Prevention Techniques against Sybil Attacks in MANETS: A Literature Survey

[1]Bindu Chaurasiya, [2]Mohit Shrivastav, [3]Devendra Kumar
[1.3]M.Tech. , [2]Assistant Professor
[1]CSE Department,
[1]School of Engg. & IT, MATS University, Gullu-Aarang Campus, Raipur (C.G.), INDIA

***Abstract* - Security is a major aspect of concern in any kind of Ad-hoc networks. In Mobile ADHOC Networks (MANETs), mobility among nodes creates difficulty for securing and support of conveniences. That's the main reason which makes such wireless networks vulnerable to various kinds of attacks. One of the attacks is Sybil Attack which leads to decrease in performance of network in terms of delivery ratio, end-to-end delay, normalized routing load etc. Sybil attacker creates multiple fake identities to misguide the network or system. In this survey paper, it is tried to summarize the previous prevention techniques against this attack and concluded with respective techniques performance.**

***Index Terms* - Mobile Ad hoc Networks, Sybil Attack, Received Signal Strength .**

I. INTRODUCTION

MANETs has some salient features such as self-organized, forms dynamic topology, unfixed infrastructure etc. The wireless communication is established among nodes via hop-by-hop communication in MANETs. But the malicious nodes may violate this one-to-one mapping of identity of the network. Sybil attack is an attack which uses multiple identities at a time and increases lot of misjudgments among the nodes of a network. Sybil attacker node may use identity of other legitimate nodes present in the network and creates false expression of that node in the network and disturbs the transmission of packets among the nodes of the network. it is necessary to eliminate the Sybil nodes from the network to have secure communication **[1].** To detect such kind of attack the following goals must be fulfilled by every security algorithm as suggested by author in **[2]:**

1. **Authentication**: Each and every node, participating in communication must be genuine and legitimate node. Authentications among nodes ensures about surety of data packet transmission while communicating with each other.
2. **Availability:** All services should be available all the time to all the nodes for the proper functioning and security of the network. This ensures that all services would be delivered by nodes on time accurately.
3. **Integrity:** It gives the assurance that the data received by the receiver will be same as the data send by the sender. This ensures data has been received by the receiver node is same as sent by the sender.
4. **Confidentiality**: It means that some data is only accessible by the authorized users. It ensures that messages can be delivered to desired destined nodes in un-modified form.
5. **Non-repudiation**: It means sender and receiver cannot deny that they didn't send or receive the data. It ensures about matching of messages between sender and receiver nodes.

Sybil attack was first introduced by J. R. Douceur **[3]**. According to him, the Sybil attack is an attack in which a single entity can control a substantial fraction of the system by presenting multiple identities.

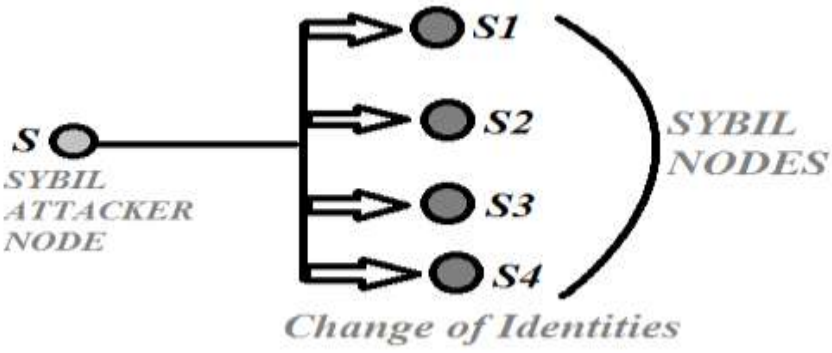

Fig. 1: A Sybil attacker node with change of identities

Fig.1 represents a Sybil attacker node S along with its four Sybil nodes (S1, S2, S3 and S4). Actually the Sybil nodes are the fake identities created by the attacker node. Whenever the Sybil attacker node communicates with any valid node by presenting all its Sybil identities, the valid node will have illusion that it has communicated with five different nodes. While in reality, there exists only one physical node with multiple different IDs.

II. LITERATURE SURVEY

A Levine et al. **[4]** surveyed countermeasures against Sybil attacks and categorized these techniques as follows.

Trusted Certification: In this technique a central authority is employed to bind a network into single identity certificate. This technique is considered to be good defending solution against Sybil attacks for establishing a Sybil-free domain of identities. However such technique is much more effective but it has some drawbacks also like costly initial setup, central authority failure and lack of scalability or may create bottleneck in large scale systems.

