Evaluation of Sybil Node in MANET Based on Received Signal Strength

Chaman Kumar*

Assistant Professor, Faculty of Information Technology
IIMT College of Engineering, Greater Noida, India
*chamankumar31@gmail.com

Abstract

Detection of Sybil attack in MANET has been a serious issue in mobile ad hoc network. This article proposes a new approach towards Sybil attack detection where legitimate and Sybil nodes are distinguished using received signal strength (RSS). Generally a Sybil attacker creates multiple forged identities with higher transmission power than that of the legitimate nodes. Four detector nodes were used to calculate the signal strength from the Sybil node and to draw a relation between them.

Keywords: MANET, Sybil attack, NS2, RSS

1. Introduction

Mobile ad hoc networks are vulnerable to varieties of security attacks due to their inherent characteristics. Mobility, decentralized architecture, scalability and resource constraints open paths for malicious attackers who not only disrupt the network activities but also spoof secure information. Sybil attack [1] is the one such attack in which a spiteful attacker creates arbitrarily many forged identities and uses them time to time to communicate with legitimate nodes in the provided network where attacker can also compromise the true nodes in the network in order to launch the attack. The notion of the attack remains same however the dimension may differ. In WSNs and MANETs, the Sybil attack poses a serious concern. By giving incorrect routing information or directing routing and information packets to malicious peers, this attack severely interrupts routing protocols. In order to destabilize the target network, the Sybil attacker launches a series of follow-up attacks. If the attacker node provides its phoney identity (Sybil nodes) by altering the transmission power, the assault becomes much more severe and difficult to detect. Since Sybil attack has a serious impact in MANET applications its mitigation is thus an inevitable issue in order to maintain a secured network. Various Sybil detection methods have been suggested and implemented by the researchers over a period of times among which trusted certification [2] is said to remove Sybil attack completely. But this technique has some infeasibility in case of establishing central authority in a very large network.

The RSSI based technique [3] on the other hand records RSSI of the nodes time to time in order to find a matching between a node' ID and its RSSI. Nodes with different IDs but same RSSI are tracked as Sybil. Again this technique is applicable to WSN only. Moreover, this method does not incorporate the mobility of nodes and uses the IDs of nodes for matching. Also the nodes with varying transmission remain undetected by this method. In this research, we looked intoa specific group of Sybil attack where the Sybil attackers adjusting their transmission power on a regular basis in order to mislead the genuine nodes. To detect this type of attack we propose a Sybil attack detection technique which uses the RSPs (receive signal power) by the detector nodes to distinguish between legitimate nodes and suspected ones. We calculate the signal power receive by the detector node and try to find out a relation between the calculated values which will be effective in detecting the nodes which vary their transmission power keeping its position unchanged only to represent it as a separate identity. In the subsequent section we represent the related work in section 2, problem domain in section 3, model formulation in section 4, simulation results in section 5 and analysis and discussion in section 6.

2. Literature Available

Various Sybil detection techniques have been suggested over time. Among those few of them are able to bring down the to a reasonable level of threatwhile some techniques suffer from various constraints. Many approaches that have been suggested to prevent and mitigate Sybil attack are categorized as follows:

2.1 Trusted Certification

One of the most promising solutions for preventing Sybil attacks is having trusted certification [2]. It requires a single certification authority (CA) to verify an organisation and its related identity are one and the same. Douceur has demonstrated that trustworthy certification is the universal strategy that has the greatest chance of entirely eliminating the Sybil attack [1]. This strategy may appear to be excellent for dealing with the Sybil attack, however there are a number of concerns with the certifying agency and entity-identity mapping implementation. The adoption of this approach in a big network is likewise limited by its high overhead and cost.

2.2 Testing Process

One among the most extensively utilised approaches for defending against Sybil attacks is resource testing. Because the network entity's resources are restricted, the number of resources consumed by the entity can be compared to the standard unit of the assets maintained by that entity. Any mismatch implies a Sybil attack is possible. Resources are generally defined as energy storage, available memory size, computing capabilities, bandwidth, and channel capacity. Newsome et al. [4] introduced radio resource testing as an expansion of the material testing method towards wireless sensor networks.The essential premise of this technique is that every physical equipment has only one radio, which is unable of receiving and transmitting messages on atleast one channel at the same time.

