International Journal of Advanced Research Foundation
Website: www.ijarf.com (ISSN: 2394-3394, Volume 4, Issue 3, March 2017)

Analysis on Intrusion & Detection of Sybil Attacks in Mobile Adhoc Networks Using Classification

D. Badru
Assistant Professor, Dept. of CSE
Swami Vivekananda Institute
of Engg & Tech
Hyderabad, Telangana, India

P. Deepthi
Assistant Professor, Dept. of CSE
Swami Vivekananda Institute
of Engg & Tech
Hyderabad, Telangana, India

B.Sankaraiah
Assistant Professor, Dept. of CSE
Swami Vivekananda Institute
of Engg & Tech
Hyderabad, Telangana, India

***Abstract* – Intrusion & Attacks detection in mobile Adhoc network has been challenging issue in the network scalability resource of proposed methods. This work shows detection algorithms suffer from the above constraints and could not exhibit proper efficiency and performance, the Sybil method which utilizes network scalability and its efficiency within the available resource. Classification method inference rule is used to initially isolate the nodes whose behaviours do not come with the genuine nodes later stage we employ a trained machine learning to out sybil node from the suspected nodes. The use of classification rule helps to avoid complex mathematical computation as this rule uses simple if then clause based on nodes attributes which can be easily extracted from a real network. the benefit of this technique that can find out any number of sybil nodes at one and also minimize the chance of false positive scheme by using simulation and result shows satisfaction rate with few false positive.**

***Keywords* – MANETs, Routing, Sybil Attack, Machine learning, classification.**

1. INTRODUCTION

Mobile Adhoc networks arewireless communication nodes that dynamically self-organize in topology which consists of large number of mobile nodes. Adhoc mobile can join and interconnected through wireless interface makes it highly susceptible to various link attacks, secure networking is protocols which ensure the confidentiality availability authentic integrity of networks. As the transmission takes place in open vulnerable to security attacks. The mobile hosts dynamically establish paths among one another in order to communicate success of MANET communication highly relies on the collaboration of mobile nodes. Mobile adhoc networks are infrastructure incorporates characterises such as frequently changing topology bandwidth and battery power etc. cryptographic authentication can mitigate types of attacks affect the routing protocol by dropping data packets or tunnelling them to other locations malicious nodes create illegitimate identities either by stealing or fabricating new ones which do not have real existence. The attacks rigorously disrupt the network performance by manipulating the routing table corrupting packets.The malicious node is range of the legitimate node and enters into where in internal attacks the malicious node creates many Sybil identities either by compromising the existing true nodes or by generating arbitrarily new identities prevents by authentication mechanism but it cannot mitigate internal attacks.Sybil attack can communicate directly with the legitimate node or a third party between two legitimate nodesboth stolen or fabricated identity and use them simultaneously attack the new identity is replaced by the previous one only one identity is active at same time. Other type of Sybil attack simultaneously uses all its identities for an attack causes interruption in the network may be dimension Sybil attacker enters into a system by using these fake identities and builds up basis for severe attacks in order to disrupt the targeted system. Sybil node exploits the routing protocol and consumes intercepted packets to replay other attacks wormhole and black hole attack impact on the wireless adhoc networks its detection becomes inevitable authentication because of its infrastructure computational and management overhead.

Sybil detection technique is easy to derive and not require high setup cost detection technique as Fuzzy Neural Networks is based on the concept of fuzzy inference rule and Artificial neural network, keeping in mind the inherent constraints associated with it fuzzy inference rule to initially differentiate between the suspected nodes and the legitimate nodes in the network. The packet drop of individual node and calculate the deviation from the normal values during attack are graded using fuzzy logic and the mamdani inference rule is applied to categorize trust distruct and enemy nodes, next stage we use trained artificial neural network that finally sorts out the Sybil nodes from the distrust and enemy nodes and detection result shows rates upto 90% with maximum of 10% false positive. The graphically approach not only traces the Sybil nodes with higher accuracy but also minimize the chances of false positive. Detection scheme neither uses any localization method that requires any extra hardware nor use any central authority which incorporates high costing and maintaince in scalable network that performs well in large scale network artificial neural network is useful tool where large amount of data are available to be difficult to train the artificial neural network with a large volume of data set with

International Journal of Advanced Research Foundation
Website: www.ijarf.com (ISSN: 2394-3394, Volume 4, Issue 3, March 2017)

high accuracy.Sybil attack model for adhoc network to show the impact of Sybil attack on the network which chooses AODV routing protocol and consider its performance metrics network throughput packet delivery ratio average delay and percentage packet loss. We also study the variation of network performance when the number of malicious nodes and Sybil nodes increase, fuzzy neural network which works in two stages a fuzzy inference rule and tested the efficiency of fuzzy neural network by applying on the attack model in NS2.35 and have shown result graphically.

