International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
*ISSN (Online)*2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP339-344

Survey Of Sybil Attack In Wireless Networking

Chandrakant A. Gawande[1],Nikhil Darade[2]
Vipula Ghodke[3], Devashree Gawande[4]
[1 2](Computer Engg.Dept.,Dr. D. Y. PatilInsti.Of Engg.And Tech.,SavitribaiPhule Pune University,India)
[3](E&TC Engg. Dept.,MKSSS's Cummins College Of Engg. For Women,Savitribai Phule Pune University,India)
[4](E&TC Engg.Dept.,Dr.Babasaheb Ambedkar Technological University,Lonere, India)

Abstract :- The task to achieve security in Mobile ad hoc networks (MANETs) is quite challenging. The opennature, central management, high mobility of nodes and lack of infrastructure.Wireless networksare highly susceptible to various types of attack.Sybil attack is the main attack, which allows for forming other attacks on the Wireless Network. Hence the current research is being done on tackling security of transmission powerand traffic levels.

Keywords:-Defense, Illegal Identities, Security,Sybil Attack.

I. INTRODUCTION

Wireless Sensor Network(WSN) comprises of large numbers of nodes, they can communicate with each other and to base station. Every node contains an electronic circuit, microcontroller for interfacing with battery and sensors, external memory and a radio transceiver. WSN is being used for various applications such as healthcare monitoring, air monitoring and monitoring the combat zone for various security purposes. In WSN, an intruder easily tends to attack the low physical protection and communication of sensor nodes due to its broadcast nature.These characteristics WSN poses challenges and opportunities both in getting the security goals, as validating genuineness, availability, integrity, non-repudiation, confidentiality, and access control. There are vast varieties of attacks which targets the weak of WSN routing protocols.

Most sophisticated and subtle routing attacks have been identified in some recently published papers such as a Sybil attack [5], Byzantine [4], wormhole [7], Black hole [4] and Rushing [8] etc. A Sybil attack is an attack [8] in which a malicious node illegally claims multiple identities by impersonating other nodes or by claiming fictitious identities. Sybil attacks are also capable of destroying routing mechanisms. In case of multi-path routing, there are chances of supposedly disjoint paths might be passing through various Sybil identities of a single malicious node. A legitimate node may choose any of the Sybil nodes while forwarding the packets on the basis of the closest location to the destination node; but in reality it will be passing the packets through the malicious node.

The rest of this paper in organized in the following way: Section 2,represents the literatureresview on Sybil Attacks in WSN. Section 3, represents the Survey In Tabular form . In section 4, represent our conclusions and suggestions for future research.

II .SPECIFIC TYPES OF SYBIL ATTACKS

There are various malevolent applications of Sybil attacks in several environments such as those among, but not limited, the variations enlisted below.

2.1Equitable Resource Allocation

Sybil attacks can also be used by attacker to achieve an illegal access and disproportionately exploit large part of resources, which were intended to be served amongst all other nodes on the network impartially. This attack refuses originalnodes, which deserve the share of resources. And also provides the illegal node with more scope for other attacks.

2.2Routing

Sybil attacks can destroy routing protocols in ad hoc networks, especially in the mechanism of multicast routing. The separate paths that were initially seem to be disjoint may pass through the Sybil nodes of a just single attacker. In another defenseless concept where malicious nodes may appear inmany places at a time is Geographical Routing [12].

2.3Tampering with Reputation and Voting Systems

A Sybil attack may be very dangerous where voting schemes are used. For example, an intruder may create enough illegal identities to continuously report and consequently remove legitimate nodes from the network. Unfortunately, these illegal nodes can protect themselves from ever being removed as since they are in collision.

2.4 Data Aggregation

To save energy readings of Sensor Network are calculated by query protocols in a network itself rather than returning the reading of every single individual sensor. Sybil identities may report incorrect sensor readings thereby disrupting the complete calculated aggregate. Alteration by an intruder might be done with numbers of identities.

