Review on the various Sybil Attack Detection Techniques in Wireless Sensor Network

Palak
M-Tech Scholar
Department of Computer
Engineering and Technology,
Guru Nanak Dev University,
Amritsar, Punjab, India

ABSTRACT
The paper signifies that the advancement with Wireless Sensor System (WSNs) have attracted lots of consideration in an area as well as in the learning community. Wireless networking technologies boast several attributes like self-organization, all round flexibility, risk-free transmission as well as future notification. Security is now a significant cover for various mission-critical applications in WSNs. This paper has been focused on that how to shield against a serious attack, the Sybil attack. It has additionally done the comparison of many Sybil attack recognition technique predicated on various guidelines which screen and well-timed detects Sybil attacks in large-scale WSNs. Also another comparison has been done on the basis of the parameters used in each technique.

Keywords
Wireless Sensor Network, Security, Sybil attack detection techniques and Parameters.

1. INTRODUCTION
Individuals are generally continually inventing technologies in order to complete their needs. WSNs really area, however, acquiring engineering consisting of multifunction alarm nodes which might be modest bigger and also converse wirelessly around limited distances. Sensor/probe nodes integrate qualities with regard to feeling the earth, info producing and also communicating with sensors. The unique qualities associated with WSNs boost flexibility minimizing individual contribution in operational chores like battlefields. WSNs can perform a crucial role in most applications, such as patient wellness, keeping track of the environmental remark and also be developing attack surveillance. Sooner or later WSNs can be an important part of the lives.

1.1 Wireless Sensor Network
A wireless sensor system makes up a big variety of sensing component nodes in addition to a platform station. It consists of the sensor nodes, base station. Sensor node is the most important element in WSNs [1]. It is sensor node's task to sense data, convert them to digital form and understand communication protocol to be able to send and receive data frames. To satisfy WSN's common needs, such as flexible node deployment and easy network rearrangement, wireless communication between sensor nodes is often required. It is also a way to deal with wire inaccessibility. A Sensor node needs to be equipped with some physical resources in order to fulfill all these requirements. These resources can be divided into four subsystems:

- Sensor subsystem - senses values and converts them to digital form.
- Processor subsystem - stores gathered and configuration data in local memory, executes functions according to gathered data or received messages.
- Communication subsystem - enables node to exchange messages with other nodes in range.
- Power subsystem - supplies the other subsystems with power from batteries.

Besides sensing unit nodes, a base station can be found in WSN. The major goal of the base station is to manage, visualize and analyze the sensed information. It also forwards the collected data to the remote server application where the data of all other WSNs is analyzed at much wider range.

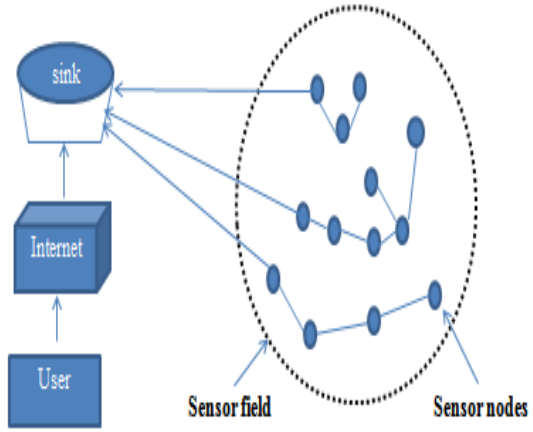

Fig 1: Wireless Sensor Network

WSN's purpose is to broadcast the sensed data to the base station. This implies that requests move from the base station to sensor nodes, but more importantly, sensed data moves in the opposite way i.e. from sensor nodes to the base station. In a manner of speaking the gateway node is a sink-hole of the WSN.

1.2 Security challenges in WSN
Security in WSNs is as important as in other styles of systems, especially in armed forces and security applications (e.g. intruder recognition). Attackers may try to obstruct traffic in sites (i.e. execute a denial of service assault) or bargain data with the addition of some spoofed sensed data to network (i.e. aggregating invasion). Attackers from the within (corrupted node is positioned into WSN) can commit routing disorders by leading data movement to spoofed sinkholes. In WSNs, various attacks are found that degrades the throughput of the network system. In the various attacks, a Sybil attack is the most dangerous attack that affects the whole network.