Many academics propose using resource tests to discover Sybil nodes instead of eradicating them completely. It could also be used to apply to a wide range of related disciplines.

2.3 Recurring cost

This technique is a version of testing resources, in which various resource are tests and performed on a regular basis to foist a "cost" on the attacker for each detects that he owns or brings in the networks. However, while various studies have validated that technique [5-7], it may be insufficient in limiting the attack since, as Levine et al. [2] point out, an unauthorized user incurs just a single charge (for computer resources) which can be reclaimed via the performance of the assault itself. Only if the ratio of the attacker's motive function value towards the cost / identity surpasses the critical value is an attack considered successful (the value that used for a specific application domain). They results that recurrent expenses or fees / identity are more efficient than just a single resource test as a deterrent against Sybil assaults. The only drawback is that it either electronic cash or a large amount of human labour [5].

2.4 Privilege attenuation

In Fong [8] proposed a new type of Sybil attack in which the attacker generates pseudonymous or fictitious identity inside Social Network System (SNS) then brings them together to favourably modify the network's current trust connections. These connections are represented by a social graph, which is a graph-theoretic connection model that occurs between both the producer of a resources and a potential user of that resource. Some major Social Network Systems, such as Facebook, use such models.When phoney identities on social media sites work together, they may obtain access to personal, sensitive, and restricted user information, as well as undertake large-scale crawls of the social network [9]. To mitigate this issue, Fong presented a customized form of Denning's Principle of Privilege Attenuation, or POPA, as a sufficient and necessarycondition for preventing such assaults, as well as a static policy analysis to validate POPA compliance [8].

2.5 Incentive–based detection

In [10], Margolin and Levine presented the Informant protocol, which is built on an incentive structure policy which is not restricted toward any application domain. To thank Sybil for exposing themselves, as an entity is hired as a detective. The detective receives the target peer's name and a security deposit, while the objective partner receives the deposit as well as a reward for revealing itself. The minimal reward for revealing a Sybil node is determined by a Dutch auction. This strategy, however, only works if the Sybil appears spontaneously.

2.6 Position verification

This technique is only applicable to radio ad hoc networks. This would be based on the idea that 2 or more identities should not occupy the same network place at the same time.

Tangpong devised a method for position verification termed triangulation [11]. Sybil nodes are identified using proposed technique as they appear in the same location as the compromised node which generates them. The authors of [12] offered a solution depending on the technique described above. In a highly mobile and dense network, however, this technique produces false positive results.

2.7 RSSI-based scheme

The Received Signal Strength Indicator (RSSI) of signals was proposed by Demirbas and Song [13] as a tool for Sybil detection. After accepting a message, each receiver adds the RSSI of a signal towards a sender ID in it, according to this technique. The sender receives Sybil attack when two messages with the same RSSI but separate IDs are received later. Sybil assaults may be identified with 100% accuracy using this method, with only a few false positives. This technique, however, is only relevant to sensor networks. Furthermore, to thwart this technique, a Sybil node will send messages with alternate identities and transmission powers. The scenario becomes more complicated with a MANET since the attacker changes direction from time to time.

2.8 Random key Pre-distribution

In a cellular sensor network, this method is implemented to construct secure routing among two communicating nodes [14]. A node is provided with a set of keys at random, from which it evaluates the common keys it exchanges with some of its neighbour. To secure node-to-node privacy, the shared keys are being used between the nodes. The validating of the keys linked with a node seems to be the technique's most important requirement. Validation guarantees that the key can be validated by the network. However, there is a slim chance that only a Sybil identity would pass a key validation testing because the set of keys linked with a random identity is unlikely to overlap with the come to terms key set in a meaningful way.