2. RELATED WORK

The method to get rid of Sybil attack is deployment of trusted certificate has some drawback which is lack of scalable expensive initial setup and single point of failure assumption that every entity has one single identity on wide area network. Several task are spread to all node of the network for testing the resource of every node to verify if the node to complete the task. Trusted devices mapping of network entities hardware devices is one to one single hardware device like network card is vault to single network entity no path to stop entity from getting assigned to several hardware devices. The control system and behaviour based access BARTER in which nodes swap their profiles and then normal behavior of each nod is estimated proposed by observing the dynamics of node which were exchanged by nodes can detect Sybil identities, many designs trust are proposed in social network by using different modification random walk based Sybil defences and states that can perform confronted with some real world attacks that exhibit primitive structure. The two main trends of Sybil defense in social network based on random walk method while the second consider community detection how the two approach can go hand to yield robust Sybil defense protocol that are competitive with the state of the art. Fuzzy multi-agent security system for wireless sensor network which can differentiate agents that can be trusted frim the basis of fuzzy multi agent security system for wireless sensor network which can differentiate agents that can be trusted from those that cannot be trusted on the basis of fuzzy negotiations among agents present in the network, Sybil detection anticipated in reputation based system that uses a non-monetary entry fee per identity to discourage Sybil attackers without using any costly method this perform better than confident protocol in diving evil throughout and evil nodes utility in the presence of whitewashing node. Review of intrusion detection protection mechanisms show that intruders often find new way of attack and cause damage to computer system and network to the protection mechanism learn from experience and use the existing knowledge of attacks to infer and detect new intrusive activities, attacker may try to attack an existing protection mechanism to robust.

Every identity is participating charged a fee for instance recurring fee for every participating can be used as proposed by Margolin et al for prevention from sybil attackers and recurring fee prevents from one time charge. That recurring fee can recognize price to sybil attacker that linearly increase with the whole amount of identities that are participating, on the hand fee that is one-time incurs at stable cost only based on monetary mechanism of payment but CAPTCHAs that is non-monetary mechanism of payment cooperation in network messaging service. Received signal verification seems more capable among all causes of being lightweight solutions and without using GPS conversely sometimes require extra hardware like directional antennae or extra overhead incurred due to periodic localization of nodes.

3. MANET ATTACKS

Adhoc network vulnerable due to fundamental characteristic as open distributed node autonomy of nodes participation in network lack of centralized authority which can enforce security on the distributed co-ordination. Routing protocols devised for use in MANET have their individual characteristic rules. Most widely used routing protocol is Adhoc on Demand distance vector routing protocol relies on individual node cooperation in establishing valid routing protocol devised for multi hop networks each of them is based on trust node participating in network.

3.1. Cache Poisoning Attack: Each node keeps few of most recent transmission routes timeout occurs for each entry so each route lingers for some time in node memory that if malicious node performs routing attack then they will stay in node route table until timeout occurs or better route is found. Attacker node can be advertise a zero metric to all of its destination such route will not be overwritten unless timeout occurs, advertise itself as a route to a distant node which is out of its reach, effect of cache poisoning can be limited by either adding boundary leashes or token authentication maintain its friend list based on historical statistics of nodes performance.

3.2. Blackmailing cooperative attack: In a blackmailing attack cooperative attacker nodes accuse an innocent node as harmful node effectively is done on those distributed protocols that establish a good and bad node list based on review of participating node in MANET, protocol tries to make them more secure by using majority voting principle but still if sufficient no attacker node become part of MANET it can bypass the security as well.

Dynamic trust based distributed as MANET routing is cooperative process while building a route each node must evaluate its neighbour node, the method builds a distributed trust relationship and maintain dynamic trust information as the trust part of long chain single malicious node victimize an innocent node easily. Another solution will be building a friend list of trusted nodes identity must be determined by the user who created the MANET so it become a closed system of trusted node.

3.3. Sybil Attack: Sybil attack manifests by faking multiple identities by pretending to be consisting of multiple nodes in

International Journal of Advanced Research Foundation
Website: www.ijarf.com (ISSN: 2394-3394, Volume 4, Issue 3, March 2017)

the network so the single node can assume the role of multiple nodes and monitor hamper node at a time. If sybil attack is performed over a blackmailing attack then level of disruption can be quite how the identities are generated in the system.

