6. REFERENCES

[1] Vinay Singh, Sanjay Kumar “Black Hole Detection in MANET Using Modified AODV Protocol”, International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2016 ISSN (Online): 2320-9801.

[2] Nidhiya Krishna “Detection and Prevention of Sybil Attack in Networks”, International Journal of

Engineering Science and Computing, April 2016, Volume 6 Issue No. 4 ISSN 2321 3361.

[3] Bhoomi Patel, JyotiParmar “Detection of Black Hole And Sybil Attack in MANET”, International Journal Of Innovative Research In Technology, Volume 2 Issue 8, January 2016 , ISSN: 2349-6002.

[4] Deepak Baberwal, Mahesh Bundele, “Detection and Prevention of Black Hole Attack for Dynamic Source Routing in Mobile ad-hoc Network”, International Journal of Innovations & Advancement in Computer Science. ISSN 2347 – 8616 Volume 4, Special Issue March 2015.

[5] AnamikaPareek, Mayank Sharma “Detection and Prevention of Sybil Attack in MANET using MAC Address”, International Journal of Computer Applications (0975 – 8887) Volume 122 – No.21, July 2015.

[6] Pooja, R. K. Chauhan “An assessment based approach to detect black hole attack in MANET”, International Conference on Computing, Communication & Automation (ICCCA), in 2015 Proceeding of IEEE Page(s):552 – 557.

[7] Ayesha Siddiqua, KotariSridevi ; Arshad Ahmad Khan Mohammed “Preventing black hole attacks in MlANETs using secure knowledge algorithm”, International Conference on Signal Processing And Communication Engineering Systems (SPACES), 2015 Proceeding of IEEE Page(s): 421 – 425.

[8] S. Karthika, N. Vanitha, “Secure Routing Protocol in Delay Tolerant Networks Using Fuzzy Logic Algorithm”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 4, Issue 5, May 2015, ISSN (Print) : 2320 – 3765.

[9] Priya Jain, RashmiNigoti “A Novel Technique for Sybil Attack Detection and Prevention in MANET”, International Journal of Computer Applications (0975 – 8887) Volume 130 – No.9, November 2015.

[10] Harsh Pratap Singh, Rashmi Singh, “A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc network using AODV protocol”, International Conference on Electronics and Communication Systems (ICECS) 2014 , Page(s):1 - 8 Print, ISBN:978-1-4799-2321-2.

[11] Danish Shehzad, ArifIqbal Umar, Noor Ul Amin, and WaqarIshaq, “A Novel Mechanism for Detection of Sybil Attack in MANETs”, International conference on Computer Science and Information Systems (ICSIS’2014) Oct 17-18, 2014 Dubai (UAE).

[12] R. Vintoh Kumar, P. Ramesh , H. Abdul Rauf “Cluster based enhanced Sybil attack detection in MANET through integration of RSSI and CRL”, International Conference on Recent Trends in Information Technology (ICRTIT), 2014 Page(s):1 – 7.

[13] Dr. DeepaliVirmani ,ManasHemrajani , ShringaricaChandel, “Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network”. In proceeding of IEEExplore-2014.

[14] GayatriWahane, Ashok Kanthe “Technique for Detection of Cooperative Black Hole Attack In MANET”, IOSR Journal of Computer Science (IOSR-JCE) 2014 e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 59-67.

[15] Wei Wei, FengyuanXu, Chiu C. Tan and Qun Li “Sybil Defender: A Defense Mechanism for Sybil Attacks in Large Social Networks” IEEE Transaction on Parallel and Distributed Systems, Dec. 2013. Vol. 24, P. 2492-2502.

[16] Isaac Woungang, Sanjay Kumar Dhurandher, RajenderDheeraPeddi and Mohammad S. Obaidat “Detecting blackhole attacks on DSR-based mobile ad hoc networks”, International Conference on Computer, Information and Telecommunication Systems (CITS), Proceeding of IEEE on May 2012 Page(s):1 – 5.

[17] Liang Xiao, Larry J. Greenstein, Narayan B. Mandayam, “Channel-Based Detection of Sybil Attacks in Wireless Networks” IEEE Transactions on Information Forensics and Security, Vol. 4, No. 3, September 2009

[18] K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007.

[19] Yu CW, Wu T-K, Cheng RH, Chang SC (2007) A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network. Paper presented at the PAKDD workshops, Nanjing, China, 22-25 May 2007.

[20] Weerasinghe H, Fu H “Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation”, Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007.

[21] Chris Piro, Clay Shields ; Brian Neil Levine “Detecting the Sybil Attack in Mobile Ad hoc Networks”, Securecomm and Workshops, Proceeding of IEEE 2006 Page(s):1 – 11.

[22] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K (2003) Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.

[23] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

[24] P. V. Jani “Security within Ad-Hoc Networks,” Position Paper, PAMPAS Workshop, Sept. 16/17 2002.