Resource Testing: This technique is discussed by H. Liming **[5]**, where to check node's computational ability, storage ability and network bandwidth. In this technique different kind of tasks are distributed among all nodes of the networks to settle on which independent node has sufficient resource to accomplish the tasks. A Sybil attacker node doesn't have additional tests imposed to its Sybil nodes and hence it would be detected.

Trusted Devices: This technique is totally dependent on hardware devices such as a network card bounded as a single network entity. But this technique doesn't guarantee against Sybil attack when an attacker node may use multiple network cards.

Use Mobility of Nodes: Capkun et al. **[6]** discussed this technique. This approach is based on the fact that all individual nodes are free to move independently so all the Sybil nodes must be bound to single physical node and move together. At such conditions, mobility of nodes in a wireless network can be useful to detect and identify at which portion of the network Sybil attack has occurred.

Reputation Based Schemes: Abbas, M. Merabti et al. **[7]** discussed this technique. Basically this technique is used to detect Whitewashing attack. In this approach, a selfish node can easily escape the consequences of whatever misbehavior it has performed by simply changing identity to clear all its bad history, known as whitewashing [7].

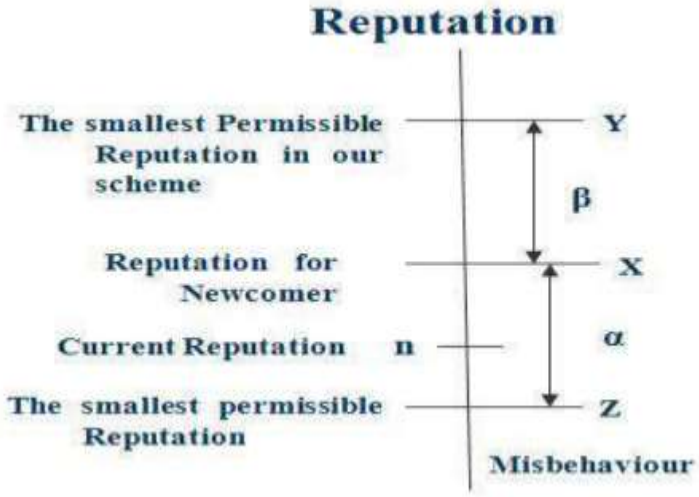

Fig. 2: (Re-produced) Reputation Level [7]

In fig.2 shows the smallest permissible reputation Z be greater than the node's initial eputation X by the amount β; also denote this modified smallest permissible reputation by Y (instead of Z) [7]. In this scheme the threshold Y, the amount of reputation β and the fee threshold are referred to be the same thing. There will always be a loss to change its identity after gaining Y [7]. Here there will always be an amount β of loss to reputation or the fee that has been paid, after a node changes its identity. Fee imposition makes whitewashing costly (in terms of battery power) for an attacker, the same is the case with Sybil attackers; hence an attacker can perform fewer whitewashes or identities with its battery [7].

Recurring Cost and Fees approach: B. N. Levine et al**.[4]** discussed this technique. This approach is a variation of the normal resource testing, and can limit the number of Sybil nodes an attacker, with constrained resources, can introduce in a period of time. This technique is time consuming and less efficient. This model charges the entry fee for every node participating in the network. And charging a recurring fee for each additional participating identity is much more costly and hence deterrent against Sybil attacker node.

RSS based Localization Technique: Yingying Chen et al. **[9]** discussed this technique. This technique is based on the shared nature of wireless nodes which utilizes the physical properties information with their transmission. Sybil attack detection is performed by measuring received signal strength (RSS) value across a set of landmarks (i.e. reference point with known locations) followed by K-means clustering algorithm. The test statics observed will be large indicating without Sybil attack and will be small indicating with Sybil attack.

RSS based analysis: Mohamed Salah Bouassida et al**. [10]** discussed this technique for VANET environment. Geometrical based analysis is evaluated using received signal strength variations of nodes that an attacker node should not increase its sending power. Then a distinguish-ability degree is obtained that how much a pair of nodes could be distinguished from each other. This mechanism can be launched individually by every node in the network in order to detect Sybil and malicious ones based on their geographical localizations.