2.5 Distributed Storage

File storage systems having WSN and peer-to-peer implementation, might have to compromise by the Sybil attack. This could be done by fragmentation and replication processes in the file system. A system can be swindled into storing data in the multiple Sybil identities of the particular node on the network.

III. METHODS PROPOSED TO COUNTER SYBIL ATTACKS

Though there is no general, universally-accepted solution to the Sybil attack, a number of approaches for various combinations of environments and attacks have been proposed. Some methods to mitigate the threat level of these attacks in a system to a satisfactory minimum without incurring an appreciable performance overhead. |One must note that although they won't completely eliminate the possibility of the attack occurring, they are more than worthy of consideration.Notable techniques for countering Sybil Attacks are as under:-

3.1Random Key Predistribution

This method helps the node on WSN for establishing protected links for communicating between themselves. [2]. In this, a set of identitiesis given at random to a node, making it to discover or calculate the common identities that it shares withits neighboring nodes. Node-to-node concealment is guaranteed by the common keys as a shared conceal session key. The major ideas are the relationship of the identity with the key given to a node and the validation of the key. Validation involves assuring that the network is able to validate the given identity that a node might have. The fake Sybil identity will not pass the key validation test as the identities associated with a random identity will, most likely, not have an appreciable intersection with the indulged key set.

3.2 Privilege Attenuation

In [13], Fong describes a different kind of Sybil attack – one that is completely different from those that plague peer-to-peer and reputation systems. It focuses on creating pseudonymous identities in a Social Networking System (SNS) and compile them to collude favorably altering the present trusted relationships in the network. These associations arerepresented through a graph-theoretic relationship model which exists in between of a resource owner and am expected accessory of that resource and is known as social graph. Such models are common in quite a few popular Social Network Systems such as Facebook. Access control policies are defined by the respective SNSs themselves. This Concept of Relationship-Based Access Control (ReBARC) [15, 16, 17, 18] is the basis for authorization decisions in the system.

When the false identities or inauthentic accounts in the SNS collude, they can gain the rights to access restricted, sensitive and personal information of the user[17].To overcome this danger, Mr. Fong have proposed a particular type of Denning's Principle of Privilege Attenuation or POPA which is sufficient and important to foil such attacks, with a static policy analysis for verifying POPA compliance [13].

3.3 Incentive-based Detection

Margolin and Levine proposes a protocol in [18] called Informant which is based on an economic incentive policy and is a general answer that is not specific with respect to any particular application domain. An entity (known as detective) rewards Sybil for revealing themselves. An identity gives the name of the target node and a security deposit to the detective while the target peer receives the deposit and a certain reward. An example, the Dutch auction is used to establish the minimum reward that will reveal a Sybil node. No physical tokens are necessary, unlike other Sybil detection methods [18].

3.4 RSSI-based scheme

In [19], Demirbas and Song recommended a technique for Sybil Identification which rely on the RSSI i.e. Received Signal Strength Indicator of messages. One additional node is required for the proper working of this protocol. A localizationalgorithm is used with this scheme. Sybil attacks can be identified with a 100% completeness beside a few false positive alerts. Though we know that the RSSI is unreliable and also the transmissions via radio are non-isotropic, the use of ratios of RSSIs from multiple receivers can solve this problem.

3.5 Recurring Costs

In this resource are tests after a specific time interval to impose some "cost" on the intruder to expose for every identity that is being controlled in the network.

However, those researchers who have adopted this method are using computational power in their resource tests. This in itself may be insufficient in tackling the attack since a malicious user liable only a one-time cost (for computing resources) that may be recovered via the execution of the attack itself, as pointed out by Levine et al in [20].

3.6 Resource Testing

Resource Testing is the most commonly implemented solution to averting Sybil attacks. The basic principle is that the quantum of computing resources of each entity on the network is limited. A verifier then verifies whether each identity has as many resources as the single physical device it is associated with. Any inconsistency indicates the possibility of a compromised node. Storage, computation and communication were initially proposed as resources.For a network such as a WSN, there are chances of having storage and computing resources in large capacities compared to resource-starved sensor nodes with an intruder. Alternatively, verification messages for crosschecking communication resources might flood the entire system itself. Hence, all three are inadequate choices for sensor networks.