2. SYBIL ATTACK

The Sybil attack means "detrimental device illegitimately dealing with various identities". Sybil node is definitely the whole process of making several copy nodes using the same personality i.e. identical node id. Such as, a detrimental node can easily state untrue identities, or perhaps impersonate various other reputable nodes inside network. Specifically, wireless sensor networks are more prone to Sybil attack because of the both open and send out communicating medium also exactly the same rate of recurrence is being shared of all nodes. Throughout Sybil attack, attacker can make various lacking legitimacy identities throughout sensor networks either by fabricating or perhaps taking this identities regarding reputable nodes. Therefore the beds base station is not able to discern this reputable as well as the forged node [1]. This confuses the base station along with other nodes and degrades the network performance.

Types of Sybil attack:

With regard to detecting a Sybil attack it is very important to know the different forms where the network is attacked:

2.1 Direct and Indirect Conversation:

Throughout lead type of attack, respectable nodes connect specifically with the Sybil nodes while in indirect attack; a conversation is done throughout the harmful node.

2.2 Fabricated and stolen identities:

Throughout this attack, harmful node brings about a brand new individuality by itself depending on the private with the respectable nodes. Whenever these kinds of harmful nodes would like to connect to their bordering nodes they use any of the imitation identities. The following cause confusion and then collapses a network. Throughout in stolen identities, enemy first distinguishes respectable private after which it utilizes it. Such type of attack could go unidentified in the event that a node whose individuality continues to be stolen is destroyed. Id duplication is done while similar identities are employed quantity of situations in similar places.

2.3 Simultaneous and non-simultaneous attack:

Throughout parallel attack, all of the Sybil identities take part as well in the network. Due to simple one individuality appearing at any given time, bicycle by means of identities may arrive at appear simultaneous. In non-parallel attack, the number of Sybil identities the attacker utilizes is equal to the number of physical devices in the network where each device presents different identities at different times [1].

3. TECHNIQUES

This paper will review various Sybil attack detection techniques and then will come to the point that where a particular technique lacks in accurate detection of the Sybil attack. As shown in the table no.1 the various techniques are compared with one another on the basis of cost, benefit, limitation and a brief summary that how they work.

But from the whole comparison, the results have shown that the UWB ranging-based Sybil assault recognition algorithm is somehow the better technique. UWB ranging-based Sybil assault recognition algorithm criteria [1], a fully distributed, which mean the information collection, monitoring, and recognition operations, are carried out on a wide range of destinations inside the network. These kinds of structures evidently mean that the complete pair of nodes from the system is designed for operating this planned anomaly-based detectors algorithm. Furthermore, due to no cohesiveness, transmissions do not suffer. Finally, throughout discovering flaws, all of our methods harmonizes with localized its audit data, especially the nodes' ranging quotations which mean just about every node performs just as one fair anomaly-based detectors technique (ADS), and therefore, it handles discovering violence limited by it.

4. RELATED WORK

Panagiotis et al. (2015) [1] introduced a new rule-based anomaly detectors procedure, identified as RADS, which often screen and timely detects Sybil attacks and then black list the annoyed nodes within large-scale WSNs. The actually suggested procedure leans on an ultra-wideband (UWB) ranging detection algorithm which are operating in a distributed manner and assisting to perform the abnormality detection tasks.

Manju V C et al. (2014) [2] suggested a combined CAM – Compare and Match Approach and PVM Position Verification method to counteract these kind of attacks. It is based on identity and location information. This approach might clear up the actual Sybil harm nearly 88% inside the WSN.

N. M. Saravana Kumar et al. (2015) [3] proposed a signature based detection approach for uncovering redirecting attacks. For any known harm, it offers specified unique, according to that the rules were created while using the guideline platform that happen to be tried for uncovering various redirecting episodes for instance wormhole, black hole and Sybil attack. The simulated final results show that this process increases the robustness of details by means of (measuring) calibrating the actual factors including packet delivery ratio and throughput while revealing the actual redirecting attacks.

P. Raghu Vamsi et al. (2015) [4] proposed a node-centric approach Sequential Analysis (SADSA) to detect the Sybil attacks. It functions in two periods, via, evidence range as well as evidence validation. A simulator results that the suggested strategy has small communicating, producing cost which is strong with discovering Sybil individual by using really low false positive as well as false negative rates.

