 ISSN: 2454-4248
486 – 495

Detection and Optimization of SYBIL Attack by using Received Signal Strength in mobile Ad-HOC Networks (MANET'S)

Dinesh Kumar

Assistant Professor

Computer Science & Engineering,
Shekhawati Institute of Engineering & Technology, Sikar, Rajasthan, India

Abstract :In this research paper, we address the Sybil attack in MANET. Most often the traditional measures against Sybil attack are not applicable in a MANET due to the differences in aims and architectures. The nodes in MANETs are mobile and limited in resources such as battery, bandwidth etc. Due to frequently changing topology it becomes expensive and impractical to authenticate communication and keep track of devices with a centralized server in such network. We proposed a framework which uses nodes attributes in order to judge their behavior. As Sybil nodes consumes data packet by providing wrong routing information repeatedly, we focus on the distinction of the node parameter value of Sybil node and legitimate node. This distinction is made on the basis of nodes attributes and by assigning fuzzy membership values to each node. For this we use fuzzy inference rule and Bezier curve as a tool. Here suspect any node means is to identify those nodes also whose behavior lie in between legitimate and Sybil nodes. In contrast to the traditional crisp logic in which a node can be either Sybil or legitimate fuzzy inference based model focus on the possibility of a node being Sybil. Later we verify their RSP values by drawing a Bezier curve at two different instant of time to identify the Sybil character.

Keywords **- MANET, CA, RSSI, SNS, POPA, APDV**

I. INTRODUCTION

Sybil attack spreads excessive hazard in routing, voting system, fair resource allocation, data aggregation and misbehavior detection system. In large-scale peer-to-peer systems there's an opportunity of security threats from faulty remote elements. Tobeat these threats, several such systems use redundancy. Peer-to-peer systems commonly rely on the existence of multiple, independent remote entities which can replicate computational or storage tasks (to preserve integrity of data) or distribute tasks among them (to protect against data leakage). This type of system must ensure that each entity has distinct identity. Otherwise, when a single faulty entity can present multiple identities, it can control a considerable portion of the network there by undermining this redundancy [1]. The security threat of the Sybil attack can destroy the voting authority of honest users in online settings [2], and also corrupt routing tables in peer-to-peer systems. In the Sybil attack, the adversary targets the victim system using its Sybil identities and continues attack in order to interrupt that system. For example, a rival can pollute the voting scheme of a reputation system [3], weaken the routing and data replication services in distributed hash tables (DHTs) [2], or cripple many critical functions of a wireless sensor network such as routing, resource allocation, and misbehavior detection [4]. The performance of a reputation system degrades if Sybil identities can be generated easily. If the reputation system accepts inputs from unreliable entities, then linking them to a trusted entity may cause threat for the system. Moreover, Sybil attacks prevent fair resource allocation among the nodes in network. This threat particularly affects decentralized systems, where it is almost impossible to rely on a single authority to certify genuine nodes [5]. However, J. R. Douceur [1] has shown that without a logically centralized authority, Sybil attacks are always possible (i.e. may remain undetected) except under extreme and unrealistic assumption of resource parity and coordination among entities. Since the Sybil attacker can create many fake identities, it thus can increase the probability that the malicious node is selected by other nodes as part of their routing paths. Besides, the Sybil attack can significantly reduce the effectiveness of fault-tolerance schemes such as multi-path routing [6, 7] because other nodes will treat the forged nodes generated by the spiteful node as different nodes and establish different routes through that malicious node. A Sybil attacker may also satire nodes in geographic routing protocol, such as the GRID routing protocol [8].

Many techniques contribute a lot in prevention, detection and recovery of Sybil attack, each of them has a certain limit to exhibit its efficiency. Exploring the loop holes of these techniques is an important research area as it motivates the future researchers to find a scope or research gap that will bring out new techniques which recover the existing limitations.

The proposed study focuses on the security aspects in Mobile Ad hoc Network (MANET), specifically against Sybil attack which is one of the most dangerous threats in MANET. To analyze the problem systematically the entire work incorporates a number of objectives which are to be integrated finally. The first and foremost objective of the current study is to propose a new technique to detect Sybil attack in MANET using trust based model. For this we need to design an attack model and show the impact of Sybil attack on the performance metrics. Then we have to propose the detection algorithm based on the attack model. Our second objective is to show how the proposed methods use simpler tools like fuzzy inference and Bezier curve in order to avoid complex calculation and hardware implementation used in other existing techniques. Third objective is to judge the correctness of the

algorithm. This is achieved by implementing the technique in network simulator NS2.35.The final objective is to analyze the strength and weakness of the proposed study in the context of efficiency, accuracy, performance, application domain etc.

II. LITERATURE SURVEY

Douceur [1] (in 2002) has proved that trusted certification is the only approach that has the maximum potential to eliminate Sybil attack completely. This approach may seem to be ideal for handling Sybil attack, but there are a numbers of issues related to implantation of certification authority as well as implementation of entity-identity mapping. Significant overhead and cost also restrict the use of this method.

W. Du (in 2003) [9] introduced Random Key Pre-distribution technique which is used in wireless sensor network to establish a secure routing for communicating with each other. A set of key are assigned randomly to a node enabling it to compute the common keys that it shares with its neighbour. Node to node privacy is ensured by using the common keys. The key ideas are the association of the identity with the key assigned to a node and the validation of the key. Validation ensures that the network is able to validate the key. There is a little probability that a forged Sybil identity will pass the key validation test as the keys associated with a random identity are not likely to have a significant intersection with the compromised key set.

Resource testing [10] is another one of the most widely used techniques to defend Sybil attack. The idea behind this approach is that the resources used by the entity in the network are limited. A verifier compares the amount of resources utilized by the entity with the typical value of the resources possessed by that entity. Any discrepancy indicates the possibility of Sybil attack. Generally, storage of energy, available memory size, computational capability, bandwidth, and channel capacity may be considered as resources.