Radio resource testing, proposed by Newsome et al in [6], is an extension of the resource testing verification method for wireless sensor networks. The main assumptions of this approach are that any physical device has only one radio and that this radio.is incapable of transmitting and receiving messages on more than one channel at any given time.

Resource trialshave been suggested by many for a minimal defense against Sybil attacks where the goal is to reduce their risk substantially rather than to eliminate it altogether.

3.7 Location / Position Verification

This solution is specific to Wireless ad hoc Networks. Methods employing this technique make use of the fact that any identities that are projected by any single physical device must be in the same location. Locations are verified using specific methods such as triangulation [23]. So for an attacker with a single physical device, all Sybil identities will be in the same place or will appear to move together.

Tangpong et al. have proposed a solution in [24] based on the above strategy

3.8Trusted Certification

Certification is by far the most frequently cited solution to defeating Sybil attacks [5]. It involves the presence of a trusted certifying authority (CA) that validates the one is to one correspondence between an entity on the network and its associated identity. This centralised CA thus eliminates the problem of establishing a trust relationship between two. communicating nodes. Douceur has proven that such kind of certification is the only method that may potentially eliminate Sybil attacks completely [1]. Although this approach intuitively seems like the ideal method to tackle these attacks, there are a number of implementation issues specifically about how the CA shall establish the entity-identity mapping. In real-world applications this may incur an appreciable performance cost particularly if performedmanuallyonlargescalesystems.

TABLE 1: Various approaches to detect Sybil attacks in different application domains,their advantages and their limitations

S. No.	Technique to mitigate Sybil attack	Advantages	Disadvantages / Limitations	Application Domain
1	Random Keys Predistribution	Node-to-Node concealment is guaranteed	Limited to Sensor Networks [2]	Sensor Networks
2	Privilege Attenuation	An access control policy specifies a graph-theoretic relationship between the resource owner and resource accessor	Applies only to network having invariable policies. Significant run-time and storage overhead for generalized extensions of the idea [11]	Social Network Systems
3	Economic Incentives	Applicable to all Domains	May encourage Sybil attackers that have no interest in overturning the application protocols, but they are interested in being paid to reveal their presence [9]	General
4	Received Signal Strength Indicator (RSSI) – based scheme	Sybil attacks can be identified with a 100% completeness	Does not deal with existing Sybil nodes in the network, Positions based calculations are always expensive, Finite to Sensor's Networks only	Sensor Networks
5	Recurring Costs	Only one-time cost to recover a malicious user	Requires the use of electronic cash amount or of significant human effort [6]	General
6	Testing Resources	Reduces the risk of Sybil attack substantially	Incompetent for most systems [1][3]	General
7	Location or Position Verification	Ease in implementation	Limited only to ad hoc networks	Wireless ad hoc networks

8	Trusted Certification	Eliminates Sybil attack completely	Notable performance overhead and expense [1][2]	General

IV.CONCLUSION

In this paper, we have surveyed the main typesof Sybil attacks that might be done on various Wireless Sensor Network. We have also enlist notable methods that have been proposed over time to tackle these attacks. Further, we have elaborated on their profile suspects, advantages, and limitations.

After surveying these papers we feel that still there is a wide scope for reseach in Sybil Attack Detection.

