A Novel Technique for Sybil Attack Detection and Prevention in MANET

Priya Jain
Department of Information Technology
Samrat Ashok Technological Institute
Vidisha, India

Rashmi Nigoti
Department of Information Technology
Samrat Ashok Technological Institute
Vidisha, India

ABSTRACT

The attacker quickly affected the routing performance and drops the all packets that contain some data for receiver. This research 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. Routing protocols for MANET must handle obsolete routing information to hold the dynamically changeable topology. Incorrect routing information accomplished by malicious nodes to extent drop of packets, be considered malicious information. Whereas there are adequately many correct nodes, 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 SDP has immobilized the malicious functioning of Sybil attacker and enhance routing performance in presence of attacker. 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.

Keywords

Security, MANET, SDP, Routing, Sybil attacker

1. INTRODUCTION

1.1 MANET

The MANET (Mobile ad hoc Network) is basically a collection of nodes that are movable in nature and does not rely on a predefined infrastructure or centralized administrator for communicate with each other [1] [2]. It makes use of intermediate nodes to transmit packets and if the target node is out of their radio range. In comparison to traditional wireless network, MANET is mainly based on a network i.e. decentralized infrastructure. MANET doesn't require a predefined infrastructure; hence, all the nodes are open to move everywhere [1] [2] [3]. As it is known that MANET has the capability of self-configuring and self-maintenance network without the help of any centralized infrastructure, which is frequently not feasible in serious mission applications such as in military environment or emergency operations. Least configuration and quick formation make MANET available to be used in emergency operations, where an infrastructure is not available or unfeasible to install in situations like natural or human induced tragedy, military conflicts, and various medical emergency situations. Due to these unique characteristics, MANET has become more and more widely used in the industry [4]. However, considering the detail that MANET is accepted between critic mission applications, network security is of crucial consequence. Disastrously, the open medium and remote distribution of MANET make it susceptible to different kinds of attacks. For example, owing to the nodes' lack of physical security, malicious attackers can quickly confine and compromise nodes to get attacks. In particular, in MANET, considering the evidence that maximum routing protocols, assume that every node in the network reacts cooperatively with other nodes and apparently these nodes are not malicious [5], but the chances of malicious actions are always be positive at any time in network moreover, because of MANET's distributed architecture and dynamic topology, a traditional centralized monitoring technique is no longer appropriate in MANETs. In that case, it is imperative to develop a Sybil attack Detection and Prevention (SDP) System. The SDP scheme identify the attackers and block the attacker's misbehavior procedures that affect routing performance in dynamic self established MANET. The Sybil attacker [5, 8] is generating the false multiple identities for communication to normal nodes in network. The intermediate nodes are not known the attacker is communicating with it in network abs attacker starts packets dropping.

In this paper the proposed security scheme is to achieve the complete control on routing misbehavior through Sybil attacker. The proposed scheme is identified the attacker on the basis of particular identification (ID) and this ID of the attacker is present in every node in network which received the unwanted or untruthful packets. The SDP scheme is broadcast the network ID after identification and block this attacker action.

1.2 Attacks in MANET

In MANETs attacks can be differentiated as active and passive attacks, build upon on either the normal activity of the network is disrupted or not [4] [5].

1.2.1 Passive Attack

An intruder exchanges data without altering it is called Passive attack. The attacker does not actively originate malicious actions to shark other hosts. Here, Information acquisition is main goal of the attacker that is being transmitted, thus disregarding the message confidentiality. After all the activity of the network is not disorganize, these attackers are crucial to recognize.

1.2.2 Active Attack

Attackers take part in disrupting the normal operation of the network services is called Active attack. A malicious host can construct an active attack by altering packets or by announcing fake information in the ad hoc network. It misleads routing procedures and diminishes the performance of network. External and internal attacks are comes under the category of active attack.

1.2.3 External Attack

Attacks that are coming from nodes that are not legal part of the network are called External attack. In these attacks, it is possible to disturb the conversation of an organization from the parking lot in front of the community office.

1.2.4 Internal Attack

An attack coming from compromised nodes that were once innocent part of the network are called internal attack. In ad hoc wireless network a legitimate node, that are much more oblige and laborious to observe when distinguished to external attacks.

The most of the attackers [6] [7] are affecting the performance of ad hoc network and execute malicious activities at the time of sending and receiving the data. The attackers are categorized according to different layer of network like Eavesdropping, jamming attack, Sybil attack, Black hole attack, gray hole attack [8], wormhole attack, Denial of Service (DoS) attack and so on [6] [7], because the different attacker is clash the network performance at different layer.

