Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Algorithmic Approach for Detection of Sybil Attack in MANET

Sangeeta Bhatti*, Prof Meenakshi Sharma

Dept. of CSE, SSCET, Badhani,

Punjab, India

Abstract— Security is an utmost anxiety in any ADHOC network. Mobility of nodes postures a difficulty for giving security amenities in Mobile ADHOC Networks (MANETs). As ad-hoc network uses wireless communication link between the mobile nodes that's why it is more vulnerable to attacks. The Sybil attack is a predominantly harmful threat, where an individual node illegitimately claims numerous identities in mobile ad hoc networks. In this paper we proposed an identity verification and resource based algorithmic approach for the detection and elimination of Sybil nodes. In proposed technique secure identity of nodes are assign to all nodes to detect the Sybil node. The Sybil node is detected with involvement of base server by verification the identity and resources node through the trustworthiness of Secure Id of all node. Here the notion of unique id using secure id is used which lead to more secure communication in network.

Keywords— Sybil Attack, Unique Keys, Identity Verification, Resources, MANET

I. INTRODUCTION

Mobile ad-hoc networks (MANET) symbolises complex distributed systems which are continuously self-constructing, infrastructure less network of mobile devices connected by deprived of wires. Since MANETS are mobile that's why they use wireless acquaintances to connect to numerous networks. It can be a usual Wi-Fi connection or any other medium e.g. a cellular or satellite transmission.

Basically MANETs are of two types i.e. open and closed networks. Closed MANETs do not provide any kind of open access. Hence all nodes that are establishing the network are pre-distributed through some kind of identifications which are necessary toward joining the network. On the other hand open MANETs do not have any kind of well-defined boundaries i.e. anyone can join and left the network at any time. The major problem in open MANET security i.e. to provide protection from selfish and malicious nodes in the network operation.

Sybil attack is one of the vital and challenging problem in open mobile Adhoc networks. Sybil attack is a serious threat to these networks due to need of a distinctive, individual and persistent identity per node plus absence of central identity management. A Sybil attacker can affect to the ad hoc networks in many ways. For example the attacker could make usage of numerous identities concurrently or one after another, to play with the trust computation system. Sybil attack can disrupt the whole routing structure by contributing in the routing, giving the false impression of separate nodes on dissimilar positions or node-disjoint paths and altering the trust values of nodes randomly out-vote honest nodes. Moreover, the assailant might go offline, if detected and then again reconnect through additional set of identities to introduce a new attack. Unique identification of nodes in MANET is a challenging task due to the absence of any central authority.

In this paper we proposed an identity verification and resource based approach for the detection and elimination of Sybil nodes. The paper is organised as follow. In section II, Related work is discussed. Section III represents the research queries, proposed work is discussed in section IV. Section V represents the algorithmic representation. Results are discussed in section VI, Conclusion and future scope of the proposed technique is given in section VII.

II. RELATED WORK

This section describe the various work done in analysing and prevention from Sybil attack in MANETs.

Wenyu et al[1] proposed two-class undirected assorted association stochastic block models to discover opponent's Sybil identities within the network. The proposed model distinguishes Sybil identities through simulating the reproductive procedure of social networks. R. Vintoh et al [2] has used certification authority and RSSI as different parameter to find out the Sybil nodes. In this the responsibility of certification authority is given to cluster head and RSSI is used to form the cluster. Sohail et al [3] proposed a lightweight scheme to identify the nodes of Sybil attacker by deprived of using centralized trusted third party or any extra hardware, such as a geographical positioning system or directional antennae A. Aranganathan et al [4] also proposed a mobile agent based scheme to recognise the Sybil nodes without using centralized trusted third party or any extra hardware such as directional antenna or a geographical positioning system.

Sarosh et al[5] evaluated the efficiency of existing authentication techniques for MANET from preventing Sybil attack, the infrastructure needed modelled by these techniques and availability of these practices to different types of ad hoc networks. Sarosh Hashmi [6] proposed an authentication model for MANETs which exploits hardware id of the device of each node for authentication. In this an authentication agent is created that identify the hardware id of the node. Zolidah et al[7] calculated the throughput performance in AODV with the presence of wormhole and Sybil attack. The simulation result represents that there is different recital in throughput when there is an attack. Muhammad et al[8] proposed a novel scheme for the detection a Sybil attack resistant to collusion through integrating a trust based mechanism that would mitigate the benefit (the payoff gained) from collusion.