Recurring cost method is a variation of resource testing where resource tests are conducted periodically to impose a certain “cost" on the attacker that is incurred for every identity that he controls or introduces into the network. B. Awerbuch (in 2004), P.Maniatis (in 2003 and 2005)[11] have certified this method and have used computational power in their resource tests. This itself may be inadequate in controlling the attack since a malicious user incurs only a one-time cost (for computing resources) that may be recovered via the execution of the attack itself, as pointed out by Levine et al (in 2006). The detection of an attack is deemed successful only if ratio of the attacker's objective value to the cost per identity exceeds the critical value (the value that exists for a particular combination of application domain and attacker objective). They conclude that using recurring costs or fees per identity is more effective as a deterrent to Sybil attacks than a one-time resource test. B. Awerbuch (in 2004) [12] proposed that only limitationwith this approach is that it requires electronic cash or significant human effort.

N. B. Margoline and others (in 2006) [13] stated that trusted certification is one of the most prospective solutions to prevent Sybil attack. It requires one certification authority (CA) that validates the one to one correspondence between an entity and its associated identity.

Demirbas and Song (in 2006) [14] proposed a method for Sybil detection based on the Received Signal Strength Indicator (RSSI) of messages. Upon receiving a message, the receiver will associate the RSSI of the message with the sender identity, and later when another message with same RSSI but from a different sender is received, the receiver can detect the Sybil attack. Sybil attacks can be detected with a completeness of 100%with few positive alerts. However, a Sybil node can transmit message with different identities using different transmission power intensity to defeat this scheme and transmission is also non-isotropic. It also cannot deal with existing Sybil nodes in the network, location calculations are also costly. It is applicable to sensor network only.

Margolin and Levine (in 2007) [15] proposed a protocol called Informant that is based on an economic incentive policy that is not specific to any particular application domain. An entity is taken as detective to reward Sybil for revealing themselves. An identity gives the name of the target peer and a security deposit to the detective while the target peer receives the deposit and a certain reward. A Dutch auction is used to establish the minimum reward that will reveal a Sybil node.

Fong (in 2011) [16] considered a different kind of Sybil attack that aims to create pseudonymous or fake identities in a Social Network System (SNS) and get them to collude to favorably alter the existing trust relationships in the network. These relationships are represented via a graph-theoretic relationship model that exists between the owner of a resource and a prospective user of the same resource and is called a social graph. Such models are common in some popular Social Network Systems such as Face book.

Cao (in 2012) [17] stated that when the fake accounts in the SNS collude, they may gain the ability to access personal, sensitive and restricted user information or perform large-scale crawls on the social graph. To counter this threat, Fong (in 2011) has proposed a particular version of Denning's Principle of Privilege Attenuation or POPA that is both a necessary and sufficient condition to thwart such attacks, along with a static policy analysis for verifying POPA compliance.

Position verification is another technique to mitigate Sybil attack and its implementation is confined to wireless ad hoc network. This is based on the fact that the same location in a network should not be occupied by two or more identities simultaneously. The method like triangulation [18] can be used for location verification. Sybil nodes can be identified by this approach because they will appear exactly at same position as the malicious node that generates them.

Tangpongetal.[19] (in 2009) have proposed a solution based on the above strategy. However, this technique yields false positive result (i.e. suspects a legitimate node as a Sybil node) in case of high mobility and high density of nodes.

 ISSN: 2454-4248
486 – 495

III. PROPOSED WORK & RESULTS

We implement and evaluate proposed detection algorithm. We have used Network Simulator NS-2.35 where we design a MANET consisting of 44 nodes among which 0 and 33 are made attacker (fig I). Node 0 compromises node 1 whereas node 33 compromises node 38. The attacker nodes change their transmission power between 1.8 watt and 2-watt time to time and take of the IDs of the compromised node. The compromised nodes provide wrong routing information to the source node for attracting data traffic towards them. When data packets reached these nodes they forward them to the attackers. The attackers in tum consume the data packet instead of forwarding them towards destination. This causes a disruption in the network and hence network performance degrades. The parameters listed in table 4.1 are the simulation parameter used for the attack model. The trace files and NAM files are generated according to the need.

Table I NS- 2.35 Simulation parameters used in attack model

Parameter	**Level**
Propagation Model	TwoRayGround
Transmission Power	1.8w
Frequency	2.472 * 109
Initial Energy	100 J
Collision Threshold	100 dB
Carrier Sense Threshold	5.011872×10-12w
Receive Power Threshold	5.82587×10-09w
Ideal Power	712×10-6w
RXPower	35.28×10-3w
TXPower	31.23×10-3w
SleepPower	144×10-9w
Number of Nodes	44
Protocol	AODV
MAC	802_11
Maximum Packet in ifq	50
Topology	Flat Grid
Area Covered	(500×500) sqm.
Node Movement (Sink)	at 50 towards position 25,20 at 100 towards position 490, 480
Node Movement (Source)	at 10.0 towards position 20, 18
Simulation Time	150s
Speed of the sink node	15m/s
Speed of the source node	1 m/s
Starting time of attacker	30.0s
Attacker vary id in each	20.0s

Node 1 sends wrong routing information to node 6 periodically by representing it as node 0 and increases its sequence number higher than the most recent value. Thus node 6 presumes that node 0 has the shortest route towards destination and it sends data packet to node 0. Node 0 consumes the data packets when it reaches to it. The same thing happens for node 33 and node 38. Here the attacker nodes periodically take off the identities of the Sybil nodes and consume data packet on their routes. Node 0 and node 33 vary their transmission power time to time in order to represent different IDs having different transmission power.

