Sybil Attack detection by Enhanced Lightweight Technique in MANETs – A Review

Barinderpal Singh

ABSTRACT

Mobile Adhoc networks are more susceptible to attacks as it consists of free a node which communicates with each other through wireless links between them. Security is an utmost concern in any ADHOC network. There are many attacks which wreck the communication among the nodes of network. Among those attacks there is a Sybil attack which poses a serious threat and causes severe hazards to the network. Sybil attack is an attack which uses multiple identities at a time or one identity at a time in order to launch a synchronized attack on the network or can switch identities in order to weaken the detection process This attack can decrease the trust of any genuine node by using identity of that node and gather the secret or important data. Sybil attackers distribute secret data in other networks and it reduces the secrecy of network. In this paper, Enhanced lightweight Sybil attack detection techniques with its types are discussed. The purpose of this paper is to summarize the existing Sybil attack detection techniques that have been suggested over time to decrease or eliminate their risk completely.

Index Terms: Sybil attack, Mobile Adhoc Network.

Introduction

MANET is used in many realistic application such as personal area network, military and police environment, home area network, disaster relief operations. (MANETs) represent complex distributed systems that consist of wireless mobile nodes that can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies [1]. There are some security goals to check whether MANET is safe or not [13]. Some of the security goals are availability, confidentiality, integrity, non repudiation and authentication. These security goals should be well maintained in any network for proper communication.

Ad hoc network is an autonomous system consisting of nodes, which may or may not be mobile, connected with wireless links and without using pre-existing communication infrastructure or central control. Due to random change of topology and infrastructure less nature of MANET, the network can easily be attacked by several attacks. Attacks are classified as Active and Passive attacks.

Sybil Attack is an active attack which creates lots of fake intuition in the network like decrease the trust of legitimate node by using their identities, disturbs the routing of packets so that they cannot reach to its desired destination, and many more. Also the attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or node-disjoint paths [11]. Sybil attackers can create an arbitrary number of virtual non-existent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic [3]. Therefore, Sybil attacks will have a serious impact on the normal operation of wireless ad hoc networks. It is strongly desirable to detect Sybil attacks and eliminate them from the network. In this paper, a Lightweight Sybil Attack Detection Technique is proposed which is used to detect the Sybil nodes in the network.

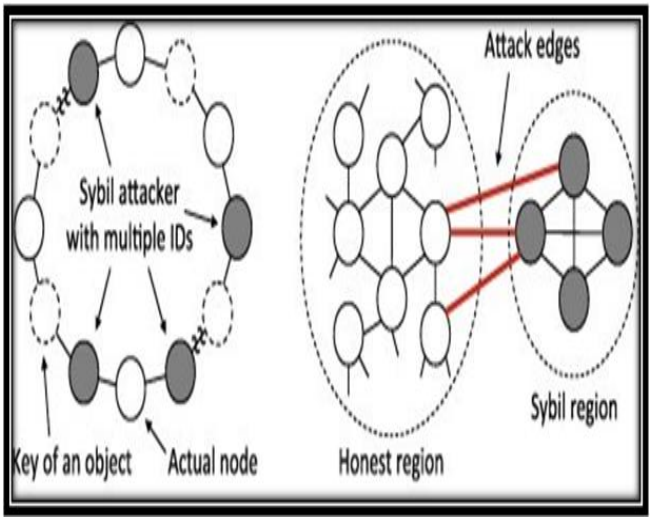

Figure 1: Sybil Attack showing attackers with multiple ID's

Related work

In any network, the most important part is to maintain security. Due to security there will be safe communication among nodes and ultimately that results into good output of network. The work done to remove Sybil attack in MANET is following:

Garg [14] et al proposed a scheme where two parameters are used i.e. energy and frequency. By using these two parameters it is giving better results than previous. In this threshold value of speed is taken as same i.e.10m/s and threshold value of energy and frequency are set as average energy of network and average frequency of network. Sometimes there is Sybil nodes whose speed is less than 10m/s and these nodes are detected as legitimate nodes.

Piro et al. [4] proposed a scheme to detect the Sybil nodes by examining the behaviour of nodes. This scheme gives high false positives results when group of nodes move in same direction. According to this scheme, the nodes which move freely, independently in different directions are considered as genuine nodes and the nodes which moves together are suspected as Sybil nodes and it keeps observing these suspected nodes.

Sarosh et al [7] evaluated the efficiency of existing authentication techniques for MANET from preventing Sybil attack. He 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.

In [5] authors discuss about the social networking concept to prevent the Sybil attack. On the basis of trust relationship, analysis can be made about the nodes that whether they are Sybil or legitimate nodes. According to this, Sybil node is not able to develop trust relationship with the legitimate nodes present in the network as it changes its identities again and again.