1.3 Routing Protocols in MANET

In MANET currently, there are mainly two kinds of routing protocols, namely, and geographic routing and topological routing [2] [9].A Routing where mobile nodes make use of topological information to provoke routing tables or examine routes directly are called topological routing. Each node appreciates its own position and form routing decisions based on the location of the destination and the location of its local neighbors in geographical routing.

The investigation of topological routing has lasted for decades, and a variety of topological routing protocols have been refined. Generally, two classes of the topological routing protocols are available, named as, proactive routing and reactive routing. Route information is propagated periodically in the network in proactive routing.

Thus, a routing table is preserved by each node which encompassing route entries to other nodes. When packets arrive at an intermediate node, the next hop can be selected by looking up the routing table. A well-known example of proactive routing is referred to as Destination-sequenced distance-vector (DSDV) [10]. In reactive routing, no routing table is maintained at the nodes. When needed, the source node triggers a route search procedure to discover the routing path to the destination. Both Dynamic Source Routing (DSR) [12] and Ad hoc On-demand Distance Vector Routing (AODV) [11] routing are referred to as representative examples of reactive routing. By exploiting the strength and avoiding the weakness of each type, hybrid topological routing protocols are proposed, such as Zone Routing Protocol (ZRP) [13], which keep up a routing zone of k-hop proactively and triggers the inter-zone route discovery reactively.

2. LITERATURE SURVEY

Many of the researchers have proposed the security schemes against attacks. The latest research in field of Sybil attack is discussed in this section.

Sohail Abbas et al. [14] present security scheme that detects Sybil identities. In this method, the legitimate identity and Sybil identity is differentiated based on the entry and exit behavior on neighborhood nodes. In this method, the node's radio range is spitted into two zones, 1.Grey zone (Outer Zone), 2.White zone (Inner Zone). The legitimate node gives its first entrance in grey zone because it gradually increases and decreases its movement. The Sybil identity at the first time displays in white zone because of frequent identity changes. Due to off identity changes, the node gives high RSSI value in its first display. Hence, it was conclude that the identity is changed. The neighborhood RSSI value is affected by the following factors, 1.Transmission rate, 2.Node's mobility, as a fast moving node also gives first appearance as high RSSI, therefore, the false positive rate is increased. He distinguish Sybil identities and new legal nodes on the basis of how nodes appear into their region (community), i.e. benign nodes emerges in the neighborhood of another nodes as nodes arrive into their radio range; as a result, the signal strength firstly receive by nodes will be quite low.

Muhammad Nawaz Khan et al. [15] investigated a system for "Intrusion Detection" in Ad hoc Mobile Networks. In this title the analysis is on distributed-ID, in each mobile node a smart agent evaluate the routing packets and also examines the complete network behaviour of MANETs. It endeavour like a Client-Server model using Markov process. The proposed local distributed- SDP demonstrate a balance between false positive and false negative rate.

Liang Xiao et al. [16] 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, either freely or mingled with another physical-layer security strategy, detection of spoofing attack is example of this.

S. Capkun et al. [17] exploited mobility to enhance security in MANETs. In a fully self-organized MANETs where there is no central authority, nodes establish security associations purely by mutual agreement. Users can activate a point to point secure side channel (SSC) using infrared or wired media between their personal devices to authenticate each other and set up shared keys when those are in close proximity to each other. The author attempts to solve the problem of impersonation and Sybil attacks by binding a user's face and identity using these SSCs. However, SSCs are based on the assumption that nodes are connected through wired or infrared connections.

B. N. Levine et al. [18] recommended to distinguishing Sybil identities through observing node fluctuations. Nodes are keeping track of identities which are usually looked together (Sybil identities) as against to the authentic distinct nodes that move independently in different directions. Anyhow, the proposal will yields high false positives where node density is immense, like in a conference hall or nodes moves in a same direction, just as a majority of soldier moving toward a target.