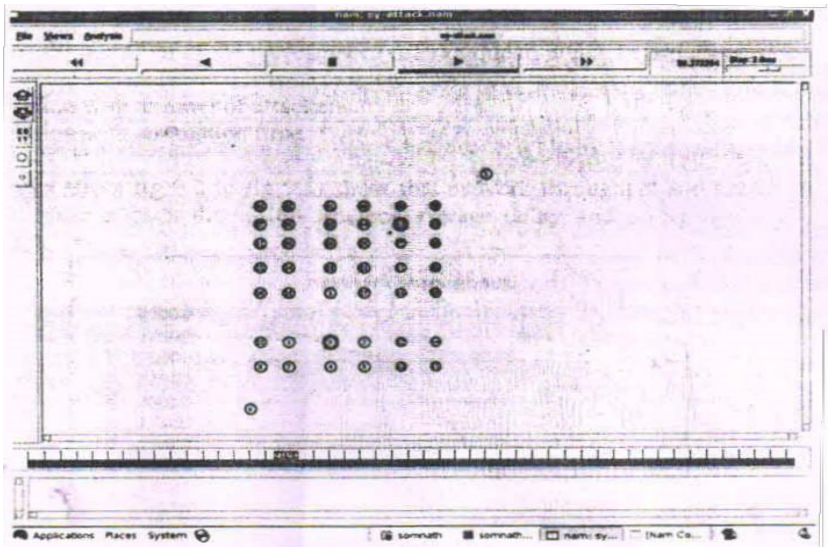

Fig I Simulation with 44 nodes

 ISSN: 2454-4248
486 – 495

Now we show the impact of Sybil attack on the above attack model. Here we assume that the Sybil node delivers wrong routing information to the source node in order to behave like a legitimate neighbour having shortest routing path towards destination. Since the detection technique is based on MANET we have chosen AODV routing protocol for communication. As we know that AODV is an efficient routing protocol for MANET, we have chosen some of its performance metrics and have shown the effect of Sybil attack on it. The performance metrics are defined briefly below:

Total throughput: The network throughput represents the ratio between the numbers of data packets generated from the source node, to the number of data packets received at the destination in percentage. The greater value of throughput implies a higher performance of the protocol.

Packet drop: Packet drop is the average number of packets dropped by the network during communication. A minimum packet drops results in higher performance of the protocol. In mobile ad hoc networks, wireless link transmission errors, mobility, and congestion are major causes for packet loss. A packet may be dropped at the source if a route to the destination is not available or the buffer that stores pending packets is full. It may also be dropped at an intermediate host if the link to the next hop has broken.

Average end-to-end delay: it is the average time taken by a data packet to arrive the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

Σ (arrive time - send time) /Σ Number of connections.

The lower value of end to end delay means the better performance of the protocol.

Packet lost: packet lost is the total number of packets dropped during the simulation.

Packet lost = (Number of packet sent - Number of packet received). The lower value of the packet loss means the better performance of the protocol.

We show the variation of the performance metrics due to attack in two dimensions:

Variation with number of attackers.

Variation with simulation time.

The results (from fig II to fig V) show that network throughput and packet delivery ratio decrease in each dimension whereas average delay and percentage packet drop increase.