3. Attack Model

In this section we concentrate our motivation towards designing a special category of Sybil attack model in which a Sybil node changes its identification and transmitting power on a regular basis to execute the attack. The proposed scheme aims to detect this type of attack in MANET where the nodes move with certain velocity. We design the specified attack model with the help of network simulator NS2.35 and demonstrate the attack scenario graphically.

During transmissions, a Sybil node can alter its transmission capability to introduce a various virtual illegitimate node. During communication, the adversary compromises some genuine nodes and uses them to symbolize itself. The compromised nodes communicate incorrect transporting data to the source host via a reply routing packet, claiming to have the quickest routing path to the attacker's destination. When communication travels via the attacker, all data packets are dropped totally. In ability to

intervene as a new valid neighbour in the network, the attacker uses a greater transmission capacity than the legal nodes during the attack. As a result, during an assault, the Sybil nodes' transmission power exceeds that of the other nodes. The source and destination nodes, we assume, are moving. To produce relative movement between all the nodes, the destination node moves on the way of the source and far from the source node. The discarding of packets by an attacker significantly lowers network throughput during communication. We also looked at the attacker's movement by changing the pace to three parameters and analyzing the effect on network performance. For our experiment, an attacker having four peers, one source node, and one target is used, and even the topology is described in the NAM document (fig. 9) while implemented on the NS2.35 platform.

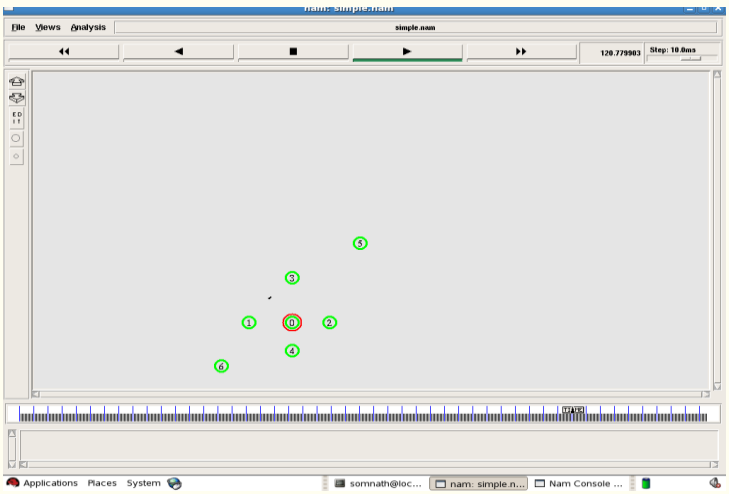

Figure.1 Topology of attack model

Node 6 seems to be the source, while node 5 seems to be the sink, according to the assault model (destination). Sybil is given to Node 0, jeopardising another existence (node 1). After a 5-second time interval, Node 0 switches its transmission power between 1.8 and 2 watts. The sink node is moving towards the source at a rate of 15m/s. Because of this assumption, the network's other nodes are relatively mobile in relation towards the source and the destination. The simulation is run over a period of 150 seconds. When the destination and source nodes are well within the communication range, the greatest transmission occurs between 100s and 125s. The attack is carried out between the hours of 100 and 150.

4. Theoretical Model

We offer a short theoretical background of the suggested detection approach in this part.

The RSPs of the suspicious nodes are calculated in this section. Sybil node, we believe, does not vary its position over time. In light of this, we chose four detecting nodes (Fig. 2) in close proximity to the Sybil node. The propagation model used by the nodes

when interacting with one another is an essential factor to consider. To compute the RSP, we use the Two-Ray Ground Modeling Approach described by the following equation.

$$P_r=\frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L}$$

Where P_t seems to be the transmission power and G_t is used to denote the transmitterantenna gains and G_r are used to denote thereceiver antenna gains, respectively. L ($L \geq 1$) seems to be the overall loss. In ns simulations, $L = 1$ and $G_t = G_r = 1$ are commonly used, where d is used to denote the Euclidean distance distanceb/w each observer node and the suspected node.