Noor Alsaedi et al. (2015) [5] proposed the hierarchical trust discovery technique intended for uncovering Sybil invasion throughout WSNs. The trust energy technique includes lots of various stages connected with confirming the ID, situation, along with confidence evaluation based on the energy from the sensor nodes. The outcome has proven that this process is frequently good at discovering Sybil affect throughout WSNs.

P. Raghu et al. (2014) [6] proposed a new Lightweight Sybil Attack Detection Framework (LSDF) to diagnose Sybil attacks. The particular recommended composition works with a couple of elements: primary, facts range; subsequent, facts agreement as well as LSDF may diagnose Sybil task precisely having handful of evidences.

Krishna Kant et al. (2014) [7] displayed an approach to discover Sybil problems using Sequential Hypothesis Testing without having incorrect result associated with incorrect positives as well as incorrect negatives. The particular recommended strategy has become screened with Greedy Perimeter Stateless Routing (GPSR) protocol with more accuracy. Its emulator success shows that a displayed strategy is robust next to Sybil attacks.

R. Amuthavalli et al. (2014) [8] suggested the actual RPC algorithm which detects a valid direction by way of reviewing

each and every node can be a trustable node or even a Sybil node and also directs the results quite safely. Being a powerful and also correct technique, it increases data transmission in the network as well as raises the throughput.

Wei Shi et al. (2015) [9] proposed a lightweight detection mechanism based on LEACH-RSSI- ID (LRD). By analyzing the RSSI-ID tables the Sybil attack can be detected with high detection rate and accuracy.

Imran et al. (2014) [10] suggested a new approach One Way Code Attestation Protocol (OWCAP) intended for WSNs, a new cost-effective and also a safe and secure rule attestation design that shields against Sybil Attack as well as against the core attacks.

T.G. Dhanalakshmi et al. (2014) [11] in this research is finished for Sybil strike and also forecasted a new communal RAI – Relate and Identify Tactic and also LVT Location Verification technique to steer clear of these types of attacks.

Rupinder Singh et al. (2016) [12] recommended a Trust Based Sybil Detection (TBSD) technique to detect Sybil nodes in WSNs, which is based on manipulative trust values of adjacent sensor nodes and the nodes with the trust values less than a threshold value are detected as Sybil node.

Reza et al. (2014) [13] introduced a distributed and efficient algorithm based on broadcasting two-hop messages to detect Sybil nodes in wireless sensor networks. Also it outperforms similar existing algorithms with respect to true and false detection rates.

5. COMPARISON TABLE

Table 1: Compares the different Sybil attack detection techniques

Ref No. & Year	Technique	Cost	Benefits	Summary	Limitations
R. Amuthavalli et al. (2014) [8]	Random Password Comparison Method	Cheap	Dynamic, Avoid ID-duplication, Improves efficiency.	If the intermediate node's information did not match with the RPC database, node is considered to be a Sybil node.	It is necessary to include the route repair mechanism in case of route failure.
P. Raghu et al. (2014) [6]	Light-weight Sybil Attack Detection Framework	Cheap	Robust, 99.9% detection accuracy, Along with well-known noise factor and also mileage measurement, the localization errors can be predicted.	Nodes methods to a conclusion on deciding a Sybil attack with the immediate observations, receive as inputs to sequential probability proportion test to validate the observations.	Need a bigger quantity of samples to attain accuracy.
Krishna Kant et al. (2014) [7]	Sequential Hypothesis Testing	Cheap	Distributed nature, Simple, Robust.	Registers the Sybil attacks accurately without the need of untrue affect associated with false positives and also false negatives.	Require 6 to 8 samples.
Manju V C et al. (2014) [2]	Combine CAM and PVM	Costly	Solve the particular Sybil harm up to 88% inside the WSN.	Sybil node is detected by location wise as well as identity wise.	Require more efficiency for large systems.
Imran et al. (2014) [10]	One Way Code Attestation Protocol (OWCAP)	Cheap	Not only detect Sybil attack but also other insider attacks.	A code attestation scheme that provides maximum basic safety keeping the calculations, indication and storage area overheads down level.	Need to development of a code attestation application, More storage required.
T.G. et al. (2014) [11]	RAI – Relate and Identify Tactic and LVT Location Verification technique	Cheap	Solve Sybil attack up to 88% , Maintain the secure data transmission.	Focused about how precisely the RAI and LVT technique prevent the Sybil attack.	Often RAI is unable to discover the actual Sybil attack and then LVT technique is carried out.
Reza et al. (2014) [13]	Two-hop Messages	Cheap	Dynamic and Distributed algorithm, Better performance in viewpoints of true detection and false	Nodes detect their neigh-boring Sybil nodes by broadcasting two-hop messages to their two-hop neighbors.	As the amount of network malicious nodes rises, the false detection rate rises too.