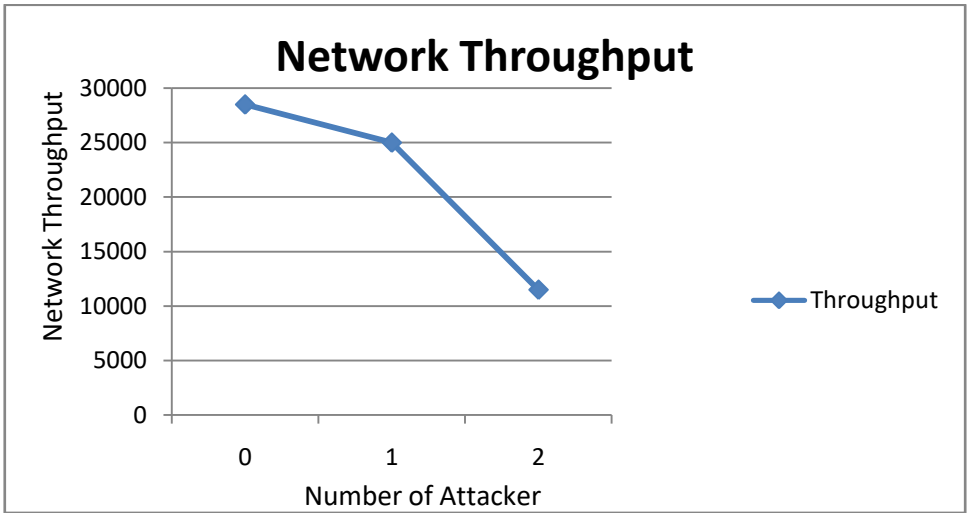

Fig II Variation of Network Throughput with Attackers

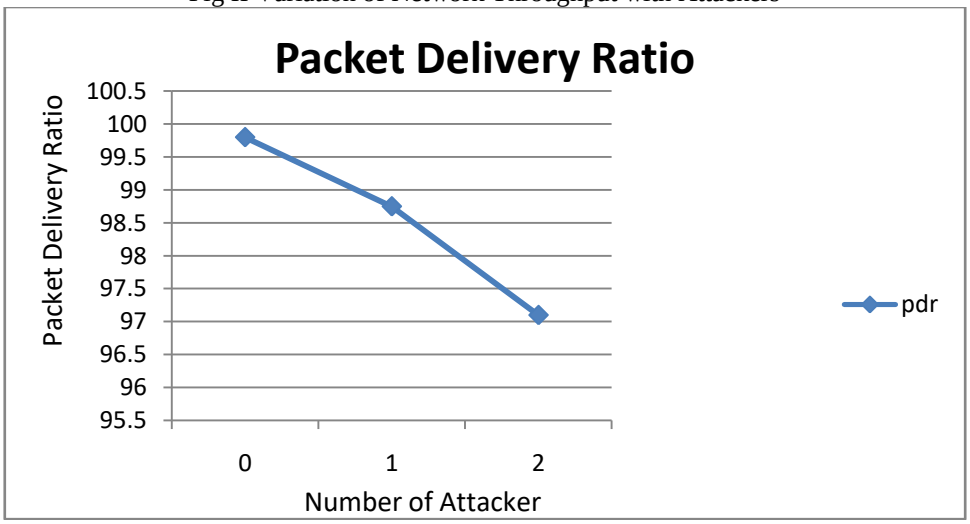

Fig III Variation of Packet Delivery Ratio with Attackers

 ISSN: 2454-4248
486 – 495

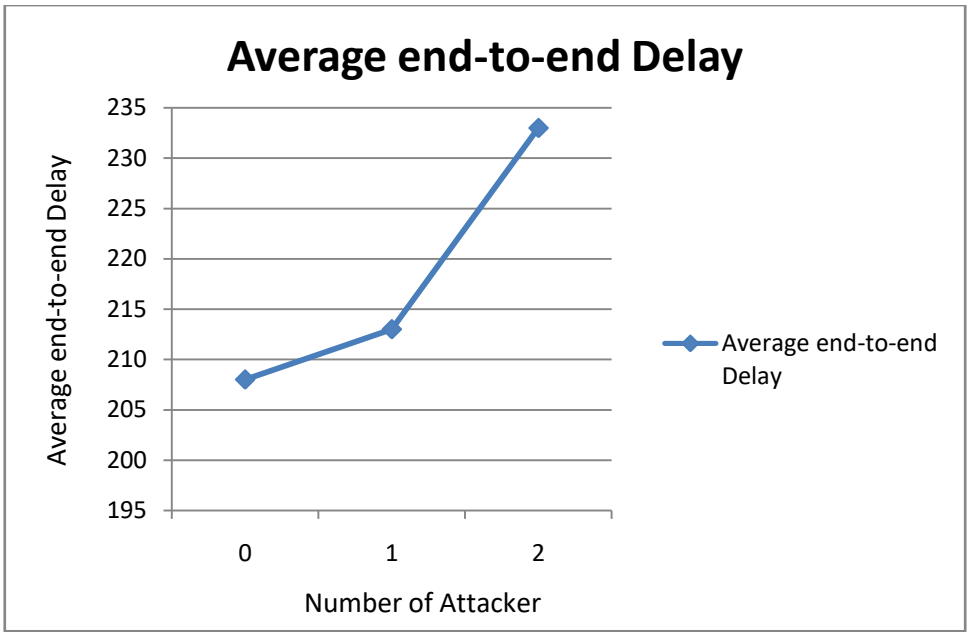

Fig IV Variation of Average Delay with Attackers

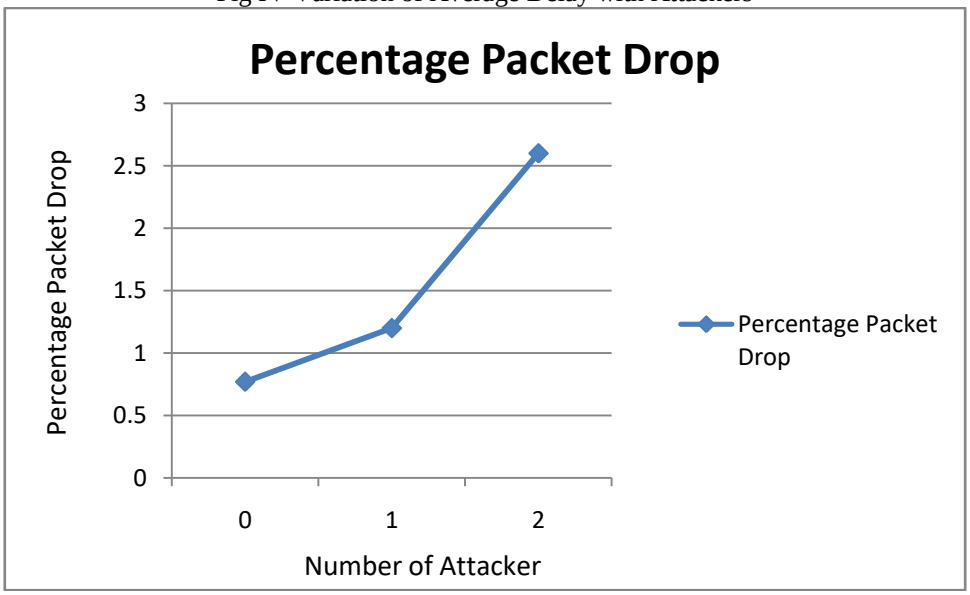

Fig V Variation of Packet Drop with Attackers

In the second dimension we consider the impact of Sybil attack on the network performance for various simulation times. The variation of each of the network parameters is shown graphically.