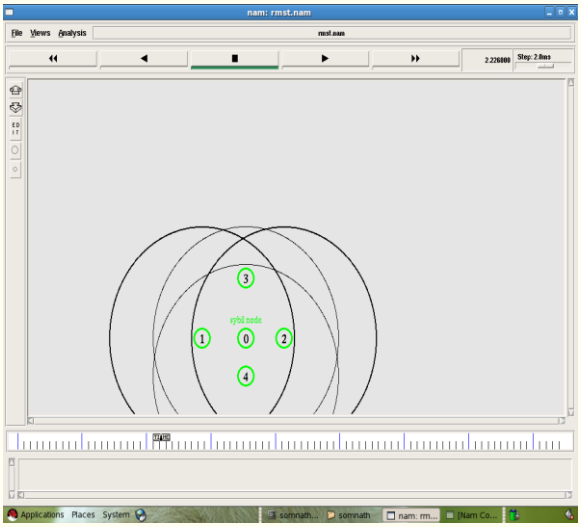

Figure.2 representing four detector nodes in the radio range of a node 0.

We can now determine the position of a Sybil node in terms of four detector nodes using these assumptions. If node I (xi,yi) gets a radio signal from Sybil node 0(x, y), then the RSP is

$$R_i = \frac{P_t \alpha}{d_i^4} \qquad 1)$$

Where, P_t represents transmitted power of node 0, R_i is RSP of node i, α is constant, d_i is Euclidean distance from the source node.

Similarly for node j the RSP is

$$R_j = \frac{P_t \alpha}{d_j^4} \qquad 2)$$

Taking the ratios of these two RSPs we get

$$\frac{R_i}{R_j} = \frac{d_j^4}{d_i^4}$$

$$\text{Where} \frac{d_j^2}{d_i^2} = \frac{(x-xi)^2+(y-yi)^2}{(x-xj)^2+(y-yj)^2} \qquad 3)$$

Proceeding in the similar fashion we get $\frac{Rj}{Rk}$, $\frac{Rk}{Rl}$, $\frac{Rl}{Ri}$(as eq. 3) for the nodes i, j, k, l respectively at a given time (say t_1). These numbers are used to examine the path(x,y) of the suspected node (node 0) by putting the known coordinate values of the nodes $l(x_i,y_i)$, $k(x_j,y_j)$, $j(x_k,y_k)$, $i(x_l,y_l)$.

Now if the Sybil node changes its transmission power in another time (say t_2) then the calculated RSP is

$$R_{i1} = \frac{P'_t \alpha}{d_i^4} \qquad 4)$$

for node i.

Similarly we calculate RSPs for nodes j, k and l. again these values can be used for locating the Sybil node at a new position. Equation 1 and equation 4 are used to calculate the RSPs of the suspected nodes for two different time instant $t_1$and t_2 .As the Sybil node don't change its position

$$\frac{R_i}{R_j} = \frac{R_{i1}}{R_{j1}}$$

5. Simulation Results

The proposed model uses Network Simulator NS-2.35 with the parameters specified in Table I to build and test proposed method. The trace and NAM file is created based on the requirements.We have used equation 1 and 4 for the calculation of RSPs. The following tables describe the details of the simulation parameter used.

Table 1 .Typical simulation parameter values for the NS-2.35 utilizing the AODV routing protocol

Parameter	**Value**
Transmission power	1.8/2 w
Frequency	2.472×10^9
Initial energy	100 J
Collision threshold	100
Carrier sense threshold	5.011872×10^{-12}
Receive power threshold	5.82587×10^{-09}

Ideal Power	712×10^{-6}
RxPower	35.28×10^{-3}
TxPower	31.23×10^{-3}
SleepPower	144×10^{-9}
Simulation time	150s
Speed of the sink node	15m/s

As described in section 4, we test our detection technique inside a MANET of seven nodes, with node 0 acting as the attacker. Node 1 periodically delivers incorrect transmitting data to node 6 by portraying this as node 0 & increasing its sequence number above the least recent value. As a result, node 6 assumes node 0 seems to have the shortest path to the target and transmits data packets to node 0. When the data packets reach Node 0, it is consumed. The compromised node removes the identity of the Sybil nodes on a regular basis and sends data packets to the Sybil node. To depict itself as a separate node, Node 0 changes its transmission power from time to time. We consider the signal power receive by the detector nodes at two different instant of time 103s and 115s and calculate their ratios to arrive the conclusion.