Somnath et al [9] also introduced a new method for the detection Sybil nodes based on clustering in addition to resource testing. Himika et al [10] discussed an enhanced lightweight Sybil attack detection technique which is used to detect Sybil attack. Kuo-Feng et al [11] developed a scheme in which the node identities are verified merely through analysing the neighbouring node information of each node in order to protect WSNs against such Sybil attack. E.A. Mary [12] proposed a certification based localized authentication scheme for the prevention of Sybil identities Athichart et al [14] proposed a robust Sybil attack detection framework for MANETs centered on cooperative monitoring of network activities.

III. RESEARCH QUESTIONS

The main purpose of this paper is detection of Sybil Attack in MANETs and design a secure network, thus the performance of the network can enhanced. And to protect the network from Sybil identity generate unique id with secure id to build more secure communication in network. The research queries are as follow:

RQ 1:- As MANET has no centralized management system, it is more vulnerable to several types of attack such as Sybil attack that arise the question of designing a secure network.

- This model aims to propose a algorithmic approach for detection of Sybil attack in MANETs.

RQ 2:- A Sybil attack can creates multiple virtual fake identities per entity, and consume the energy and another resources and transmit false information, which led to the question of effective utilization of available resources while preserving the information.

- This query will check are the existing algorithms satisfying this condition.

IV. PROPOSED WORK

In our proposed work, we are detecting the presence of malicious Sybil node in the route discovery phase. We used three orthogonal dimensions i.e. direct v/s indirect communication, fabricated v/s stolen identities, and simultaneity for the detection of Sybil nodes.

Basically there are two ways to validate an identity. The one way is direct validation where a node directly tests whether the identity of other node is valid or not and another way is indirect validation where already verified nodes are allowed to vouch for or refute other nodes.

In the proposed identity verification and resource based algorithmic approach the key pool defense is used for direct validation of nodes. During direct validation we try to detect the malicious nodes when it try to initiate communication with a legitimate node in a network. A unique identification is needed to create a secure link to other nodes. A node is registered itself to base server. Basically a base server is that server which responsible for all activities or area where node participate to each other. It plays an important role to assign the unique identification to all nodes in a network. This server have identification authorities to check the validity of all nodes in the network.

A. Registration Phase

In first step, node has registered itself in base server which will generate unique identification to all nodes on the basis of resource evaluation.

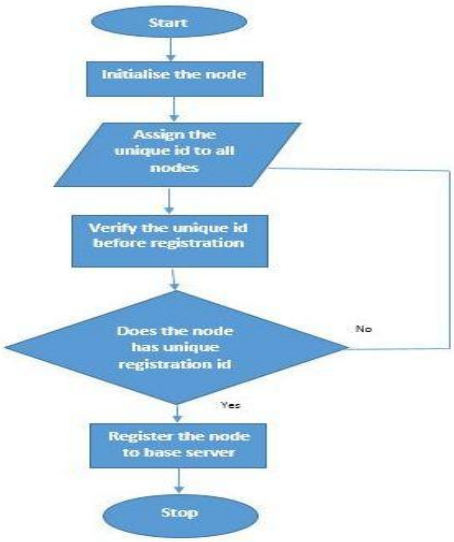

Figure 1. Registration Phase

B. Unique-id (Uid) Generation:

U-id composed of MAC address and node resources. The resources is depend upon radio signals, position verification and previous registered id of nodes. In order to complete registration node required unique id and session key.

U-id = {MAC add + NR}

{Where **MAC add** is MAC address

NR is node resources}

NR = [RS + PV + PR _id]

{Where **RS**= radio signal, **PV**= position verification of nodes, **PR id** =Previous registered id if any}

Registration Completed= UID + Session Key

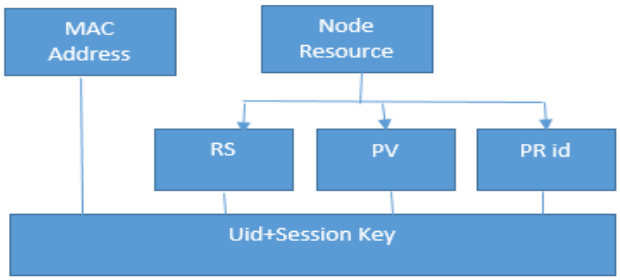

Figure 2: Unique-id (Uid) Generation.

Once the node is registered it is eligible to communicate with other nodes in network. Sybil nodes try to hamper the network communication. Now during message transfer Sybil node will acquire identification similar to that legitimate node and try participate in the network. To detect the Sybil node we proposed a new technique on the basis of identity verification and resource verification.

