INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue1)
Available online at: www.ijariit.com

Sybil Attack in Wireless Sensor Networks: A Survey

Mandeep Kaur
CSE Department
Bhai Gurdas Institute of Engg. & Tech
contactmgrewal@gmail.com

Mr. Avinash Jethi
Asst Professor
CSE Department
Bhai Gurdas Institute of Engg. & Tech

Abstract: The wireless sensor networks are prone to various attacks; this is primarily due to the fact that these networks once deployed are left unattended. So any attacker with the intention of stealing the information from the network can compromise any node and gain access to the data being propagated in the network. Various attacks possible are black hole attack, wormhole attack, Sybil attack, clone attack etc. This paper represents the various techniques that have been presented in the past for the detection and prevention of the Sybil attack.
Keywords—Sybil attack, unattended, wormhole.

I. INTRODUCTION

Wireless Sensor Network is a platform for a variety of application areas in such as environmental monitoring and homeland security domains. So it attracts many researchers to work on various problems related to WSN. The coverage, connectivity and energy related issues are very important in WSNs. More attacks are possible in WSN as compared to wired network. In applications like military, without security, the use of Wireless Sensor Network is any application would result in disastrous consequences. Security allows Wireless Sensor Networks to be used to maintain integrity of data and availability of all messages in the presence of resourceful adversaries. The main objective of confidentiality and authenticity is expected in sensor networks to safe guard the information traveling among the nodes of the network or between the sensor nodes and the sink node from disclosure. The WSNs are comprised of a group of nodes for scalar or multidimensional data gathering. Sensor nodes are employed to collect the information, compress and process it for storage purpose and to transmit the processed data to a sink such as an intermediate cluster head or a base station. The transmitted information is then presented to the system by base station connection. Traditional security goals for an ad-hoc network and specific to the WSN security goals can be classifies in two categories as primary and secondary. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self-Organization, Time Synchronization and Secure Localization [11].

Sybil Attacks

In a Sybil attack a node presents multiple identities to the rest of the nodes. Sybil attacks are a threat to geographical routing protocols, since they require the exchange of coordinates for efficient packet routing. Ideally, a node only sends a set of coordinates, but under a Sybil attack, an adversary could pretend to be in many places at once.

II. EXISTING WORK

Manjunatha et al. [1] recommended that system confirms the physical position of every node. Sybil nodes can be identified utilizing this methodology since they will seem, by all accounts, to be at precisely the same position as the malicious node that creates them. By setting a point of confinement on the thickness of the system, in-district check can be utilized to firmly tie the quantity of Sybil characters that a pernicious node can make.

Zeng et al. [2] proposed a novel convention to restrict the impact of Sybil attacks by consolidating ant colony optimization (ACO) calculation, where a node does arbitrary strolls and it will take off trails on the way. Be that as it may, with the irregular work, the trails of the primary node left on every node get to be weakened, toward the end of directing it just blurs away. In view of the way of the ACO and limit the quantity of attack edge in a productively and helpfully. Consequently, framework can guarantee a legit

© 2017, IJARIIT All Rights Reserved

node would acknowledge and be acknowledged by other fair nodes in framework with high likelihood, likewise, dismiss Sybil nodes with extraordinary likelihood.

Amuthavalli et al. [3] proposed a calculation to distinguish Sybil nodes in WSN called Random Password Comparison [RPC]. This calculation sends and controls the position of node in this way keeping the Sybil attack. The RPC strategy is changing and precise in distinguishing the Sybil attack. This technique enhances information transmission in the system and will likewise build the throughput.

Sharmila et al. [4] proposed a calculation to discover a Sybil node in WSN. Their system is partitioned into three stage in first stage they send ID and force quality to the head nodes, the head node checks for nodes with force esteem beneath the limit esteem. In second stage, the separation between the recipients and sender are zero, and afterward the node experiences Sybil attack after that if the nodes are close, then the nodes will be distinguished as Sybil nodes regardless of the possibility that they are definitely not. In third stage, the steering method in the bunch is checked to confirm on the off chance that there was a bounce between the Sybil characters, and if there exists a jump between the Sybil personalities, then the nodes are most certainly not Sybil nodes.

Sheela et al. [5] proposed a calculation to identify clones and any vindictive nodes in remote sensor systems. Their framework has two calculations based on versatile specialist. MARCAD (Mobile Operator based Cloning Attack Detection) is to recognize clones and any noxious nodes. Another is MASAD (Mobile specialist based sinkhole Attack Detection) calculation is to tell how a node employments the worldwide system data to course information parcels by staying away from sinkhole attack.

Rupinder et al. [6] proposed a calculation Mobile Agent Based Clone Attack Detection Algorithm (MACAD). In MACAD calculation, the framework is intended to make each node mindful of area and character of numerous nodes (Say n) so that every neighbor of node A confirms the mark and checks the credibility of Location of A. At the point when a node finds a crash distinctive area claims with the same ID. It shows the two clashing cases as confirmation to repudiate the copies.

Newsome et al. [7] proposed random key pre-distribution, appoint a random arrangement of keys or key-related data to each sensor node, so that in the key set-up stage, every node can find or figure the basic keys it offers with its neighbors; the basic keys will be utilized as a mutual mystery session key to guarantee node-to-node mystery. Those thoughts are: (1). Partner the node personality with the keys allotted to the node. (2) Key acceptance, i.e., the system having the capacity to confirm part.