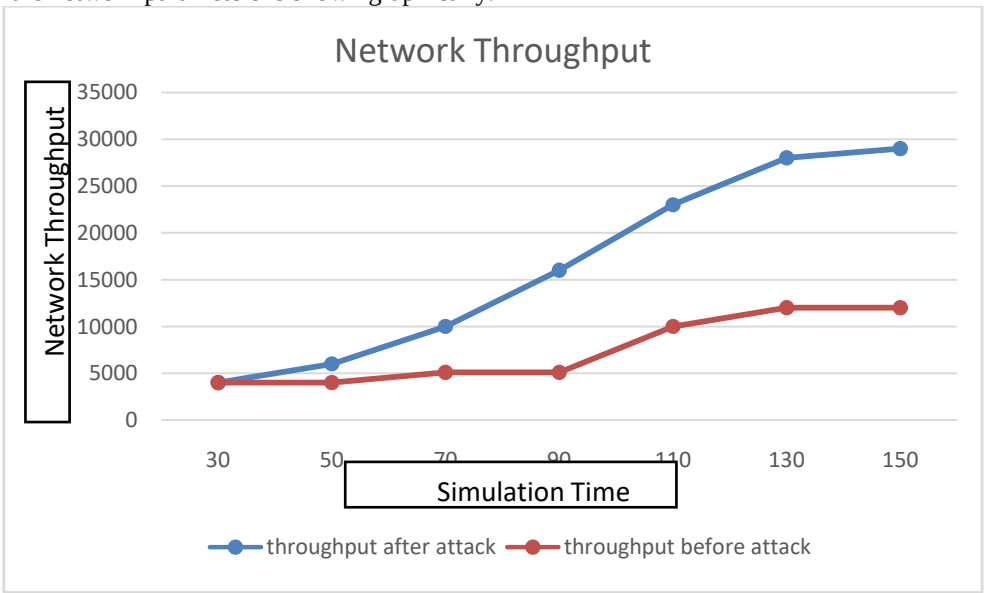

Fig VI Variation of Network Throughput with Simulation Time

 ISSN: 2454-4248
486 – 495

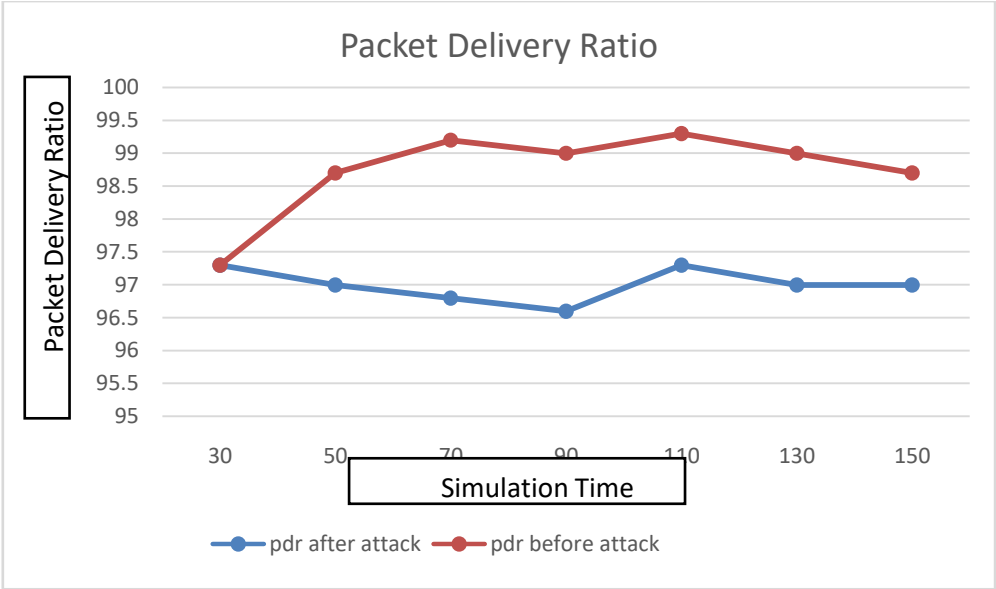

Fig VII Variation of PDR with Simulation Time

From fig VI and VII it is clear that network throughput and PDR decreases as simulation time increases. This is due to the fact that after a certain time interval the attack gets executed and the attacker remains alive up to simulation time 150s. This causes the degradation of network performance.