In this technique the registered node is assigned the unique id then the base server compare the unique id of all nodes within the session and assign a new secure id to all nodes.

Secure Id=CUid – Uid

Where **CUid** = change unique id

Uid=unique identification of nodes.

Basically the secure id lies between 0 and 1. If the node has value 0 then it is Sybil node. Where 0 means that same number of resource node in the network has been registered which has same resources.

V. ALGORITHMIC REPRESENTATION

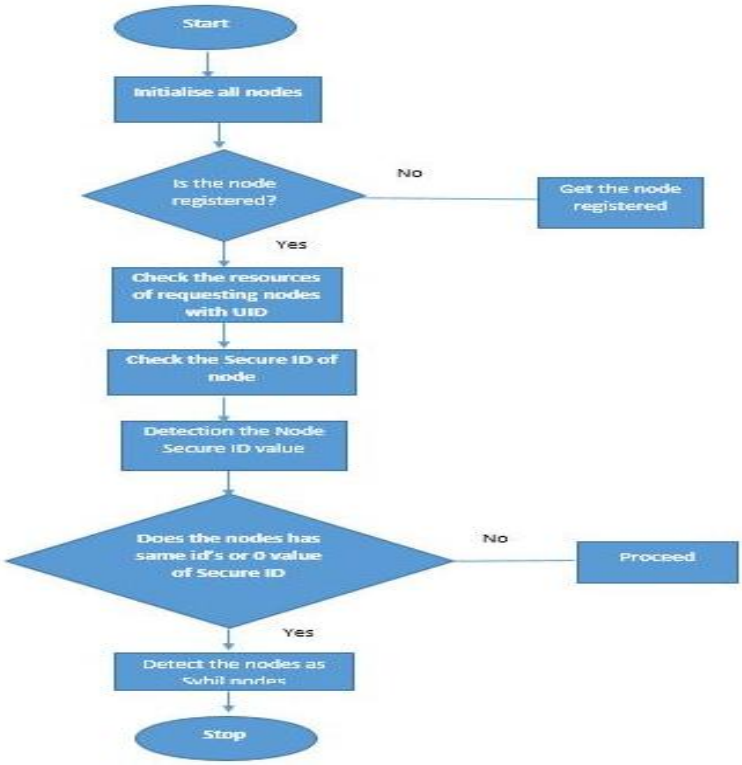

Figure 3. Flow Chart Representation of Algorithm

VI. SIMULATION AND RESULTS

The simulation study depicts the following results of the proposed algorithm for detection of Sybil attack in MANETs. To study the performance of our proposed work by using NS2. Simulation parameters used are listed in Table 1.

Table 1. Simulation Parameters

Parameters	Values
Area	1500 * 1100 meter
No of Node	35
simulation duration	950 s
physical/Mac layer	IEEE 802.11 at 2Mbps
Initial energy per node	2 Joules
Data Rate	2.0

We consider the following parameters to measure the performance of proposed Sybil Attack Detection technique

1. Throughput– It is defined as the amount of data traffic successfully received and forwards to the higher layer by WLAN MAC

$$\text{Throughput} = \frac{\text{No. of delivered packets} * \text{Packet size} * 8}{\text{Total duration of Simulation}}$$

2. PDR– Packet delivery ratio is defined as the ratio between the number of data packets received and the number of data packets sent.
3. Energy consumption – This is the average of ratio of number of data packets reached at destination to the sum of the energy consume by all nodes in the network.
4. Packet Dropped– It is the difference between total number of packet transmitted by transmitter and total number of packet received by receiver at receiver end.

Figure 4 depicts the average throughput. The Graphs shows that, the Throughput rate of proposed algorithm is 97% with respect to time. Graph show that initially the throughput was low as it was time required to setup up a secure connection but later the graph shows the average rate of increase in throughput in proposed algorithm of detection of Sybil attack is very high.