BARTER [8] is a behavior-based access and admission control system for MANETs in which nodes initially exchange their behaviour profiles and calculate individual local definitions of normal network behaviour. During admission, each node issues an individual decision based on its definition of normalcy. These individual decisions are then combined via a threshold cryptography that requires agreement among a fixed amount of MANET nodes to change the status of the network.

Kifayat [19] Presented a lightweight scheme to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system.

In [9] authors proposed DCA scheme. This scheme helps to prevent the Sybil attacks with the help of certificates. Certificates are distributed to all nodes present in the network and nodes use these certificates as a proof of their identities.

Attacks in different layers

Each Layer is vulnerable to various threats and is susceptible to attacks. The Following table shows the classification of security attacks in different layers in MANET.

Table 1. Attacks in Layers

S.No.	LAYER	ATTACK
1	Application layer	Repudiation, data corruption
2	Transport layer	Session hijacking, SYN flooding
3	Network layer	Wormhole, blackhole, Identity Spoofing , Sybil Attack
4	Data link layer	Traffic analysis & monitoring, disruption MAC (802.11), WEP Weakness
5	Physical layer	Jamming, eavesdropping

Sybil attack with types

Lightweight sybil attack technique is termed as lightweight as it does not use any extra hardware or antennae for its implementation. It is used to detect Sybil Attacks [12].

It includes:

1) Sybil nodes: There are two types of Sybil nodes. In first type it simultaneously use many identities at a time either by spoofing others identities or by creating its own identities. In second type it uses one identity at a time.

2) Maximum value: In this authors supposed that normal nodes do not have speed greater than 10m/s. The nodes whose speed is greater than 10m/s are detected as Sybil nodes.

3) RSS: In this RSS (Received Signal Strength) upper bound threshold value is calculated. The upper bound value is calculated as average of RSS value when nodes are moving at 10m/s speed. When new node enters in a network then its RSS value is compared with RSS upper bound value, if it is greater or equal to upper bound RSS value then it is detected as Sybil node.

Types of sybil attack [10]

1. **Misbehavior detection**: A Sybil node increases the reputation, credit, trust value by using its virtual identities. Thus the accuracy to detect a malicious node is reduced.

2. **Distributed storage**: It is based on replication and fragmentation mechanism. Data will be stored on Sybil identities and the Sybil attack affects the architecture where it replicates the data on numerous nodes.

3. **Data aggregation**: By sybil attack one malicious node may able to alter the reading. Some sensor network protocols aggregate the reading of sensors in order to conserve energy rather than returning individual readings.

4. **Routing**: In routing mechanism, one node will be present in various paths and different locations at the same time. The nodes are supposed to be disjoint is affected by Sybil identities. [18]

5. **Fare resource allocation**: Since the Sybil node has multiple identities it affects the allocation of resources. Many identities can obtain an unfair share of resources thus reducing the actual share of legitimate nodes.

6. **Voting**: Sybil attack may be particularly dangerous in case of any situation where there is a voting scheme in place for purposes such as recording and identifying node misbehavior in the system, updating reputation scores and so on. Most of the decisions are made by voting. Since the Sybil node has many identities, a single node has a chance of voting many times thus destructing the process. [17]

Study of techniques to prevent sybil attack

In this paper different techniques have analyzed that are used to defend, detect and cure Sybil attack [15]. Different methods to deal with Sybil attack are based on following techniques:

- Based on Registration
- Based on Key pre-distribution
- Based on Location Privacy
- Based on signal strength

1*) Based on Registration*

A difference between peer-to-peer networks and adhoc networks is that in adhoc networks, there may be a trusted central authority managing the network, and thus knowing deployed nodes. One of the methods to prevent the Sybil attack is to achieve identity registration. To detect Sybil attacks, an entity could poll the network and compare the results to the known deployment. The central authority may also be able to broadcast that information securely to the network [18]. To prevent the Sybil attack, any node could check the list of "known-good'' identities to validate another node as legitimate. Registration is likely to be a good initial defense in many scenarios, with the following drawbacks. The list of known identities must be protected from being maliciously modified.

2) *Based on Key pre-distribution*

In this technique, Node-to-node secrecy is ensured by using the common keys as a shared secret session key. The main ideas are the association of the identity with the key assigned to a node and the validation of the key. Validation involves ensuring that the network is able to validate the keys that an identity might have. In random key predistribution, a set of keys are assigned in arbitrary fashion to a node enabling it to discover or compute the common keys that it shares with its neighbouring nodes. This technique enables nodes on an adhoc network to establish secure links for communicating with each other [2].

