IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-5, Issue-11 E-ISSN: 2347-2693

# Fuzzy based Sybil attack detection in Wireless Sensor Network

**Palak**

Dept. Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, India

*Corresponding Author: palakpalak23@gmail.com*

**Available online at: www.ijcseonline.org**

Received: 17/Oct/2017, Revised: 28/Oct/2017, Accepted: 10/Nov/2017, Published: 30/Nov/2017

***Abstract***— Wireless Sensor Networks (WSNs) are mostly vulnerable to the various attacks. The performance of the wireless sensor networks plays vital role but attacks degrades the performance. One of the attacks is the Sybil attack, in which a malicious node creates a huge number of fake identities in the network. The study indicates that the UWB ranging-based Sybil attack detection in wireless sensor network has better results but it can be improved further by utilizing the optimistic decision making technique. This research work mainly focus on the wireless sensor network which use fuzzy membership function for Sybil attack detection which further improves the WSNs. This proposed technique provides 95% accuracy and higher the value of F-measure and lower the false probability rate and error rate.

***Keywords*—** Wireless Sensor Network, Sybil attack, Fuzzy membership function.

## I. INTRODUCTION

Wireless Sensor Network (WSN) is a wireless group composed spatially dispersed out autonomous instruments by using alerts for us to cooperatively be mindful of physical or environmental conditions, including temperature, sound, anxiety, movements or possibly impurities, from various locations. [1] An everyday wireless sensor network (WSN) system is created by merging a good number of autonomous versions, plus nodes utilizing routers together with a gateway. The dispersed technique of calculating nodes communicate wirelessly to a central opening, which provides a link with the reinforced sphere where one can obtain, examine, and in addition to display their particular way of calculating statistics. Anyone can utilize routers for getting an additional connection link amongst close nodes and therefore the entry for expansion space gateway in addition to dependability during a wireless sensor network [2]. Security is definitely transforming into a serious interest for most mission-critical applications, WSNs happen to be envisaged in order to support. These inherently inclined elements involving WSNs have appointed them predisposed o several varieties attacks. This work restrains their emphasis to look after against an extremely destructive sort of attack, the Sybil attack. Sybil attack can easily make an attempt weaken the multilevel functionality and additionally compromise the safety just by disrupting many network protocols.[3] Sybil node is the process of making two or more copy nodes sticking with the same i.d i.e. same node id. Exceptionally, wireless sensor networks are usually more likely to Sybil attack with the opened and also over the broadcast communication medium as well as same rate is something that is revealed with all of nodes. Found in Sybil attack, attacker tends to make different illegitimate identities throughout sensor networks whether with fabricating and even theft the actual identities involving legitimate nodes. So that the base station cannot decide the actual legitimate as well as forged node [5].

A variety of attacks are possible in WSNs and Sybil is one of them, in which a malicious node illegitimately takes multiple identities. Sybil attack can result in badly affecting the routing in the sensor networks. A large number of network security schemes are available for the protection of WSNs from Sybil attack.

Rest of the paper is organized as follows, Section I contains the introduction of Wireless Sensor Network including the applications and various attacks, Section II contains the explanation of the Sybil attack and Fuzzy membership function, Section III contains the related work, Section IV contains the gaps in literature, Section V explains the methodology with flow chart, Section VI describes results and discussion, Section VII concludes research work with future directions.

## II. SYBIL ATTACK AND FUZZY MEMBERSHIP FUNCTION

### *A. Sybil attack*

In WSNs, each node is recognized as one entity and just one single abstract idea is presented of an identity.[6] Therefore, in WSNs nodes are susceptible to any scheme that allows identities to be falsified or forged. An attack that results in such a malicious activity is called the Sybil attack. So, a single node in Sybil attack intentionally and illegitimately produces numerous false or forge identities to sensor nodes in the WSN. This is done by either stealing legal identities of other nodes or creating new (fake) identities. [7]A Sybil node in the network is a disobedient nodes extra identity. As a result, a single entity of the network may get a selected number of times (depending on number of identities) in order to contribute in network operations that basically relies on redundancy, thereby in this way it can control the outcome of the operation in order to defeat the redundancy mechanisms. Sybil attack can be activated while broadcasting. Figure 1 provides a scenario of Sybil attack.