103.009395 0->4[0->-1] -95.031927

103.009395 0->2[0->-1] -98.678358

103.009395 0->1[0->-1] -101.761372

103.009395 0->3[0->-1] -104.432000

115.660425 0->4[0->-1] -96.085532

115.660425 0->2[0->-1] -99.731964

115.660425 0->1[0->-1] -102.814977

115.660425 0->3[0->-1] -105.485605

Obviously -95.031927/-98.678358 = -96.085532/-99.731964 which verifies our result.

6. Conclusion and Future Work

The authors tried to find out the relation between the signals powers receive by the detector nodes surrounding the Sybil node and trying to represent them graphically. As a future work this graphical representation will differentiate between a Sybil node and a legitimate node. However the interesting point will be to see the cases where legitimate node also varies their transmission power according to their requirements. Also in case of MANET there is node movement. As a future work the authors want to incorporate the speed of the Sybil node in the detection approach.

7. Conflict of interest

The authors declare that they have no conflict of interest

References

[1]. Douceur JR. The Sybil attack. In Proceedings for the First International Workshop on Peer-to-Peer systems (IPTPS'02) LNCS: Springer, US; 2002. 2429. pp. 251–260.

[2]. Kolshwar AS, Sherekar SS, Thakre VM. ADouceur JR. Analytical Classification of Sybil Attack Detection Techniques. In Hemant J et al. (eds). IDCTET. LNDCT: Springer, Singapore; 2021.57.

[3] Angappan A, Sarayanbaya TP et al. Novel Sybil Attack detection using RSSI and neighbor information to ensure secure communication in WSN. J. Ambient Intel.l Human Comput. 2021; 12: 6567-6578.

[4] Newsome J, Shi E, Song D. Perrig A. The Sybil attack in sensor networks: Analysis & Defences. In Proceedings of the third international symposium on Information processing in sensor networks (IPSN'04); 26–27 April; Berkeley, California: ACM; 2004.pp 259–268

[5] Majid M, Habib S, Javed AR et al. Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review.Sensors.2022; 22: 2087

[6] Teekaraman Y, Manoharan H, Manoharan A. Diagnoses of reformed responses in curative applications using wireless sensors with dynamic control.
Sustainable Computing: Informatics and Systems.2022; 35: 100677.

[7] Maniatis P, Roussopoulos M, Giuli T, Rosenthal DS, Baker M. The locks peer-to-peer digital preservation system. ACM Transactions on Computer Systems. 2005; 23(1): 2–50.

[8] Fong P. Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems. Symposium on Security & Privacy: IEEE; 2011. pp. 263-278.

[9] Azab A, Idrees A, Mahmoud MA, Hefny H Q. Fake Account Detection in Twitter Based on Minimum Weighted Feature set. International Journal of Computer and Information Engineering. 2016; 10(1):13-18

[10] Margolin, N. Boris, and Levine, Brian Neil, Informant: Detecting Sybils using incentives. In Proceedings of Financial Cryptography (FC) (February 2007. LNCS: Springer, Berlin; 2007. 4886. pp. 192—207

[11] Tangpong A. Managing Sybil Identities in Distributed Systems. Ph.D. thesis: Pennsylvania State University; 2010

[12] Wang C, Zhu L, Gong L et. al. Accurate Sybil Attack Detection Based on Fine Grained Physical Channel Information.2018;18(3): 878.

[13] Jamshed MA, Ali K, Abbasi QH, Imran MA. Challenges, Applications, and Future of Wireless Sensors in Internet of Things: A Review. IEEE Sensors Journal.2022; 22(6): 5482-5494.

[14] Du W, Deng J, Han YS, Varshney PK. A pairwise key pre-distribution scheme for wireless sensor networks. ACM Transactions on information and system security. 2005; 8(2):228-258