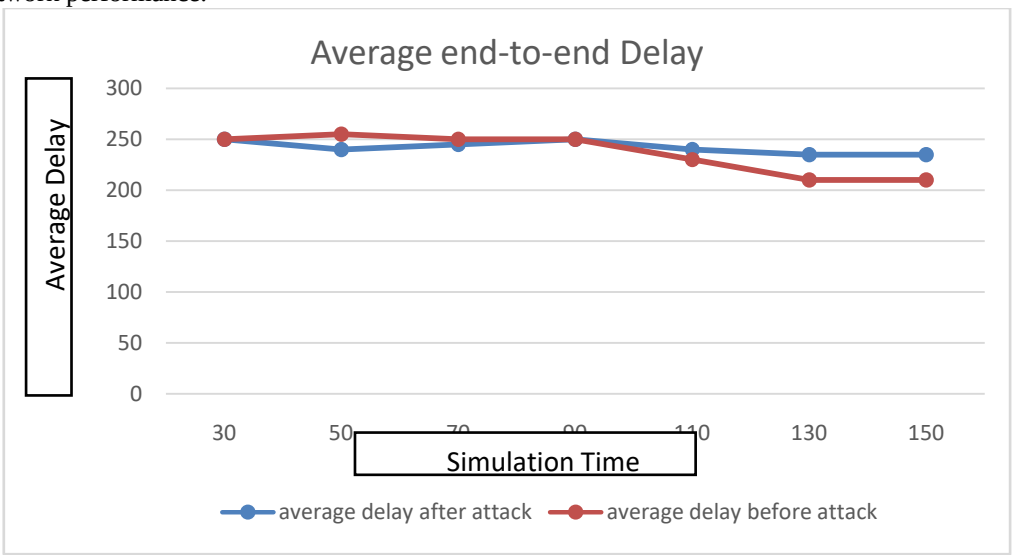

Fig VIII Variation of Average Delay with Simulation Time

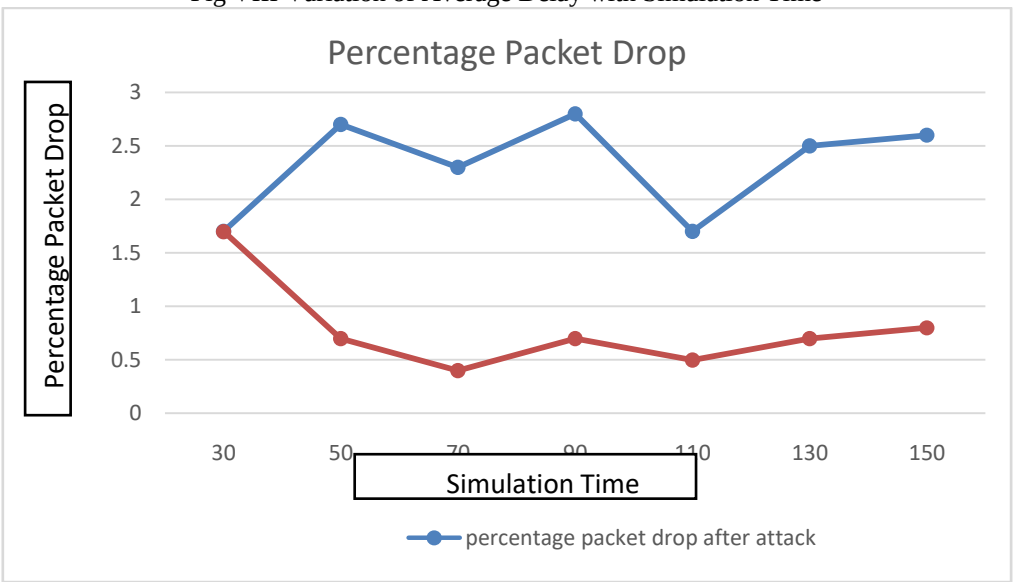

Fig IX Variation of Packet Drop with Simulation Time

The above figures (fig VIII and fig IX) show an increase of packet drop and average delay with simulation time which indicates that the attacker executes attacks for rest of the simulation time.

 ISSN: 2454-4248
486 – 495

In the next section we show the result of the proposed detection technique step wise according to the algorithm.

Simulation Result after step4 of the Algorithm

According to the step 4 of the proposed detection method we fetch the packet drop of 44 nodes (except source and destination) before and after attack and calculate the deviation as shown in table II

Table II Packet drop deviation after attack (no. of node 44 speed 0m/s)

Node	Packet drop before attack	Packet drop after attack	Deviation of packet drop
0	11	6	5
1	2	0	2
4	6	0	6
7	0	14	14
9	4	0	4
13	12	0	12
33	14	41	27

Now we use fuzzy membership values to derive the three categories of nodes as below:

Node- 0,1,4,9 legitimate
Node-13 suspected
Node-7, 33 highly suspected

In the step9 and step10 we consider suspected and highly suspected nodes for further verification.

Simulation result after step9 and step10 of the algorithm

In this section we will draw the Bezier curve by using the RSPs of each of nodes 13, 7 and 33 before and after attack. We calculate the distance between the tangent of the Bezier curve for each of the nodes 7,13and 33 and compare it with the threshold to finally trace out the Sybil nodes.

Table III Threshold comparisons (no. of node 44 speed 0m/s)

Node	RSP(watt) values at t1	RSP(watt) values at t2	Distance between the tangents (unit)	Above/below threshold?	Sybil node	Legitimate
7	ti=10.006805 -91.622661 -98.554133 -99.731964 -103.409211	ti=10.006805 -91.622661 -98.554133 -99.731964 -103.409211	0	Below		Yes
13	t1=103.147536 -91.904370 -98.835842 -105.767314 -107.998749	t2=10.009620 -91.348672 -98.280144 -105.211615 -107.443051	10.01	Below		Yes
33	t1=12.018746 -85.869020 -96.085532 -99.160379 -106.937425	t2=30.146384 -84.815415 -95.031927 -98.106774 -105.883820	21.72	Above	Yes	

Table III is used to draw Bezier curve for each of the nodes 7, 13, 33. Here we show the Bezier curve for node 33 in fig XI. While fig X shows the Bezier curve for node 13 which is considered for calculating threshold.

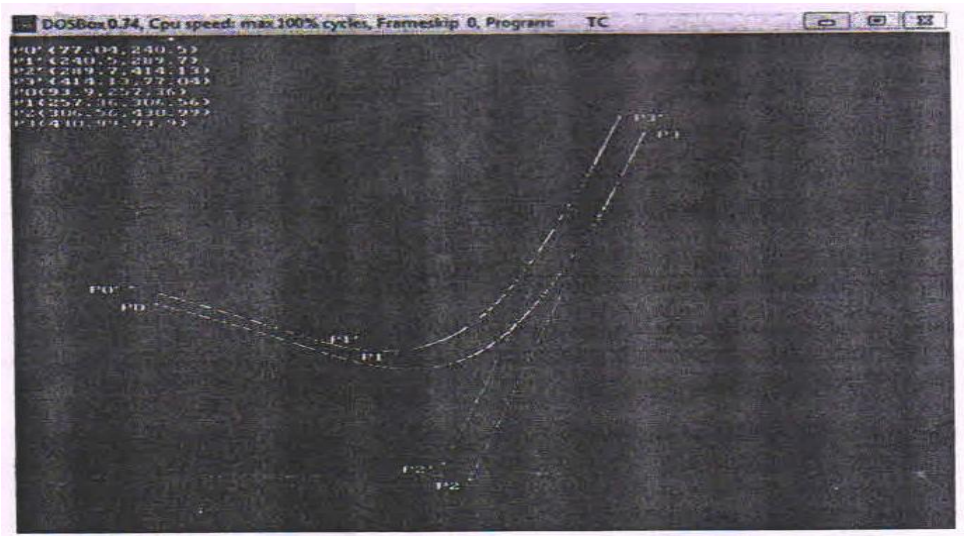

Fig X Bezier curve for legitimate node (threshold calculation)