Karen et al. [8] proposed Key-based authentication. This was broadly considered regarding its storage overhead, computational proficiency and versatility against partial bargain of the system. It has a pleasant property that the measure of overhead can regularly be demonstrated as an element of security versatility. A node may have one and only ace key imparted to everybody, a gathering key imparted to a gathering of nodes, a bunch key imparted to every one of its neighbors, or a pairwise key imparted to each prompt neighbor.

Kamdeo Prasad and Chandrakant Mallick [9] proposed a calculation called Sybil attack Detection Algorithm (SDA) is proposed to identify and keep the Sybil attack in the WSNs. The proposed SDA calculation is rapid and exact in distinguishing the Sybil attack that utilizations Mobile operator, edge esteem, arbitrary key pre-conveyance and irregular secret word area. They are utilizing irregular secret key and limit esteem to recognize and after that for the affirmation of an authentic node and a Sybil node. Besides this calculation helps in transmission of information in a more secured path by staying away from the Sybil attacks. They recreated the proposed calculation in NS2 and checked the throughput and bundle conveyance proportion consequently checked the identification execution of SDA in remote sensor system.

Manjunatha T. N et al., [10] focuses on various security issues, security threats, Sybil attack and various methods to prevent Sybil attack. In this paper, they exhibited the general idea of remote sensor system and security in remote sensor system. The different existing technique for the detection of Sybil attack have been talked about and a calculation is proposed for detection of Sybil attack in remote sensor system. By utilizing that calculation, they discover the Sybil node or not. They have moreover depicted such a variety of attacks that happen in sensor system furthermore apply to sensor node.

Mian Ahmad Jan et al., [14] proposed a received signal strength based scheme to detect the Sybil nodes in wireless sensor networks. In this paper, the authors proposed a lightweight scheme for Sybil attack detection. The proposed scheme requires coordination of any two high energy nodes and performs detection using signal strength of received packets. They have used clustering-based hierarchical architecture to detect forged identities of an adversary. Each node transmits control packets to its two nearest high energy nodes. The control packets contain residual energy and identity of a node. Both high energy nodes calculate signal strength of the received packets and exchange it using a half-duplex communication channel to calculate RSSI ratio. After a certain amount of time, the same operation is performed to calculate a new RSSI ratio using signal strength of received packets from the same node. If the new ratio is equal to the previous ratio and identities of a node in received packets are also different, it means that the node has forged its identities. Each node in the network undergoes a similar operation for identity verification.

CONCLUSION

In this paper, various recent researches regarding Sybil attack has been studied. The authors have used ant colony optimization, received signal strength and various cryptographic algorithms to detect and prevent against such attacks. In future, these algorithms or techniques can be compared or modified algorithm can be proposed and compared against such algorithms.

© 2017, IJARIIT All Rights Reserved

REFERENCES

1. T. N. Manjunatha, M.D. Sushma, K.M. Shivakumar, "Sybil Attack Detection Through On Demand Distance Vector Based Algorithm" In Wireless Sensor Networks, Issue June 2013(JIARM).
2. BinZeng and Benyue Chen, SybilACO, " Ant colony optimization in defending against Sybil attacks" in the wireless Sensor Network, Issue 2010(IEEE).
3. R. Amuthavalli, Dr. R. S. Bhuvaneswaran, "Detection and Prevention of Sybil Attack In Wireless Sensor Network Employing Random Password Comparison Method ", Issue September 2014(JTAIT).
4. S.Sharmila and G Umamaheswari, "Detection Of Sybil Attack In Mobile Wireless Sensor Networks", Issue MarApr 2012(IJESAT).
5. D.Sheela, V.R.Srividhya, Amrithavarshini and J.Jayashubha, "A Mobile Agent Based Security System of Wireless Sensor Networks against Cloning and Sink Hole Attacks", Issues ICCTAI'2012.
6. Rupinder Singh Brar and Harneet Arora," Mobile Agent Security issue in Wireless Sensor Networks ", Issue 1, January 2013(IJARCSSE).
7. James Newsome, Elaine Shi, Dawn Song and Adrian Perrig," The Sybil Attack in Sensor Networks: Analysis & Defenses", Issue 27 April 2004(IPSN).
8. Karen Hsu, Man-Kit Leung and Brian Su, "Security Analysis on Defenses against Sybil Attacks in Wireless Sensor Networks", Issue 2008(IEEE).
9. Kamdeo Prasad and Chandrakant Mallick, "A Mobile Agent based Sybil Attack Detection Algorithm for Wireless Sensor Network" in International Conference on Emergent Trends in Computing and Communication (ETCC 2015).
10. Manjunatha T. N, Sushma M. D, Shivakumar K. M, " Security Concepts and Sybil Attack Detection in Wireless Sensor Networks" in international journal of emerging trends and technology in computer science April 2013.
11. Vikash Kumar, Anshu Jain and P N Barwal, "Wireless Sensor Networks: Security issues Challenges and Solutions**"** in International Journal of Research in Engineering and Technology, November 2014.
12. Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, "A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network" in IEEE Trust Com, Big data SE, ISPA, 2015.

© 2017, IJARIIT All Rights Reserved