			detection rate.		
M. Saravana et al. (2015) [3]	Signature based detection approach	Cheap	Improves reliability	If the physical identity of the node changes or convinced by creating a fake identity, node is Sybil node.	Detect only known routing attacks.
Panagiotis et al. (2015) [1]	Rule centered anomaly Detection System (RADS) use UWB	Cheap	Minimum communication overhead, Feasible to be applied on practical system, High detection precision, Low false security alarm rate.	Perform distance checks and raise the alarm if variation occur and black list the Sybil node.	Insufficient compliance with old-fashioned WSNs, Need analysis of energy usage.
Wei Shi et al. (2015) [9]	LEACH-RSSI-ID (LRD)	Cheap	High diagnosis rate, accuracy and reliability, Consumes less energy.	Sybil attack found by RSSI-ID tables using LEACH protocol.	Does not compete with other attacks.
Noor Alsaedi et al. (2015) [5]	Energy Trust Detection System	Cheap	The particular Sybil diagnosis for that strategy is over 87% with considerably less volume of false positive, Saves energy as well as Reduces the overhead communication.	Confirming the actual ID, location, and rely on study depending on the power with the sensor nodes, bring about revealing Sybil attack in WSNs.	Need to evaluate the system for other attacks.
P. Raghu Vamsi et al. (2015) [4]	Sybil Attack Detection using Sequential Analysis (SADSA)	Cheap	Low processing and communication overhead. Robust with surprisingly low false positive and false negative rate.	A node-centric approach works in two stages: Information collection and Information validation.	Require to extend the method to heterogeneous and mobile WSNs.
Rupinder et al. (2016) [12]	Trust Based Sybil Detection (TBSD)	Cheap	More effective than the most of the existing techniques. Low cost.	Each node in the cluster calculates trust value of neighbor nodes and sends it to the CH; the node with average trust value less than a predefined threshold is detected as the Sybil nodes.	Not considered the effect of mobility of sensor nodes.

Table 2: Compares the Parameters of the different Sybil Attack Detection Techniques

Citation	Supports energy	Delay Time	Throughput	Packet Delivery rate	False Positives & False Negatives	Average number of samples	True Positives	Error Detection rate	Bandwidth utilization	Accuracy
R. Amuthavalli et al. (2014) [8]	✓	✓	✓	×	×	×	×	×	×	×
P. Raghu et al. (2014) [6]	-	-	-	×	✓	✓	×	×	-	-
Krishna Kant et al. (2014) [7]	×	×	×	×	✓	✓	×	×	×	×
Manju V C et al. (2014) [2]	×	×	×	×	×	✓	×	×	×	✓
Imran et al. (2014) [10]	×	×	×	×	×	×	×	×	✓	×

T.G. et al. (2014) [11]	-	-	-	-	-	×	×	×	×	✓
Reza et al. (2014) [13]	×	×	×	×	✓	-	-	✓	-	-
M. Saravana et al. (2015) [3]	×	×	✓	✓	×	×	-	-	-	-
Panagiotis et al. (2015) [1]	×	×	×	×	✓	×	×	✓	×	×
Wei Shi et al. (2015) [9]	✓	-	-	-	×	✓	×	×	-	-
Noor Alsaedi et al. (2015) [5]	×	×	×	×	✓	×	✓	×	×	✓
P. Raghu Vamsi et al. (2015) [4]	✓	×	-	-	×	✓	×	✓	×	×
Rupinder et al. (2016) [12]	×	×	-	-	-	-	-	×	×	✓

6. GAPS IN LITERATURE

The provided expert systems concentrate on stationary systems. Nonetheless, mobility should be analyzed as different portions of sensing unit websites such as military, health-related, and also sector needs the utilization of mobile sensing unit nodes. The recognition of indirect Sybil attacks is not reinforced by the shown systems. Nonetheless, a Sybil node may well consider the id of a legal node via imitation. The power employed by sensing unit nodes is effective crucial for the network living circuit. Even so, the research into the power usage inside construction from the RADS technique is also dismissed.