 ISSN: 2454-4248
486 – 495

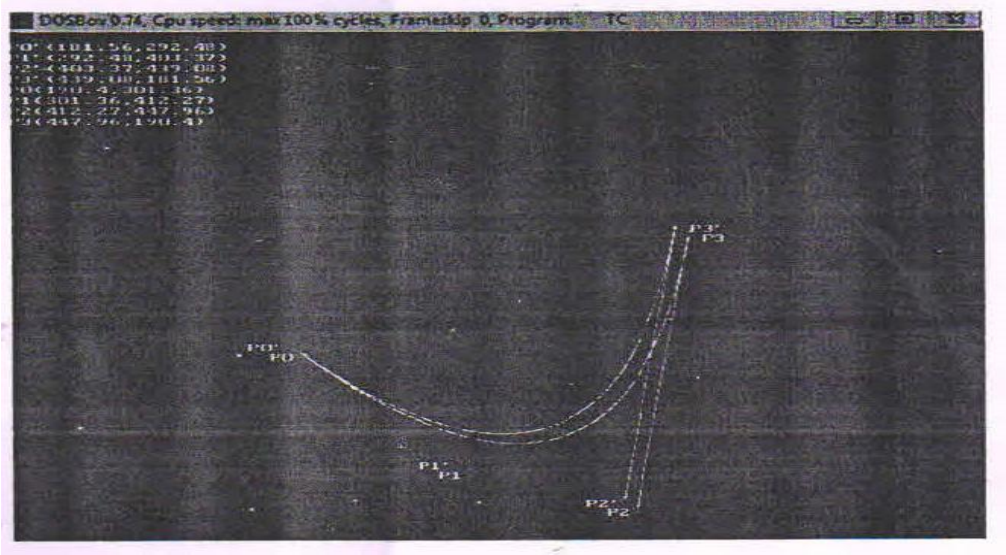

Fig XI Tangent Difference for Bezier curve of node 33

After retrieving the result of simulation for different speed of attackers at different density of the network we calculate the false positive, true positive and false negative percentages of the detection algorithm and graphically show their variations in fig XII, fig XIII and fig XIV.

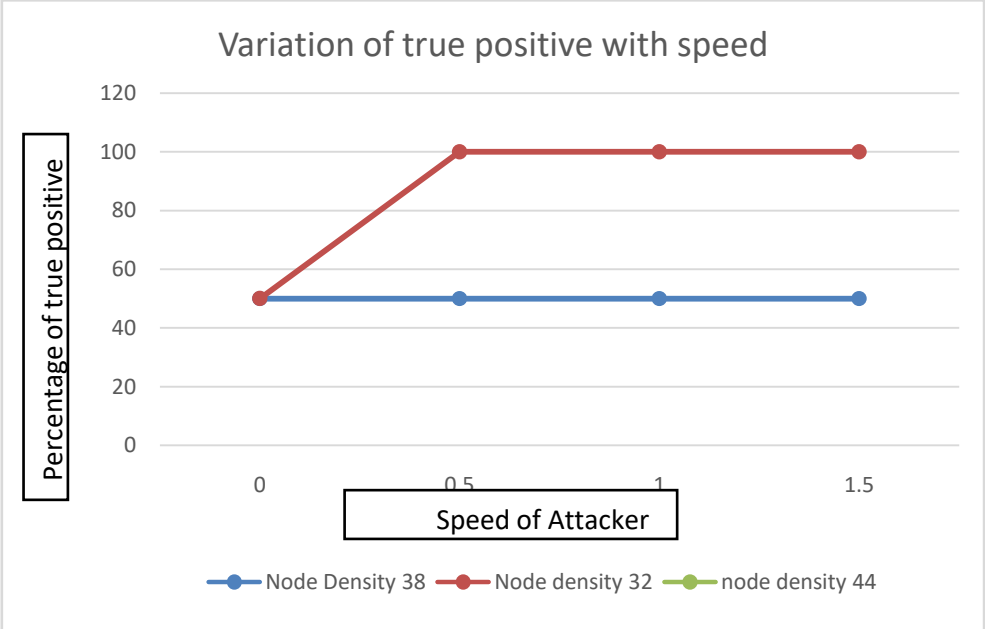

Fig XII Variation of True Positive with Speed of Attacker

From fig XII we see that percentage of true positive varies from 50% to 100% which indicates that there is a probability of the Sybil node being undetected. This is due to the fact that at the initial step the deviation of packet drop of the Sybil node does not belong to the suspected or highly suspected range and it is treated as a legitimate node.

 ISSN: 2454-4248
486 – 495

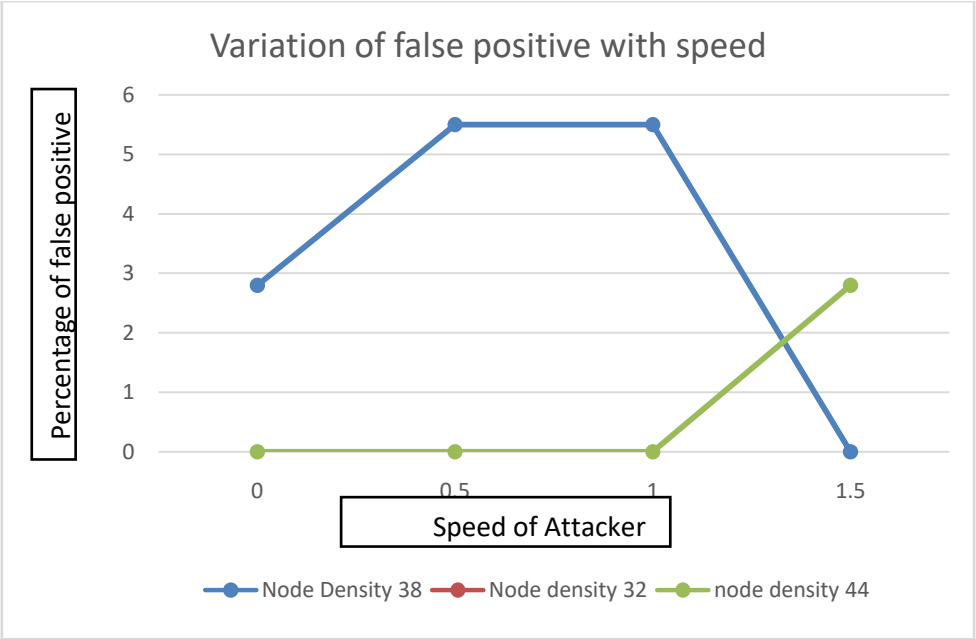

Fig XIII Variation of False Positive with Speed of Attacker

From fig XIII we get 2.5 % false positive at speed 1.5. This is because at speed 1.5 the distance between two Bezier curves for node 9 goes above the threshold value and it is treated as a Sybil node. This is quite obvious as because a legitimate node may also vary its transmission range close to the range of Sybil node. However, this behaviour depends upon several factors such as node's position, network connectivity etc.