For detecting a Sybil attack, it is very necessary to recognize the ways in which the network is attacked. The attack can be divided into following three ways:

1) *Direct and Indirect Communication:* In direct Sybil attack, the legal nodes communicate openly with the Sybil nodes in the network, whereas in indirect attack, this communication is done with the help of malicious nodes.

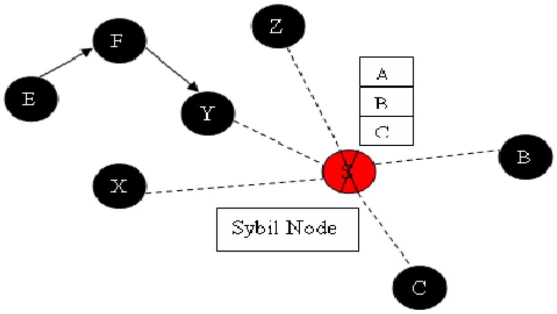

Figure 1. Scenario of Sybil attack [2]

2) *Fabricated and stolen identities:* In this type of Sybil attack, a malicious node constructs a new identity for itself. This new identity is based on the identities of the legitimate nodes.[2] The process when these malicious nodes communicate with their next neighboring nodes, they make use of any one of fake identities. This result in confusion in the network and it may collapse the entire network. In stolen identities case, the attacker first identifies legitimate existing identities and stole it. This type of Sybil attack may go unidentified in the network in the case of destroying of the node whose identity has been stolen. Node identity replication is done in the case when the same identities are used for a number of times in the same places in the sensor network.

3) *Simultaneous and Non-simultaneous attack:* : In the simultaneous type of Sybil attack, all the Sybil attack, all the Sybil identities participate simultaneously in the sensor network. Due to one identity appearing at a time, cycling through the identities will make it to appear simultaneously. In non-simultaneous Sybil attack, the number of identities that are used by assailant is equal to the quantity of physical devices that are present, where each of the devices presents dissimilar identities at different times.

### *B. Fuzzy Membership Function*

Fuzzy is defined as a good superset in common (Boolean) intuition which has been extensive to control the method of partial real truth -- real truth beliefs between "wholly genuine" along with "wholly false". Fuzzy is the better approach for the detection and provide the best accuracy.

Fuzzy classification means to use the fuzzy logic which is definitely utilized to take care of classification problems. In development of fuzzy classification technique, the main step is to build member function and then to find out several ideal fuzzy rules within the fuzzy classification technique. Fuzzy membership functions and fuzzy rules can be designed by skilled understanding technique along with other substitute that will be utilizing data driven approach. The membership function of a fuzzy set is a generalization of the indicator function in classical sets. In fuzzy logic, it represents the degree of truth as an extension of valuation. Degrees of truth are often confused with probabilities, although they are conceptually distinct, because fuzzy truth represents membership in vaguely defined sets, not likelihood of some event or condition.

Fuzzy is a multi-valued group, as from a single condition one cannot decide that either the node is attacker or genuine because there are other various circumstances exist or conditions exist, on all that fuzzy value will be formed and then the node as attacker or genuine is defined. Therefore, in this way Fuzzy is more affective in comparison to other techniques. The experimental results clearly indicate that the proposed technique outperforms over the available technique.

## III. RELATED WORK

**R Panagiotis et al. (2015) [1]** unveiled a fresh rule-based anomaly detectors technique, discovered as RADS, which frequently display screen and timely detects Sybil disorders and then blacklist the irritated nodes within large-scale WSNs. The actually advised procedure leans with an ultra-wideband (UWB) varying recognition algorithm which is working in a sent out manner and supporting in doing the abnormality recognition tasks. **Manju V C et al. (2014) [2]** recommended a merged CAM - Compare and Match Methodology and PVM Position Confirmation solution to counteract these sorts of attacks. It really is based on id and location information. This process might get rid of the real Sybil harm practically 88% inside the WSN. **N. M. Saravana Kumar et al. (2015) [3]** suggested a signature established detection methodology for uncovering redirecting problems. For just about any known harm, it provides specified unique, relating to that the guidelines were created with all the guideline platform that occurs to be attempted for uncovering various redirecting shows for illustration wormhole, black opening, and Sybil episode. The simulated benefits illustrates that process escalates the robustness of details through (measuring) calibrating the real factors including packet delivery proportion and throughput while uncovering the real redirecting attacks. **P. Raghu Vamsi et al. (2015) [4]** suggested a node-centric strategy Sequential Evaluation (SADSA) to find the Sybil episodes. It functions in two times, via, research range as well as research validation. A simulator results that the recommended strategy has small communicating, producing cost which is strong with finding Sybil specific by using surprisingly low incorrect positive as well as incorrect negative rates. **Noor Alsaedi et al. (2015) [5]** proposed the particular hierarchical trust finding technique intended with regard to uncovering Sybil assault throughout WSNs. The particular trust energy scheme is comprised of numerous stages associated with credit reporting the ID, scenario, along with self-confidence evaluation based upon the energy through the sensor nodes. The outcome offers proven that this particular process is generally countless at discovering Sybil affect throughout WSNs. **P. Raghu et al. (2014) [6]** proposed a brand new Lightweight Sybil Attack Detection Framework (LSDF) to diagnose Sybil attacks. The particular commended composition works through a link of elements: primary, facts range; subsequent, facts agreement as well as LSDF may diagnose Sybil task precisely ensuring handful of evidences.