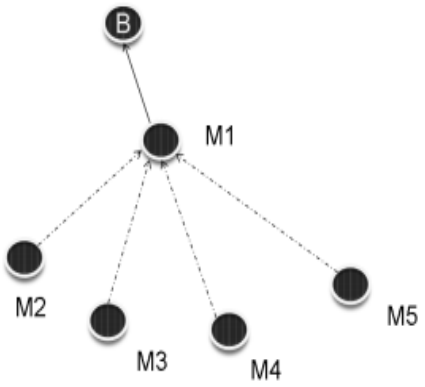

Figure1 Sybil type Attack

The figure show the node M1 assumes identities of M2,M3,M4 and M5 so node B M1 is equivalent to those nodes, one way of mitigating the attack is maintaining a chain of trust so single identity is generated by a hierarchical structure which may be hard to fake.

4. PROBLEM DEFINITION

Vulnerability is weak security system may be vulnerable to unauthorized data manipulate because the system does not verify a user's identity before allowing data access more vulnerable than wired network. Sybil is attack in mobile specially chosen network that has direct path to reach target node, Sybil occurs on node which act as a false node that selects the entire packet from source and drops the packet. The basis node S wants to reach to D it sends request to the national node if it has appropriate route to reach destination then it sends the packet throughout the path. If the clasp path then it ahead the request to the neighbour node until attain destination. The F is enlargement as a forged node that send request with maximum sequence number before any other node react even if the middle node send request to the source, second basic node S discards the reply and it assumes that the F node has direct path to reach destination and it sends the packet from that end path so the node F collects the packets coming from founded node which creates Sybil problem.

Sybil is an intrusion in the Manets lack of central monitoring device as Sybil attacks, which handles both attacks individually by dividing proposed mechanism in hash function for detecting simultaneous and request threshold validation mechanism for join and leave Sybil attack. This our proposed machine learning algorithms 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 the identity in the network. Each individual node on classification identifies to start with communication node send hello message that include its calculated condition of classification. The receiving node receives hello message from neighbour and friends in it. If the message contains label it store one place other case if hello message is with label the message id declined and node is rejected.

Proposed Algorithm

Step1 – Create a MANET consisting of a group of mobile nodes with one source and one destination.

Send the process to flow the packet from one source to destination using classification algorithm.

Calculate the packet drop deviation after attack.

Select node having packet which drop deviation and assign trust values to the selected nodes using classification rule.

Categorize the nodes as trust distruct and enemy using classification label

Identify the classification with five attribute values of the nodes as inputs before attack.

Apply the input pattern of distrust and enemy nodes to the trained neural network and calculate output and then the node with higher probability values are detected as Sybil.

Stop.

5. EVALUATION ANALYSIS

The proposed classification identify network simulator when there is no attack after simulation we fetch the values of the performance metrics for 44nodes from the trace file. The next run we consider the attack where node 0 and node 33 are made Sybil attackers then attack starts from 30^{th} changes identities periodically after each 20s we again fetch the values of same performance metrics.

Compare the value of packet drop of each node except source and sink from that packet drop plays and important role in Sybil attack because the compromised nodes take place in routing and forward data packet to the attackers who consume these packets. The abrupt packet drop in the network we calculate packet drop deviation of each node from table 4 and 5 and observes that node 0 13 32 and 33 have deviation from normal values while rest of the nodes remain unchanged. With respect to maximum deviation which 10 node 32 has a low deviation 0.2 whereas node 33 deviations 0.6 which comes under medium deviation node 0 and node 13 has the deviation range above 0.75 which fall into the category of enemy node using fuzzy inference rule three nodes out of 44 nodes with trust level.

International Journal of Advanced Research Foundation
Website: www.ijarf.com (ISSN: 2394-3394, Volume 4, Issue 3, March 2017)

Node	Packet drop before attack	Packet drop after attack	Deviation of packet drop
0	11	3	8
13	10	0	10
32	2	0	2
33	12	18	6

This work describes the simulation in order to analyse the detection efficiency of scheme under different scenario, the attributes of the network that may affect the accuracy of the proposed Sybil detection scheme such as node density and speed of attacker node. The impact of these parameters through simulation result shows that proposed algorithm successfully detects Sybil nodes with almost 100% accuracy but speed of the attacker and the node density may change the rate. To determine the metrics which identifies false positive and true positive rate defined as a legitimate node incorrectly detected as sybil attacker and true positive implies a malicious node detects the variation of these metrics in presence of the said network constraint. The speed has considerable impact on false positive at higher node densities for three different node densities sybil attacker moves with a certain speed its distance from the compromised node changes when the attacker node goes beyond the communication range of compromised nodes or other legitimate node the value of packet drops at the node change. The high node density produces high true positive fact that at high density number of connections increase the nodes frequency to send to receive packets at higher density the communication between node increase which also increase the chance to detect sybil node. At lower density connections become poor which make sybil node unable to execute the action from the evident that proposed scheme is better at high node density of MANET.