3. PROPOSED WORK

The goal of proposed methodology is to provide routing survivability under an adversarial model where any intermediate node or group of colluding nodes perform Sybil attacks. While some existing work provides protection against specific attacks that may be conducted by a single Sybil attacker node against different routing components, no other existing work provides an ad hoc wireless routing protocol for coping with a large set of attacks available to a set of colluding. Sybil Attack and its Prevention are described in this section. This section describes about formal definition of

Sybil attack detection and protection, for that historically analyze node behaviour and identify the attack symptoms and its behaviour after the detection process preventer node real time watch neighbour activity and while SDP detect node as attacker than block the node and re-broadcast the route packet and search the route without participation of attacker node that technique more reliable and efficient for MANET.

```
Step1: N: mobile nodes
$S_n$: set of senders ϵ N
$R_n$: set of receiver ϵ N
$SA_1$: Sybil attack different id in same time
$SA_2$: Sybil attacker different id in different time
Routing: AODV
SDP: Sybil detector and preventer
Radio-range: 550
Routine:
Broadcast-rreq($S_n$,$R_n$, radio-range)
Step2: While(next-hop != $R_n$ && node in range)
        {
                Receives packet
                Incr sequence number
                Forward-pkt to next-hop
                Incr hop-count
}
Step3: If (R found)
        {
                Established route from $S_n$ to $R_n$
                $R_n$ send ack to $S_n$
        }
// Sybil attacker node
Step4:  If($S_n$>1 && $R_n$>1 && time== $S_n$ time)
        {
                $SA_1$ in middle between $S_n$ and $R_n$
                If ($S_n$ broadcast-rreq && $SA_1$ is next-hop)
                {
                        $SA_1$ send false $R_n$ id to $S_n$
                        $S_n$ trust and send data $SA_1$
                        $SA_1$ capture and drop data from all incoming $S_n$
                }
        }
        Else If($S_n$>1 && $R_n$>1 && $S_n$ time is not equal)
                {
                        $SA_2$ send false $R_n$ id to $S_n$ in different time
                        $S_n$ trust $SA_2$ as $R_n$ node & send data to $SA_2$
                        $SA_2$ capture or drop the packet
                }

Protection:
Step5: SDP watch history profile of all neighbour
        If (profile != normal)
                {
                Identifies packet and $S_{id}$, $R_{id}$
                If($R_{id}$ = modified $SA_{1\_id}$ && time == $S_n$-time)
                {
                        Check packet drop or capture
                        Node id set $SA_1$ categories
                        }
                If($R_{id}$ = modified $SA_{2\_id}$ && time != $S_n$-time)
                        {
                        Check packet drop or capture
                        Node id set $SA_2$ categories
                        }
                }
Step6: SDP sense the activity of all neighbour
{
        If (next-hop receives && forward != true && modified id of $SA_1$== $R_{n\_id}$ && time == $S_n$-time)
{
        Block the $SA_1$ node
}
        If (next-hop receives && forward != true && modified id of $SA_1$== $R_{n\_id}$ && time != $S_n$-time)
{
        Block the $SA_2$ node
}
Re-search route from $S_n$ to $R_n$
Eliminate the $SA_1$ and $SA_2$
Fresh route established
Send data and go to step 5 of SDP
 }
```

4. NETWORK SIMULATOR

Proposed methodology is implemented in NS2 Network Simulator. This is an object oriented simulator, written in C++, with an OTCL interpreter as a front-end. The simulator supports a class hierarchy in C++ (also called the compiled hierarchy) and a similar class hierarchy within the OTCL interpreter (also called the interpreted hierarchy). The two hierarchies are closely related to each other; there is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compiled hierarchy. The root of this hierarchy is the class TCL Object. Users create new simulator objects through the interpreter; these objects are instantiated within the interpreter and are closely mirrored by a corresponding object in the compiled hierarchy. The interpreted class hierarchy is automatically established through methods defined in the class TCL Class. User instantiated objects are mirrored through methods defined in the class TCL Object.

4.1 Performance matrix

The performance of network is evaluated in case of AODV, Sybil attack and Security scheme.

4.1.1 Routing Load

The number of routing packets (RREQ, RREP, and RERR) transmitted per data packet delivered at the destination.

4.1.2 Packet delivery ratio

The ratio between the numbers of packets originated by the application layer to those delivered to the final destination.

4.1.3 Average end to end delay

This is the average of the time taken by the packets to reach the destination in the network. The average time to packets sends by sender and received by receiver in network.

4.1.4 Packet Loss

The calculation of number of data packets in network are drop by Sybil attacker.

4.2 Simulation Parameters

The simulation parameters like area of simulation is 800m *600m in transmission range of 550m. Rest of them that are consider for simulation is mentioned in table 1

Table 1: Simulation Parameters

Area of Simulation	800x600
Mobile Nodes	50
Radio Range (meters)	550
Transferring Mode	Unicast through Unipath
Maximum speed (ms)	40
Routing Protocol	AODV
Transport Layer	TCP, UDP
Traffic	CBR, TTP
Application Layer	FTP
Packet size	512 byte
Simulation Time (sec)	100

5. SIMULATION RESULTS

The simulation results on the basis of performance metrics are mentioned in this section.