**Krishna Kant et al. (2014) [7]** viewed a procedure for discovering Sybil problems using Sequential Hypothesis Assessment without having wrong consequence associated with wrong positives as well as wrong negatives. This recommended strategy is becoming screened with Greedy Perimeter Stateless Routing (GPSR) standard protocol with more reliability. Its emulator success implies that a viewed strategy is solid next to Sybil problems. **Biswas et al. (2014) [8]** suggested a novel attack detection technique in which node authentication has been used so that one can recognize malicious nodes and remove the false positive problem that can appear through spotting techniques. Node authentication Node authentication not merely erases false positive but yet will help with the function precise location within it and is a two bottle proof pertaining to anxiety attack detection. **Ji et al. (2015) [9]** suggested the centralized algorithmic rule so that one can recognize attack and demonstrate their correctness rigorously. With the dispersed wireless community, DAWN, the dispersed spotting algorithmic rule through wireless community code solutions, can be suggested as a result of checking transform within the circulation directions within the resourceful packets the result. The following rigorously turned out in which DAWN helps ensure the best cheaper likely involved with flourishing spotting rate. **Imran et al. (2014) [16]** got carried out an in depth review and examination of varied defenses suggested against Sybil attack. The authors have discovered their advantages and weaknesses and also propose a novel One Way Code Attestation Protocol (OWCAP) for wireless sensors networks, which can be an inexpensive and a secure code attestation system that defends not only against Sybil Strike but also against a lot of the insider attacks. It really is a fresh cost-effective in addition to a safe and sound guideline attestation design that shields against Sybil Assault as well as up against the core attacks. **T.G. Dhanalakshmi et al. (2014) [17]** forecasted a fresh communal RAI - Relate and Identify Strategy and also LVT Location Confirmation technique to stay away from this kind of attacks.

## IV. GAPS IN LITERATURE

- The introduced professional system is targeted on stationary supplies networks. Nonetheless, the ability to move must be inspected since several necessary practical application industries connected with sensing unit networks including armed service, medical care, and even community need to have the usage of mobile sensor nodes.
- The detection connected with indirect Sybil attacks isn't established by the suggested system. Nonetheless, some sort of Sybil node may well bargain the actual id connected with a legitimate node by the use of impersonation.
- The application of Fuzzy membership function is not taken into consideration within the existing work.

## V. METHODOLOGY

### *A. Proposed Methodology*

First the network is deployed on the basis of the characteristics define in the Table 1. Then, fuzzy rules are defined that decide either the node is genuine or the attacker. The membership function used in this is trapezoidal membership function. Once the data is send to the M sensor nodes, an attacker initialize in order to start the attack in the network. For this random distribution is done. The attacker is initialized because here in the network, our target is on the indirect Sybil attack detection. Once the attacker is initialized, detection start and every time radius and F-MEM values are updated based upon the fuzzy membership function. Then node trust factor is evaluated that either the node belong to the multicast node or not, if yes then it is a genuine node otherwise it is an attacker node and then radius and delay per hop is updated. After this the training and testing phase is done through WEKA and the final node trust evaluation is done based on fuzzy values.

### *B. Flow chart*

The below given flow chart explains the whole methodology.