3) *Based on Location privacy*

It is a particular type of information privacy. In Location based detection techniques it is always hard to know exact location of nodes and if location cannot be found precisely, these techniques can put only a bound on number of Sybil identities attacker can generate. According to [16], location privacy is defined as the ability to prevent other unauthorized parties from learning one's current or past location. In this technique, there are conceivably two types of location privacy personal subscriber level privacy and corporate enterprise-level privacy. Personal subscriber-level privacy must supply rights and options to individuals to control when, why, and how their location is used by an application. With personal subscriber level privacy, each individual has liberties to "opt in" and "opt out" of services that take advantage of their mobile location.

4*) Based on signal strength*

The signal strength based defense is breakable with custom radio hardware and validation may be expensive in terms of energy. Signal strength of sensor nodes depends on a number of factors and can be affected very easily. In [6], a method for Sybil detection based on the Received Signal Strength Indicator (RSSI) of messages is introduced. The cooperation of one additional node (and hence one message communication) is required for the proper functioning of this protocol. A localization algorithm is used in this scheme Sybil attacks can be detected with a completeness of 100% with few false positive alerts.

Conclusion

There are a variety of attacks that pivot on the issue of identity. Mobile Adhoc Networks suffer from different types of attacks and Sybil attack is one among these attacks on network layer. In this paper, the important kinds of Sybil attacks that can be launched on various application domains have been discussed and also listed notable methods that have been proposed over time to tackle these attacks. This paper presents an overview of work related to analyzing or solving the Sybil attack, in which one entity appears as many different identities. A number of existing methodologies for the detection of Sybil attack have been studied.

References

I. Chlamtac, M. Conti, and J. J.-N. Liu, “Mobile Ad hoc Networking: Imperatives and Challenges”, Ad Hoc Networks, vol. 1, pp. 13-64, 2003.

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.

B. Parno and A. Perrig, “Challenges in securing vehicular networks”, Workshop on Hot Topics in Networks (HotNets-IV), 2005.

C. Piro, C. Shields, and B. N. Levine, “Detecting the Sybil attack in mobile ad hoc networks”, in ProcSecurecomm Workshops, pp.1–11,2006.

H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman, “SybilGuard: defending against Sybil attacks via social networks”, presented at SIGCOMM '06: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications, 2006.

Murat Demirbas, Youngwhan Song, “An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks”, In Proceedings of WoWMoM 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2006. 5 pp. – 570.

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.

V. Frias-Martinez, S. J. Stolfo, and A. D. Keromytis, “BARTER: Behavior Profile Exchange for Behavior-Based Admission and Access Control in MANETs”, presented at the Proceedings of the 5th International Conference on Information Systems Security, Kolkata, India, 2009.

SaroshHashmi, John Brooke, “Towards Sybil Resistant Authentication in Mobile Ad-hoc Networks”, Fourth International Conference on Emerging Security Information,System and Technologies, pp.17-24, 2010.

Weichao Wang, Di Pu and Alex Wyglinski, “Detecting Sybil Nodes in Wireless Networks with Physical Layer Network Coding”, IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), 2010.

Sohail Abbas,Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat Presented “Lightweight Sybil Attack Detection in MANETs”. IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013

Sohail Abbas, MadjidMerabti, David Llewellyn-Jones, and KasifKhifayat, “Lightweight Sybil Attack in MANETs”, IEEE System Journal , Vol.7, No.2, pp.236-248, June 2013.

Roopaligarg andHimika Sharma, “Comparison between Sybil Attack Detection Technique: Lightweight and Robust”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol.3, issue.2, pp.7142-7147, February, 2014.

Roopali Garg, Himika Sharma, “Proposed Lightweight Sybil Attack Detection Technique in MANET”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 5, May 2014.

Rathee, malhotra, “Preventing Sybil Attack in Wireless Sensor Networks”, IJIRST International Journal for Innovative Research in Science & Technology| Volume 1 | Issue 12 | May 2015 ISSN 2349-6010.

A. Kumar Tyagi and N. Sreenath, “Location Privacy Preserving Techniques for Location Based Services over road networks”, ICCSP, ISBN: 978-1-4799-8080-2, India, (2015) April 2-4, pp. 1319-1326.

Sangeeta Bhatti, Prof Meenakshi Sharma, "A Review of Sybil Attack in Mobile Ad-hoc Network", International Journal of Advance Foundation And Research In Science & Engineering (IJAFRSE) Volume 1, Special Issue , ICCICT 2015. Impact Factor: 1.036, Science Central Value: 26.54.

S.Sharmila1 , G Umamaheswari, "DETECTION OF SYBIL ATTACK IN MOBILE WIRELESS SENSOR NETWORKS", [IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY Volume-2, Issue-2, 256 – 262.

S.Abbas, M.Merabti, and D.Llewellyn-Jones, "Signal Strength Based Sybil Attack Detection in Wireless Ad hoc Networks", School of Computing and Mathematical Sciences Liverpool John Moores University Byrom St. Liverpool, L3 3AF, UK.