5.1 Different time Modified ID by Sybil Attacker Scene-1

The Sybil attacker is generated the fake ID's in a different time instant. This graph analyze attacker node gives five different identification to sender for misleading of data, retrieving from the sender in two different scenarios, in first scenario it take Sybil attack in different time interval means attacker use different identification number in different time and receives the data from genuine sender and that data cannot receives by the genuine receiver. In that scenario it is found that node 26 uses five identifications 17, 23, 24, 29 and 8 and captures all the data packets in network.

5.2 Same time Modified ID by Sybil Attacker Scene -2

The second different condition of Sybil attacker in this scenario is it uses the different identification number in same time instant. It implies that the attacker is able to generate the same ID's at any time. In this scenario, more than two identifications shown at the same time and receives data packet from sender, that result detected through profile generation base scheme and after that protection scheme is applied for prevention from misleading activity. This graph analyze node number 17, 23, 24, 29 and 8 that gives different identification in same time and receives data from sender that is degrades the performance of network.

5.3 Packet Delivery Ratio Analysis

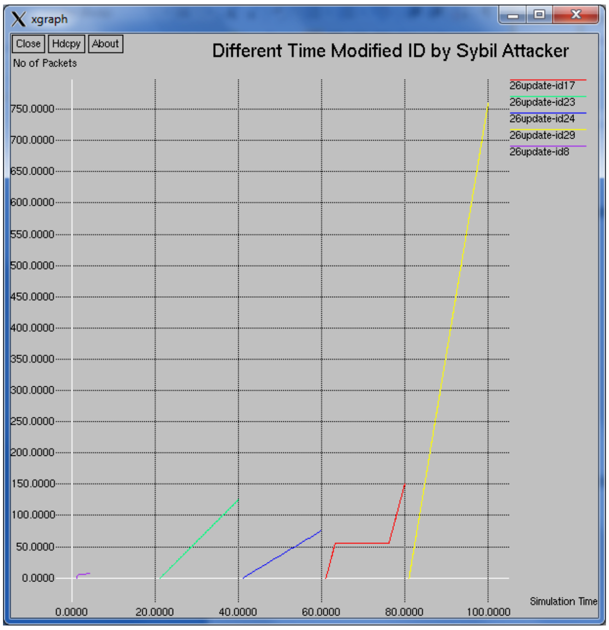
Packet delivery ratio is very important parameter for data analysis in network communication because that parameter gives the information about percentage of data receives by the receiver out of actual data packet sends by the sender, here it is analyzed that packet delivery value are evaluated in normal network as well as proposed protection system. The percentage of data receives is nearly 88 to 90 percent up to end of simulation in normal routing and proposed secure routing in presence of Sybil attacker but Sybil attack (scenario-1 and scanrio-2) has shows the performance degradation in the whole network. The PDR performance in presence of attacker is in scenario 1 is really up to negligible mark but reaches to 55 % at the end but affected from attacker the performance of scenario-2 is also same as one except the end time simulation performance.