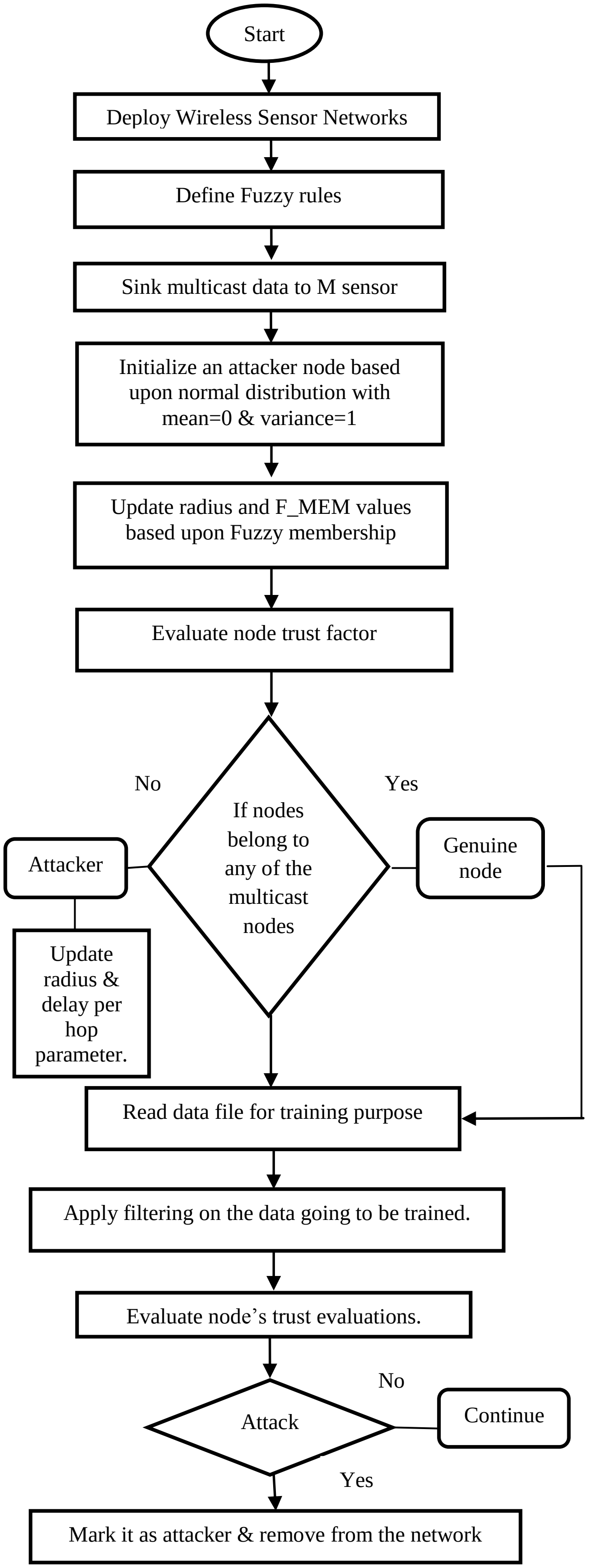
Start
Deploy Wireless Sensor Networks
Define Fuzzy rules
Sink multicast data to M sensor
Initialize an attacker node based upon normal distribution with mean=0 & variance=1
Update radius and F_MEM values based upon Fuzzy membership
Evaluate node trust factor
No
Yes
If nodes belong to any of the multicast nodes
Attacker
Genuine node
Update radius & delay per hop parameter.
Read data file for training purpose
Apply filtering on the data going to be trained.
Evaluate node's trust evaluations.
No
Attack
Continue
Yes
Mark it as attacker & remove from the network

Figure2. Flow chart of the methodology

## VI. Experimental setup and Results

Table 1. has demonstrated several different constants and variables necessary to simulate this work.

Table 1. Experimental setup

| Parameters | Value |
|---|---|
| Nodes (N) | 10 to 50 |
| Multicast nodes (M) | 5 |
| Coverage range | 700 |
| Network area | 100 by 100 |
| Sink position | 10,10 |
| max_it ( maximum migration) | 100 |
| Loop | 1 |
| C1 (fuzzyfication parameters) | 2.05 |
| C2 | 2.05 |
| x_ peak (Maximum peak value) | 100 |
| PLP (Packet Lost Probability) | 10 |

### A. *Performance analysis*

This paper has designed and implemented the proposed technique in MATLAB. First the Wireless Sensor Network is deployed as shown in the Figure 3 where G is the base station and CH is the cluster head. In Figure 4 Clusters formation starts. Figure 5 shows the detection of Sybil attack. At last the Figure 6 shows the final view after detection of Sybil attack.