V.REFERENCES

[1] Mr. Suresh N, Mrs. Madhuri T,*"Smart Duo Approach - Detection and Removal of Sybilattackers in MANETs by Clump based Scheme", IJIRCCE/Vol.2,Isssue 4, April 2014*

[2] Mr. J. Newsome, E. Shi, D. Song, and A. Perr,*" The Sybil attack in sensor networks: analysis &defence"s, In Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268, 2004*

[3] HimadriNathSaha, Dr. DebikaBhattacharyya,Dr. P. K.Banerjee, Arnab Banerjee, DipayanBose,"Study of Different Attacks In MANETs With Its Detection And Mitigation Schemes", *IJAET/Vol.III/ Issue I/January-March, 2012/383-388*

[4] B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, "An On-demand SecureRouting Protocol Resilient to Byzantine Failures",*Proceedings of the ACM Workshop on Wireless Security, pp. 21-30,2002*

[5] AmolVasudeva, Manu Sood,"Sybil Attack On Lowest Id Clustering Algorithm in the Mobile Ad Hoc Network",*International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012*

[6] Kayalvizhi, N. Senthilkumar, G. Arulkumaran,*"Detecting Sybil Attack by Using Received SignalStrength in Manet"s*",*IJIRSE-ISSN (Online) 2347-3207*

[7] E. M. Royer and C. E. Perkins, *(1999), "Multicast Operation of Ad Hoc On Demand Distance Vector Routing Protocol", In Proceedings of ACM MOBICOM, pp. 207-18.*

[8] J. R Douceur, *(2002), "The Sybil Attack", IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251–260, Springer Verlag, London, UK.*

[9] M. Demirbas and Y. W. Song, *(2006), "An RSSI-Based Scheme for Sybil Attack Detection inWireless Sensor Networks", International Workshop on Wireless Mobile Multimedia(WOWMOM'06), New York, USA., pp. 564–570.*

[10] E. M. Royer and C. -K. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks",*IEEE Personal Communications,(1999)*

[11] Y. Hu, A. Perrig and D. Johnson, "Packet Leashes: A Defense against Wormhole*",2002*

[12] "Attacks in Wireless Ad Hoc Networks", *Proc. of IEEE Infocom.*

[13] Chris Piro, Clay Shields, Brian Neil Levine,Dept. of Computer Science Georgetown Univ,"Detecting the Sybil Attack in Mobile Ad hoc Networks"

[14] P.W. L. Fong. Preventing,"Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems"*In IEEE Symposium on Security & Privacy, 2011 pp. 263-278.*

[15] C. E. Gates,"Access control requirements for Web 2.0 security and privacy",*in IEEE Web 2.0 privacy and security workshop (W2SP'07), Oakland, California, USA, May 2007*

[16] B. Carminati and E. Ferrari," Enforcing relationships privacy through collaborative access control in web-based social networks", *In Proceedings of the 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing CollaborateCom'09), Washington DC, USA, Nov. 2009 pp. 1-9, 2009*

[17] P. W. L. Fong," Relationship-based access control: protection model and policy language",*In Proceedingsof theFirst ACM Conference on Data and Application Security and Privacy (CODASPY'11), San Antonio, TX, USA, Feb. 2011, pp. 191–202.*

[18] P. W. L. Fong and I. Siahaan,"Relationship-based access control policies and their policy languages",*in Proceedings of the 16th ACM Symposium on Access Control Models and Technologies (SACMAT'11), Innsbruck, Austria, Jun. 2011 pp. 51-60*

[19] 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*

[20] B. N. Levine, C. Shields, and N. B. Margolin,"A survey of solutions to the Sybil Attack", *University of Massachusetts Amherst, Amherst, MA, 2006*

[21] Hurson, A., "Robust Sybil Detection for MANET's", *In Proceedings of 18th International Conference on Computer Communications and Networks,2009. ICCCN 2009, pp. 1 – 6*

[22] Margolin, N. Boris, and Levine, Brian Neil, "Informant: Detecting Sybils using incentives", *In Proceedings of Financial Cryptography (FC) (February 2007) pp. 192—207*

[23] AthichartTangpong, "Managing Sybil Identities in Distributed Systems", *Ph.D. Thesis at the Pennsylvania State University, May 2010*

[24] Tangpong A. , Kesidis G. , Hung-yuan Hsu, HursonA.., "Robust Sybil Detection for MANETs", *In Proceedings of 18th International Conference on Computer Communications and Networks, 2009. ICCCN 2009, pp. 1 – 6*