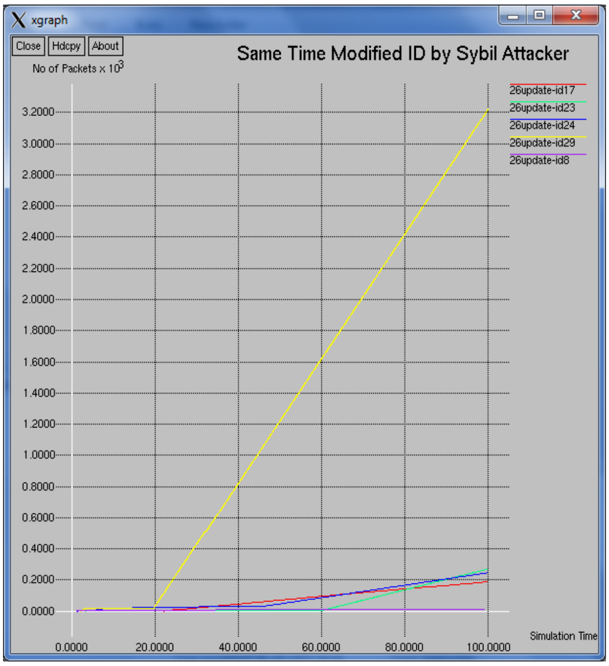
5.4 Throughput Analysis

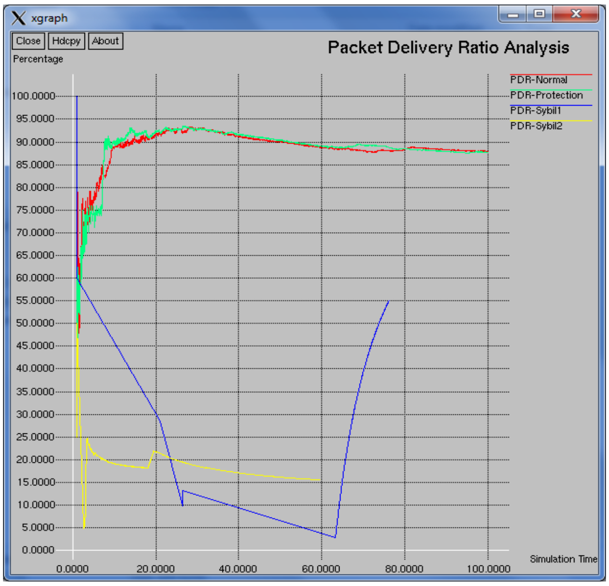
This graph represents the throughput analysis in case of normal routing, attack and SDP. The throughput has measure on number of data packets are received at destination in per second. The Sybil attacker degrades the throughput performance at sending end and also possible at receiving end. At the time of attack throughput decreases due to heavy data packets loss in network. The throughput performance degradation in term of per unit time in scenario-2 is up to 200 packets/second and in scenario-1 the performance is reaches to about 1 to 2 packets/second. But after applying proposed security scheme the throughput is more efficient than normal routing about 1400 packets /second maximum and 900 packets/second minimum.

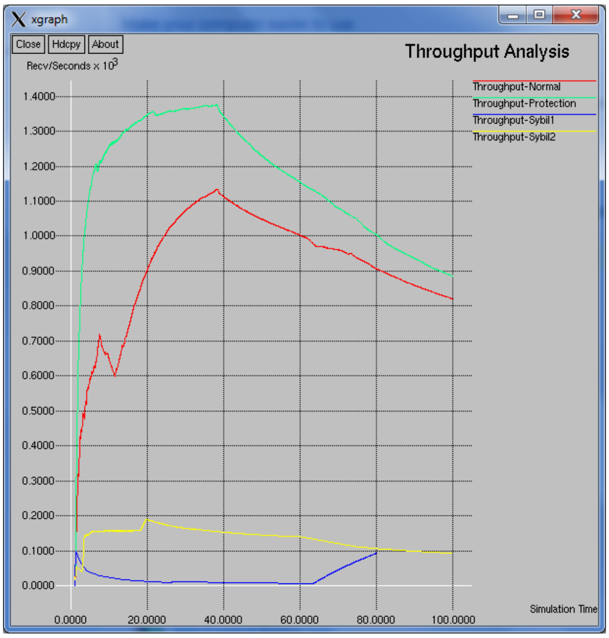
5.5 Routing Analysis

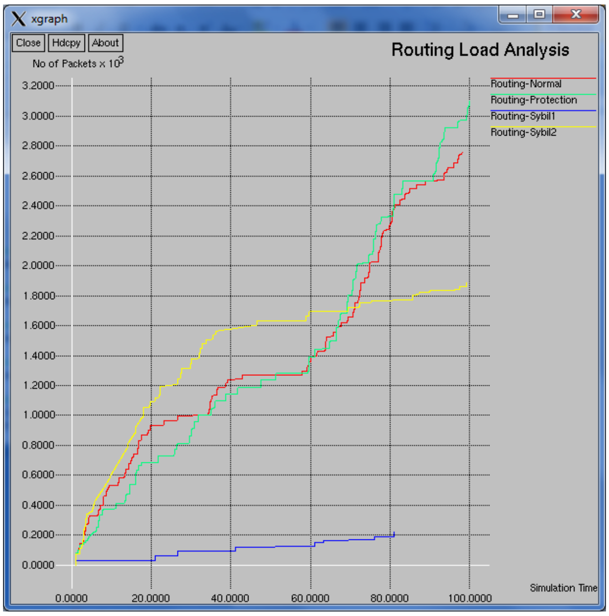
The sender is flooding the packets in network for finding the destination. Every node in network is forwarded the routing packets in network till the destination is not found. This graph analyze routing overhead in case of protection as well as normal time but in both Sybil attack scenario routing overhead is lower because if sender search actual receiver and same time any nearby Sybil attacker is present that certainly gives the misidentification number of receiver and route reply message send to sender by receiver. In that case actual sender cannot search any of the paths and actual data packets are dropped by attacker. The routing packets in normal routing and proposed security scheme are flooding more but data receiving is also high with minimum overhead.