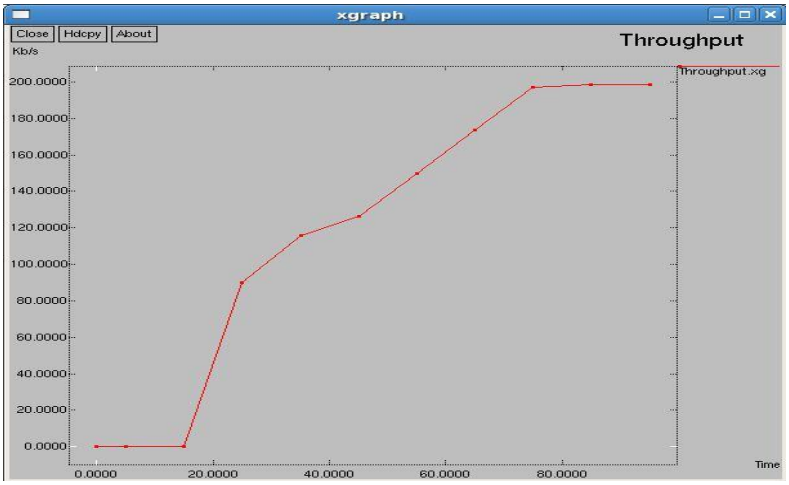

Figure 4. Represents the throughput graph of the proposed algorithm.

Figure 5 depicts the average packet delivery ratio of data. The Graph shows that initially there is drastic increase in packet delivery ratio with less increase in time in the proposed algorithm, after some time it become stable but there is no loss in packet still the delivery of packet is 97% cent.

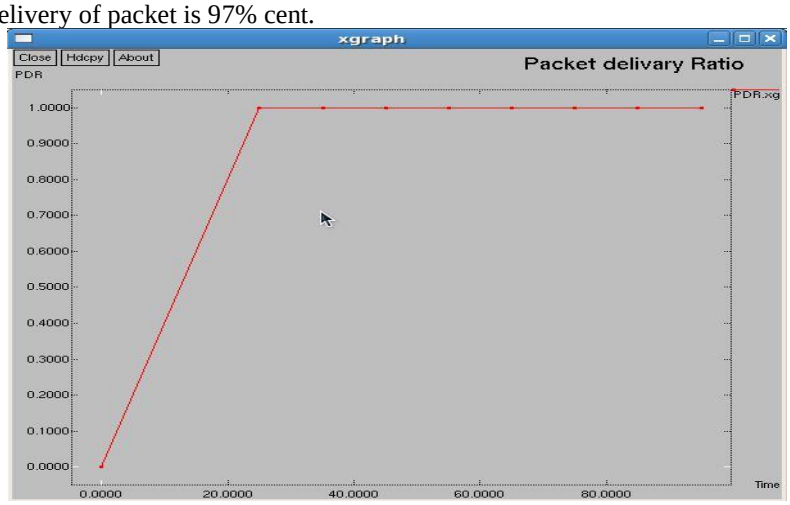

Figure 5. Represents the packet delivery ratio in proposed algorithm.

Figure 6 shows the average consumption of energy, graph depicts that the loss in energy in the proposed algorithm is drastically decreases, thus the proposed algorithm consumes very less energy.

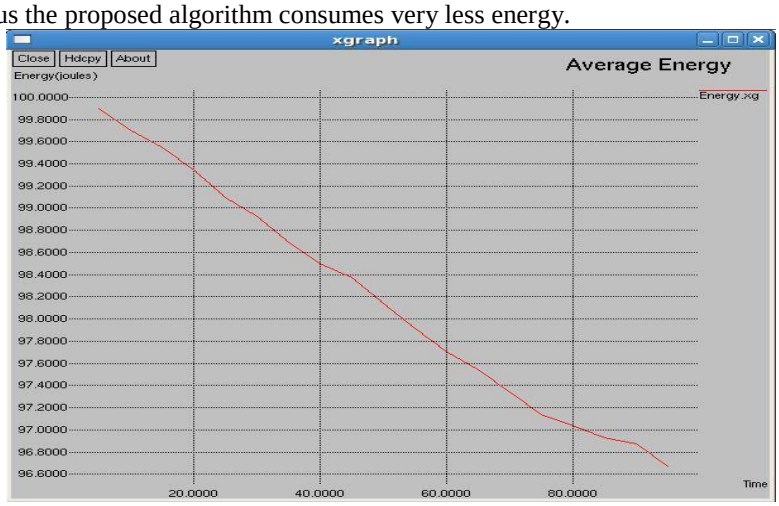

Figure 6. Represents the average energy consumption in proposed algorithm.

Figure 7 depicts the packet Drop with respected to time. The graph shows that there is no packet dropping in proposed algorithm for detection of Sybil attack in MANETs. All the packets are generated by the source are received by the receiver end.