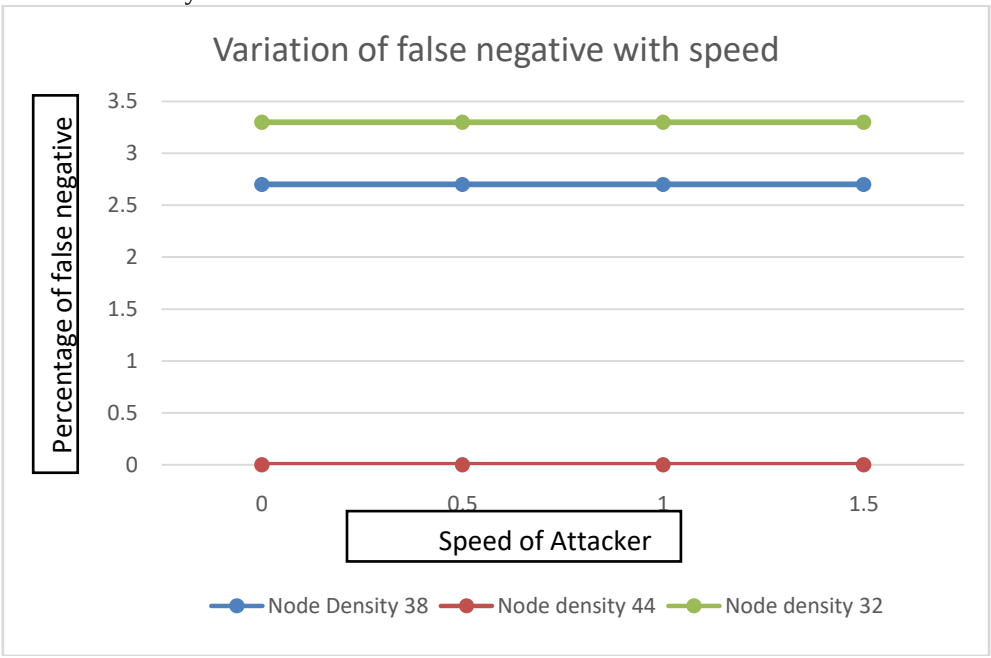

Fig XIV Variation of False Negative with Speed of Attacker

Speed has a little impact on the false negative percentage. From fig XIV we see that false negative remains same in node densities 38 and 32 while a small variation is observed in node density 44. However, there is a considerable increase in false negative in lower node densities. This is because in lower density the connectivity becomes weaker which creates hurdles in gathering sufficient information to execute the detection algorithm. Sybil nodes remain undetected due to lack of communication with other nodes.

REFERENCES

[1] J. R. Douceur, The Sybil attack. In IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pages 251-260, London, UK, 2002.
[2] G. Urdaneta, G. Pierre, and M. van Steen, A survey of DHT security techniques, ACM Computing Surveys, 43(2), Jan. 2011, http://www.globule.org/publi/SDST_acmcs2009.html.
[3] A.Josang and J.Golbeck, "Challaneges for robust of trust and reputation systems", Sept. 2009.
[4] Marco Carbone, Mogens Nielsen, and VladimiroSassone, A formal model for trust in dynamic networks, BRICS Report RS-03-4, 2003
[5] N. Margolin and B.N.Levine, Quantifying and discouraging Sybil attacks, Technical report, UMass Amherst, 2005.

[6] J. Chen, P. Druschel, and D. Subramanian, An efficient multipath forwarding method, proc. IEEE INFOCOM, pp. 1418-1425, 1998.
[7] K. Ishida, Y. Kakuda, and T. Kikuno, a routing protocol for finding two node- disjoint paths in computer networks, Proc. IEEE Int'1 Conf. Network Protocols, pp. 340-347, 1995.
[8] W.H. Liao, Y.C. Tseng, and J.P. Sheu, GRID: A fully location-aware routing protocol for mobile ad hoc networks, Telecomm. Systems, vol. 18, no. 1, pp. 37-60, 2001.
[9] Tangpong A., Kesidis G., Hung-yuan Hsu, Hurson A., Robust Sybil detection for MANETs, in Proceedings of 18th International conference on computer communications and networks, 2009, pp. 1-6.
[10] AthichartTangpong, Managing Sybil Identities in distributed systems, PhD thesis at the Pennsylvania state university, May 2010.
[11] Demirbus M., sang Y. (2000), An RSSI-based scheme for Sybil attack detection in wireless sensor networks, department of computer science and engineering, department state university of new york at Buffalo, NY 14260.
[12] Margolin, N. Boris, and Levine, Brian Neil, Informant: Detecting Sybils using incentives, in Proceedings of Financial Cryptography (FC) (February 2007) pp. 192-207.
[13] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil attack in sensor networks: analysis defenses, in information Processing in Sensor Networks, 2004. IPSN 2004. Third international symposium on, pp. 259-268, april 2004.
[14] B. N. Levine, C. Shields, and N. B. Margolin, A survey of solutions to the Sybil attack, University of Massachusetts Amherst, Amherst, MA, 2006.
[15] P. W. L. Fong, Preventing Sybil attacks by privilege attenuation: A design principle for social network systems, in IEEE symposium on security & privacy, 2011 pp. 263-278.
[16] Cao Q. Srivianos M., Yang X., and Pregueiro, aiding the detection of fake accounts in large scale social online services, in Proc. of NSDI (2012).
[17] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, in ACM CCS 2003, pages 42-51, Oct. 2003.
[18] P. Maniatis, D. S. H. Rosenthal, M. Roussopoulos, M. Baker, T. Giuli, and Y. Muliadi, preserving peer replicas by rate limited sampled voting, in proceedings of ACM SOSP, pages 44-59, 2003.
[19] B. Awerbuch and C. Scheideler. Group spreading: A protocol for provably secure distributed name service. In Proc. Automata, Languages and Programming (ICALP), pages 183-195, 2004.