6. CONCLUSION

MANETs consist of wireless equipments (called nodes hereafter) that can contact with each other without the help of a fixed infrastructure. Such as, it is well suited to create radio connectivity at any time and any place. Composite participants roam freely. This changes the network topology frequently and invalidates cached routing information. Such that the composite may fail due to loss network paths. To providing security in this network is the major concern. The attacker or malicious nodes are modifying the routing information and drop the whole packets in network. The proposed Sybil Detection and Prevention System (SDP) is provides the security from Sybil attack. The Sybil attacker replies the request of nodes from multiple Recognition (MR) of itself. The proposed security scheme is provides the secure routing and completely block the packet dropping in presence of attacker. The proposed approach is detecting the attacker by their malicious behavior and this malicious node/s is affecting the routing performance. The routing performance in presence of SDP is really enhance the routing and provides zero % attacker interaction in MANET. The proposed SDP is protected from the routing misbehavior of Sybil attacker. The throughput and routing load performance is well good as attacker presence and this variation in results shows the effect of SDP in MANET.

The other attacker are also affected the network performance in a different way. These attacker collaborative effects are very destructive for dynamic open network. Future work involve try to propose the security scheme for collaborative attack in MANET. The collaborative attack is the combined malicious effect of different and same attacks that aim to degrade the MANET performance and resource consumption.

7. REFERENCES

[1] S. Ci et al., “Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks,” IEEE Trans. Vehicle. Tech., vol. 55, no. 4, pp. 1302–1310, July 2006.

[2] C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR, 2004.

[3] K. Kuladinith, A. S. Timm-Giel, and C. Görg, “Mobile ad-hoc communications in AEC industry,” J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[4] M. Zapata and N. Asokan, “Securing Ad Hoc Routing Protocols,” in Proceeding of ACM Workshop on Wireless Security, pp. 1–10, 2002.

[5] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S. Ali, Prof. J.S. Deshpande, " A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-4071, 2010.

[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ,”Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 1-38, @ 2006 Springer.

[8] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: Analysis and defences,” presented at the 3rd Int. Symposium of Information Processing in Sensor Networks (IPSN), pp. 259–268., 2004

[9] G. Jayakumar and G. Gopinath, “Ad Hoc Mobile Wireless Networks Routing Protocol—A Review,” Journal of Computer. Science, Vol. 3, No. 8, pp. 574–582, 2007.

[10] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” Proc. ACM SIGCOMM, 1994.

[11] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On demand Distance Vector (AODV) Routing,” IETF RFC 3561, July 2003.

[12] D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad-Hoc Wireless Networks,” T. Imielinski and H. Korth, ed., Mobile Computing, Kluwer Academic Publishers, pp. 153–81, 1996.

[13] Z. J. Haas and M. R. Pearlman, “The Performance of Query Control Schemes for the Zone Routing Protocol,” IEEE/ACM Trans. Net., vol. 9, no. 4, pp. 427–38, 2001.

[14] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat ,“Lightweight Sybil Attack Detection in MANETs” IEEE Systems Journal, Vol. 7, No. 2, pp. 236 To 248, June 2013.

[15] Muhammad Nawaz Khan, Muhammad Ilyas Khatak, Muhammad Faisal “Intrusion Detection System for Ad hoc Mobile Networks” International Journal of Computer Applications (0975 – 8887) Volume 35– No.2, December 2011.

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

[17] S. Capkun, J. P. Hubaux, and L. Buttyan, “Mobility helps peer-to-peer security,” IEEE Transaction Mobile Computing., vol. 5, no. 1, pp. 43–51, Jan. 2006

[18] C. Piro, C. Shields, and B. N. Levine, “Detecting the Sybil attack in mobile ad hoc networks,” in Proceeding of Secure Communication Workshops, pp. 1–11, 2006.

[19] Network Simulator-ns-2 Tutorial Available on link, http://www.isi.edu/nsnam/ns/tutorial/index.html.