The evaluation of proposed technique is done on the basis of following metrics i.e. Accuracy, F-measure, true positive rate and false positive rate. A comparison is done between all the parameters with proposed algorithm in Figure 7 and Figure 8.

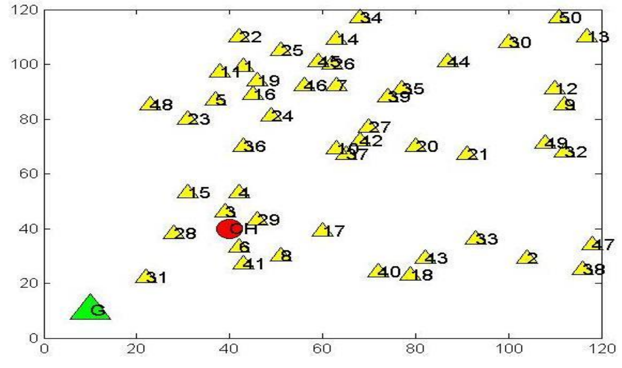

Figure3. Initiation of Sybil attack scenario in WSN

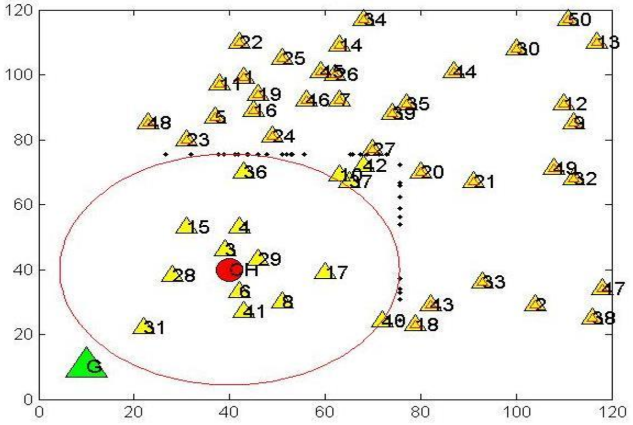

Figure4. Cluster Formation

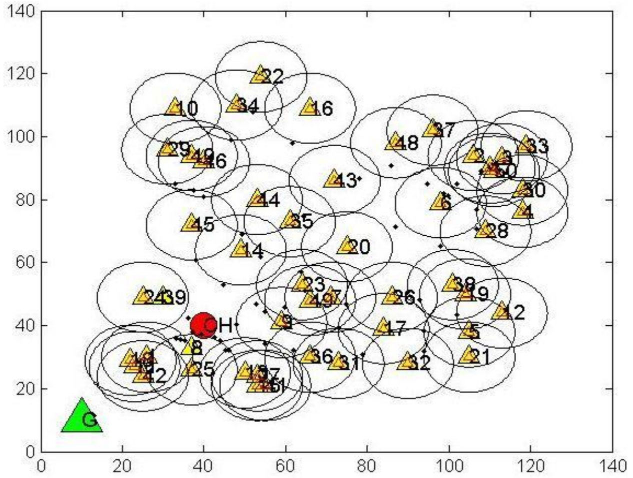

Figure5. Detecting Sybil attack

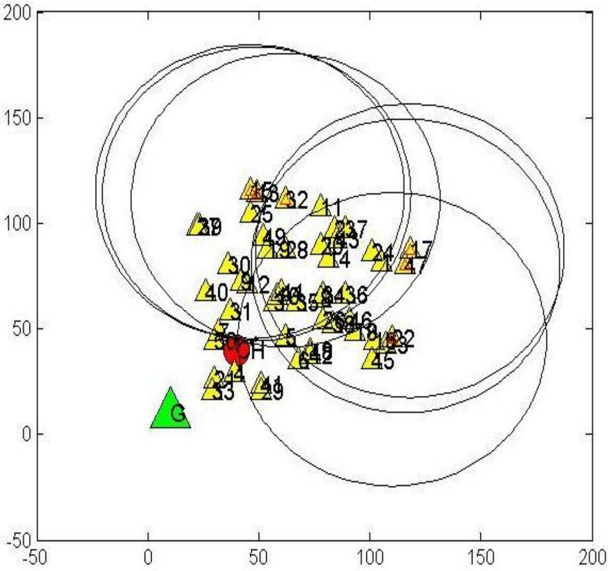

Figure6. Final view after detection of Sybil attack

## B. *Performance evaluation*

1) *False Probability rate:* It is defined as the number of instances which are classified as incorrect from the total number of instances used.