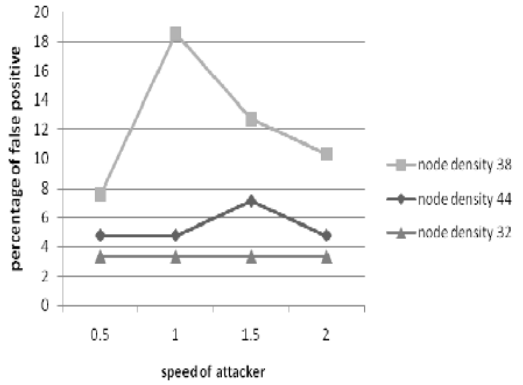

Figure 1. Positive Speed of Attacker

In the figure positive percentage speed of attacker high node density produces high true positive due to the fact at high density number of connections increase the nodes frequency to send or receive packets. Higher density communication between nodes increase which also increase the chance to detect Sybil nodes at lower density connections becomes sybil nodes unable to execute the action, the chance to detect the analysis is evident proposed scheme work better at high node density of MANET.

6. CONCLUSION

The method Sybil attack in which Sybil node identifies multiple time to time is proposed for MANET where mobility is an important, various speed of nodes to test the efficiency of the algorithm considered the performance of the alogirthm under different scalability of the network. The classification over head of the second stage of the algorithm where we have to test the less number of nodes with machine learning technique and incorporates the nodes mobility which is a crucial parameter in MANET.

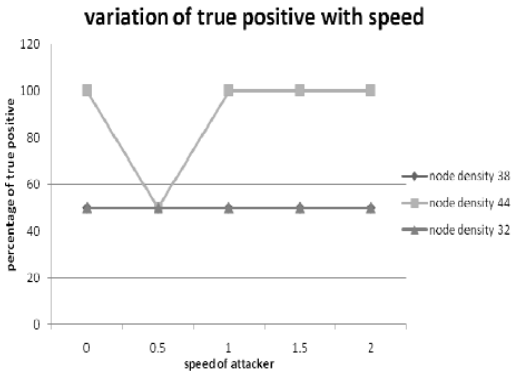

Figure2. Positive percentage Speed of Attacker

REFERENCES

[1]. Hoang Lan Nguyen: A Study of Security Attacks on Multicast in Mobile Ad Hoc Networks www.cse.yorku.ca/~lan/defense.pdf
[2]. Ruiliang Chen, Michael Snow, JungMin Park, M. Tamer Refaei, and Mohamed Eltoweissy: Defence against Routing Disruption Attacks in MobileAdHocAttacks http://www.arias.ece.vt.edu/publications/ conferenc es/TUF_Globecom_CR.pdf
[3]. Cai, Jiwen, et al. "An adaptive approach to detecting black and gray hole attacks in ad hoc network." Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. IEEE, 2010.
[4]. Alem, YibeltalFantahun, and Zhao Cheng Xuan. "Preventing SYBIL attack in mobile ad-hoc networks using Anomaly Detection." Future Computer and Communication (ICFCC), 2010 2nd International Conference on. Vol. 3.IEEE, 2010.
[5]. Bhosle, Amol A., Tushar P. Thosar, and SnehalMehatre. "Black-hole and wormhole attack in routing protocol AODV in MANET." International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol 2 (2012).
[6]. Trifaa Z., Khemakhemb M., "Sybil Nodesas a Mitigation Strategy against SybilAttack", International Workshop on SecurePeer-to- Peer Intelligent Networks &Systems (SPINS-2014), ProcediaComputer Science 32 (2014)pp 1135 –1140, June 2014.
[7]. Haribabu K., Arora D., Kothari B., HotaC., "Detecting Sybils in Peer-to-Peer
[8]. Overlays using Neural Networks andCAPTCHAs", in proceedings ofInternational Conference on ComputationalIntelligence and CommunicationNetworks, 2010.

International Journal of Advanced Research Foundation
Website: www.ijarf.com (ISSN: 2394-3394, Volume 4, Issue 3, March 2017)

About the authors:

D.Badru pursuing research scholar in Mobile Adhoc Networks B.Tech Computer Science & Engineering M.Tech Computer Science & Engineering. He is working as Asst Prof at Swami Vivekanand Institute of Engg & Tech guided many UG & PG students. His research areas include MANETs, Routing Protocols, Data mining, and Artificial Intelligence.

P.Deepthi B.Tech Computer Science & Engineering M.Tech Computer Science & Engineering. She is working as Asst Prof at Swami Vivekananda Institute of Engg & Tech guided many UG & PG students. Her research areas include MANETs, Routing Protocols, Data mining, and Artificial Intelligence.

B.Sankaraiah B.Tech Computer Science & Engineering M.Tech Computer Science & Engineering. He is working as Asst Prof at Swami Vivekananda Institute of Engg & Tech guided many UG & PG students. His research areas include MANETs, Routing Protocols, Data mining, and Artificial Intelligence.