7. CONCLUSION

Security is now a major matter of most mission-critical applications WSNs are envisaged to aid. This paper shows that Sybil attacks can strictly even worse the performance of network and security danger by disintegrating various networking protocols. So the comparison of varied Sybil attack detection techniques has been displayed which predicted on the various parameters demonstrate the information collection, monitoring, and recognition procedures are performed at lots of network locations. But still, there are few issues in detecting attacks that do not have considered the stochastic environment and also analysis of energy consumption are ignored. So in future to cope with these issues, we will propose the fuzzy regular membership function for Sybil attack detection.

8. REFERENCES

[1] Panagiotis Sarigiannidis, Eirini Karapistoli, Anastasios A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information" , Elsevier, June 2015.

[2] Manju V C "Sybil attack prevention in Wireless Sensor Network", IJCNWMC 2014.

[3] N. M. Saravana Kumar, S. Deepa, C. N. Marimuthu, T. Eswari, S. Lavanya "Signature Based Vulnerability Detection Over Wireless Sensor Network for Reliable Data Transmission", Springer 2014.

[4] P. Raghu Vamsi and Krishna Kant "Detecting Sybil Attacks in Wireless Sensor Networks using Sequential Analysis", International Journal on Smart Sensing and Intelligent System, Vol. 9, No. 2, 2015.

[5] Noor Alsaedi, Fazirulhisyam Hashim, A. Sali "Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks" , IEEE 2015.

[6] P. Raghu Vamsi, Krishna Kant "A Light-weight Sybil Attack Detection Framework for Wireless Sensor Networks", IEEE 2014.

[7] P. Raghu Vamsi, Krishna Kant "Sybil Attack Detection using Sequential Hypothesis Testing in Wireless Sensor Networks", ICSPCT 2014.

[8] R. Amuthavalli, DR. R. S. Bhuvaneshwaran "Detection and Prevention of Sybil Attack in WSN Employing Random Password Comparison Method", JATIT 2014, Vol. 67 No.1.

[9] Wei Shi, Sanyang Liu and Zhaohui Zhang "A Light-weight Detection Mechanism against Sybil Attack in Wireless Sensor Network", KSII Transactions of Internet ad Information Systems VOL. 9, NO. 9, September 2015.

[10] Imran Makhdoom, Mehreen Afzal, Imran Rashid "A Novel Code Attestation Scheme against Sybil Attack in Wireless Sensor Networks", IEEE 2014.

[11] T.G. Dhanalakshmi, Dr.N.Bharathi, M.Monisha "Safety concerns of Sybil attack in WSN", IEEE 2014.

[12] Rupinder Singh, Jatinder Singh, Ravinder Singh "TBSD: A Defend Against Sybil Attack in Wireless Sensor Networks", IJCSNS 2016.

[13] Reza Rafeh and Mozhgan Khodadadi "Detecting Sybil Nodes in Wireless Sensor Networks using Two-hop Messages", Indian Journal of Science and Technology, Vol 7(9), 1359–1368, September 2014.

[14] Priyanka Rawat, Kamal Deep Singh, Hakima Chaouchi, Jean Marie Bonnin "Wireless sensor networks: a survey on recent developments and potential synergies", Springer 2013."

[15] Udaya Suriya Raj Kumar Dhamodharan, Rajamani Vayanaperumal "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message

Authentication and Passing Method", Volume 2015, Article ID 841267, Scientific World Journal, 2015.

[16] V. Sujatha, E.A. Mary Anita "Detection of Sybil Attack in Wireless Sensor Network", IDOSI 2015

[17] Priyanka Rawat, Kamal Deep Singh, Hakima Chaouchi, Jean Marie Bonnin "Wireless sensor networks: a survey on recent developments and potential synergies", Springer 2013.

[18] Rupinder Singh, Dr. Jatinder Singh, Dr. Ravinder Singh "Sybil Attack countermeasures in wireless sensor", IJCNWC, ISSN: 2250-3501 Vol.6, No 3, May - June 2016.