$$FPR = \frac{FP}{FP + TN}$$

2) *F-Measure:* It is the measure that combines precision and recall. It is the harmonic mean of precision and recall. It is calculated as:

$$F = 2 * \left[\frac{(Precision * Recall)}{Precision + Recall}\right]$$

3) *Accuracy:* Accuracy refers to the ability of the model to correctly predict the class label of new or unseen data. It is calculated as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

4) *Error rate:* It is defined as the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. Bit error ratio is a unit less performance measure, often expressed as a percentage.

$$Error\ rate = \frac{FP + FN}{TP + TN + FP + FN}$$

Where True positives (TP) =No. of correct classifications predicted as yes (or positive), True negatives (TN) =No. of correct classifications predicted as no (or negative), False positive (FP) =No. of incorrect classifications predicted as yes (positive) when it is actually no (negative), False negative (FN) =No. of incorrect classifications predicted as no (negative) when it is actually yes (positive).

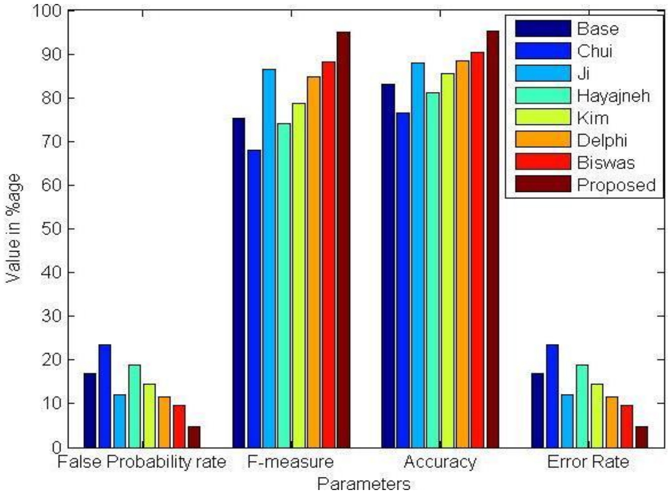

Figure7. Comparison of percentage parameters

5) *True positive rate:* TPR measures the proportion of positives that are correctly identified as such.

$$TPR = \frac{TP}{TP + FN}$$

6) *False positive rate:* FPR usually refers to the probability of falsely rejecting the null hypothesis for a particular test. The false positive rate is calculated as the ratio between the number of negative events wrongly categorized as positive (false positives) and the total number of actual negative events.

$$FPR = \frac{FP}{FP + TN}$$

7) *Precision:* Precision is a description of random errors, a measure of statistical variability.

$$Precision = \frac{TP}{TP + FP}$$

8) *Recall:* Recall (also known as sensitivity) is the fraction of relevant instances that are retrieved. Both precision and recall are therefore based on an understanding and measure of relevance.

$$Recall = \frac{TP}{TP + FN}$$

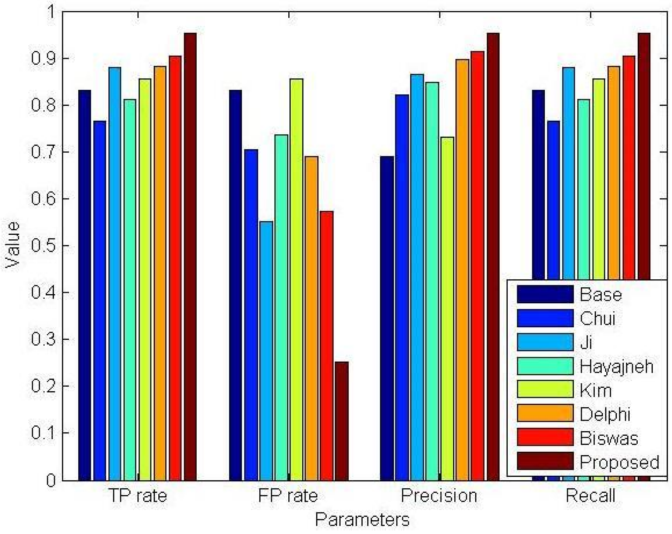

Figure8. Comparison of parameters

## VII. Conclusion and Future Scope

Security is definitely transforming into a serious interest for most mission-critical applications, wireless sensor networks (WSNs) happen to be envisaged in order to support. Sybil attack in WSNs is a severe attack. In this paper, fuzzy based Sybil attack detection in WSNs is proposed. The trapezoidal membership function is used. The research has analyzed the performance on the basis of various parameters. This proposed technique provides 95% accuracy and higher the value of F-measure and lower the false probability rate and error rate. Also the detection is done with low false positive rate. The future directions for the proposed work are as:

- Fuzzy theory based WSNs does not guarantee the high availability of services i.e. effect of failures are ignored. Therefore, in near future we will propose fault tolerance based WSNs to provide high availability of resources.
- Also, in near future some well-known backup path routing techniques will be considered to reduce the packet dropping rate further.
- Also, in near future Neuro-fuzzy system will also be used instead of standard to improve the throughput rate further.

## References

[1] Panagiotis Sarigiannidis, "*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, "*Signature Based Vulnerability Detection Over Wireless Sensor Network for Reliable Data Transmission*", Springer 2014.

[4] P. Raghu Vamsi, "*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, "Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks" , IEEE 2015.

[6] P. Raghu Vamsi and 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] J. Biswas, "*WADP: an attack detection and prevention technique in MANET using modified AODV routing protocol*," in Proceedings of the 9th IEEE International Conference on Industrial and Information Systems (ICIIS '14), pp. 1–6, December 2014.

[9] S. Ji, "*attack detection algorithms in wireless network coding systems*" IEEE Transactions on Mobile Computing, Vol. 14, No. 3, pp. 660–674, 2015.

[10] M. J. Kim, "*Algebraic watchdog: mitigating misbehavior in wireless network coding*" IEEE Journal on Selected Areas in Communications, Vol. 29, No. 10, pp. 1916– 1925, 2011.

[11] H. S. Chiu and K. S. Lui, "*DePHI: detection mechanism for ad hoc wireless networks*" in Proceedings of the IEEE 1st International Symposium on Wireless Pervasive Computing, pp. 1–6, January 2006.

[12] T. Hayajneh, "*DeWorm: a simple protocol to detect attacks in wireless ad hoc networks*" in Proceedings of the 3rd IEEE

International Conference on Network and System Security (NSS '09), pp. 73– 80, Gold Coast, Australia, October 2009.

[13] Reza Rafeh, "*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] R. Amuthavalli, "*Detection and prevention of Sybil attack in wireless sensor network employing random password comparison method*" Journal of Theoretical & Applied Information Technology, Vol. 67, No. 1, 2014.

[15] Wei Shi, Sanyang Liu, "*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.

[16] Imran Makhdoom, "*A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks*" , National Software Engineering Conference (NSEC), IEEE 2014.

[17] T.G. Dhanalakshmi, "*Safety concerns of Sybil attack in WSN*", IEEE 2014.

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

[19] A. V. Vibi, "*Detection of Sybil attack using neighboring node messaging using wireless sensor network*" International Journal of Advanced Technology in Engineering and Science, Volume No. 3, Issue No. 3, ISSN (online): 2348 – 7550, March 2015.

[20] Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal, "*Detecting and preventing Sybil attacks in wireless sensor networks using message authentication and passing method*," The Scientific World Journal, 2015.

[21] Prabhjot Kaur, "*Review Paper of Detection and Prevention of Sybil Attack in WSN Using Centralized IDs*", International Journal of Engineering Science and Computing, July 2016.

[22] A. B. Karuppiah, "*A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks*", 3rd International Conference on Eco-friendly Computing and Communication Systems (ICECCS) IEEE 2014.

[23] T. G. Dhanalakshmi, "*Safety concerns of Sybil attack in WSN*", International Conference on Science Engineering and Management Research (ICSEMR), IEEE 2014.

[24] Rupinder Singh, "*A Novel Sybil Attack Detection Technique for Wireless Sensor Networks*", Advances in Computational Sciences and Technology ISSN 0973-6107 Vol.10, No. 2, pp. 185-202, 2017.

[25] Singh R, "*Sybil Attack Countermeasures in Wireless Sensor Network*", International Journal of Computer Networks and Wireless Communications, Vol. 6, No. 3, May2016.