Sohail Abbas et al. **[7]** discussed enquiry based received signal strength technique where each node collects information about the RSS value of neighboring nodes. Based on RSS value , nodes can be distinguishes whether a node is legitimate node or Sybil

node. The RSS value low indicates that node is legitimate node and RSS value high indicates that node is Sybil node. This method keeps information in the form (Address, rss-list, time).
Following table 1 shows the comparative study of Sybil attack detection techniques with their limitations and dis-advantages.

S.No.	Sybil Attack Prevention Techniques	Limitations/Disadvantages
1	Trusted Certification	Expensive, single point of failure may happen and performance overhead
2	Resource Testing	In-effective for larger systems/ networks
3	Trusted Devices	No way of preventing an entity from obtaining multiple devices.
4	Use of Mobility of Nodes	All the nodes must move together
5	Reputation based Schemes	Possibility of selfish node to increase their trust value.
6	Recurring cost and Fee approach	Requires the use of electronic cash or of significant human effort, time-consuming
7	RSS based localization Technique	Geographical localizations needed to verify the authenticity of another nodes
8	RSS based analysis	Does not deal with existing Sybil nodes in the network, Location calculations are costly,

Table 1: Summary of Existing Mechanisms to detect Sybil Attack.

III. CONCLUSION

MANETs is very flexible kind of network due to which it suffers from different types of attacks. Sybil attack is one of the harmful attacks for such networks which work on Network Layer. Sybil attacker node creates multiple identities and thereby decreases the performance of network in terms of higher packer drop, decrease in throughput, higher delay etc. In this paper a survey of different kind of mechanisms to defend against Sybil attack is presented and concluded with each technique with its limitations and disadvantages.

REFERENCES

[1] Adnan Nadeem and Michael P. Howarth,``A survey of MANET Intrusion Detection & Prevention Approaches for Network layer Attacks," IEEE Communication Surveys & Tutorials, pp.1-19, 2012.
[2] LoayAbusalah, AshfaqKhokar, and Mohsen Guizani,``A Survey of Secure Mobile Ad Hoc Routing Protocols," IEEE Communication Surveys & Tutorials, Vol.10, No.4, pp.78-93, 2008.
[3] Brian Neil Levine, Clay Shields, N. Boris Margolin," A Survey of Solutions to the Sybil Attack," Dept. of Computer Science, Univ. of Massachusetts, Amherst Dept. of Computer Science, Georgetown University.
[4] B. N. Levine, C. Shields, and N. B. Margolin, 2006 „A survey of solutions to the Sybil attack", Univ. Mass. Amherst, Amherst, Tech. Rep. 2006-052.
[5] H. Liming, L. Xiehua, Y. Shutang, and L. Songnian, "Fast authentication public key infrastructure for mobile ad hoc networks based on trusted computing," in Proc. Int. Conf. WiCOM, 2006, pp. 1–4.
[6] S. Capkun, J. P. Hubaux, and L. Buttyan, "Mobility helps peer-to-peer security," IEEE Trans. Mobile Comput., vol. 5, no. 1, pp. 43–51, Jan. 2006.
[7] Abbas, M. Merabti, and D. Llewellyn-Jones, 2010 „Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks," in Proc. WD IFIP, pp. 1–6.
[8] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat, Lightweight Sybil Attack Detection in MANETs IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013.
[9] Yingying Chen, Member, IEEE, Jie Yang, Student Member, IEEE, Wade Trappe, Member, IEEE, and Richard P. Martin, Member, IEEE, 2010 „ Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks", IEEE Transactions ON Vehicular Technology, VOL. 59, NO. 5.
[10] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, 2009 „Sybil Nodes Detection Based on Received Signal Strength Variations within VANET", International Journal of Network Security, Vol.9, No.1, PP.2233.
[11] Douceur J.R. (Mar. 2002): 'The Sybil attack', In Proceedings for the First International Workshop on Peer-to-Peer systems (IPTPS'02), ser. LNCS, vol.2429. Cambridge, MA, USA: Springer, pp. 251– 260.
[12] Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks, Communications of the. ACM 47(6) (2004) pp. 53–57.
[13] Newsome, J., Shi, E., Song, D., Perrig, A., The Sybil attack in sensor networks:analysis & defences, In Proc. IPSN International Symposium(2004) pp. 259–268.
[14] Newsome J., Shi E., Song D., and Perrig. A (2004): 'The Sybil attack in sensor networks: analysis & defences', In Proceedings of the third international symposium on Information processing in sensor networks, pp. 259–268.
[15] 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.