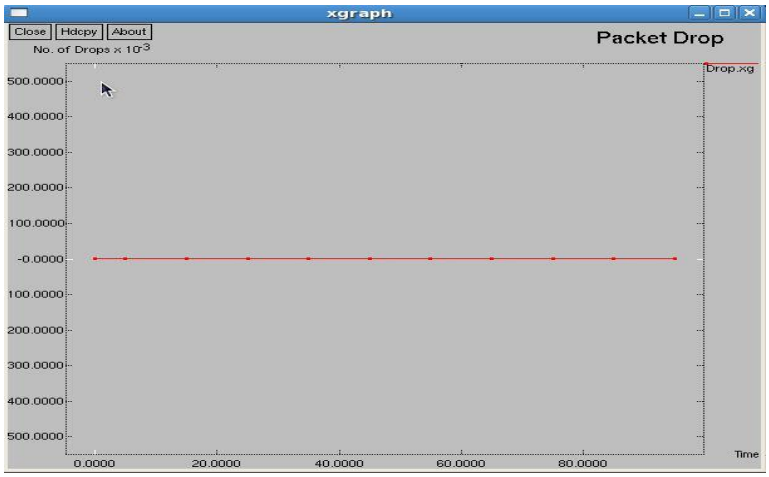

Figure 7. Represents the average number of packet dropped in the proposed algorithm.

VII. CONCLUSIONS

Security is one of the foremost issues in MANET. In this paper a solution is proposed to detect the presence of the attacker in the Route discovery phase. The proposed technique uses the secured unique identification generated by the base Server during the time of the registration of a node into the network. Hence it would lead to a secure communication network with the detection of Sybil nodes using the identity and resource verification. Results depicts that this technique increase the overall performance of the network by detect all the attacker node or Sybil node or spoofing node and achieve high throughput with high packet delivery ratio, less energy consumption and no packet dropping .

Our future work will be to make more secure wireless network and propose more effective technique to detect the Sybil node.

ACKNOWLEDGMENT

I would like to appreciatively and sincerely thank to Prof. Meenakshi Sharma for giving her valuable time for support in the research period. I also thank to my parents, and friends, who provide the guidance and financial support. The product of this research paper would not be possible without all of them.

REFERENCES

[1] Wenyu Zang "Detecting Sybil Nodes in Anonymous Communication Systems," International Conference on Information Technology and Quantitative Management, Elsevier 2013.

[2] R. Vintoh kumar, "Cluster Based Enhanced Sybil Attack Detection in MANET through Integration of RSSI and CRL" *International Conference on Recent Trends in Information Technology, IEEE 2014*.

[3] Sohail et al," Lightweight Sybil Attack Detection in MANETs" *IEEE SYSTEMS JOURNA 2012*.

[4] A. Aranganathan et al, "Mobile Agent based Security in MANETS against Sybil Attack," *International Conference on Control, Instrumentation,* Communication *and Computational Technologies (ICCICCT),* IEEE 2014

[5] Sarosh Hashmi, John Brooke, "Authentication Mechanisms for Mobile Ad-hoc Networks and Resistance to Sybil Attack," *The Second International Conference on Emerging Security Information, Systems and Technologies, IEEE 2008.*

[6] Sarosh Hashmi, John Brooke, "Towards Sybil Resistant Authentication in Mobile Ad hoc Networks," *Fourth International Conference on Emerging* Security *Information, Systems and Technologies, IEEE 2010*

[7] Zolidah Kasiran and Juliza Mohamad, "Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV" in Conf. Rec. IEEE 2014.

[8] Muhammad Sajid Khan et al "Collusion-Resistant Sybil Attack Detection Scheme in Mobile Ad hoc Networks," *National Software Engineering Conference (NSEC), IEEE 2014*

[9] Somnath Sinha, Aditi Paul, and Sarit Pal, "The Sybil Attack in Mobile Adhoc Network: Analysis And Detection" *in Conf. Rec. IEEE 2013*

[10] Himika, "Enhanced Lightweight Sybil Attack Detection Technique," 5th International Conference- Confluence, the Next Generation Information Technology, *IEEE*, 2014.

[11] Kuo-Feng Ssu, Wei-Tong Wang and Wen-Chung Chang "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information,", *Elsevier 2009.*

[12] E.A. Mary, "Sybil Secure Architecture for Multicast Routing Protocols for MANETs" *CCIS 190, pp. 111–118,* Springer-Verlag *2011.*

[13] Bo Yu, "Detecting Sybil attacks in VANETs" / J. Parallel Distrib. Comput. 73 pp. 746–756, Elsevier 2013.

