Retraction

Retraction: Detecting Sybil Attack In Wireless Sensor Networks Using Machine Learning Algorithms (IOP Conf. Ser.: Mater. Sci. Eng. 1042 012029)

Published 11 August 2022

This article has been retracted by IOP Publishing following an allegation that this article may contain tortured phrases [1]. IOP Publishing has investigated in line with the COPE guidelines. During the investigation, the authors admitted that a paraphrasing tool was used in the creation of this paper and were unable to demonstrate they performed the work described. IOP Publishing has also been unable to verify that any peer review was conducted on this article. Given these issues, the journal has lost confidence in the validity of the findings presented and agree this article should be retracted.

IOP Publishing wishes to credit PubPeer commenters [2] and the Problematic Paper Screener for bringing the issue to our attention.

The authors neither agree or disagree to this retraction.

[1] Cabanac G, Labbe C, Magazinov A, 2021, arXiv:2107.06751v1
[2] https://pubpeer.com/publications/EDD0BB483D37A9FF6A6DEFC68DE0A0

Retraction published: 11 August 2022
Detecting Sybil Attack In Wireless Sensor Networks Using Machine Learning Algorithms

Mandala Mounica¹, Mrs.R.Vijayasaraswathi², Mrs. R.Vasavi³

¹M.Tech Student of Software Engineering, Dept. of Computer Science & Engineering, VNR VignanaJyothi Institute of Engineering and Technology, Hyderabad, Telangana, India
²AssistantProfessor,Dept.ofComputerScience&Engineering,VNRVignanaJyothiInstitute Of Engineering and Technology, Hyderabad, Telangana, India
³AssistantProfessor,Dept.ofComputerScience&Engineering,VNRVignanaJyothiInstitute Of Engineering and Technology, Hyderabad, Telangana, India

monicagoud9@gmail.com
vijayasaraswathi_r@vnrvjiet.in
vasavi_r@vnrvjiet.in

Abstract. In sensitive areas such as battlefields, a Wireless Sensor Network (WSN) is especially in military and civilian applications and it is of utmost importance to develop security in these networks. In various respects, this can improve the quality of life. But to be used for protection reasons in multiple situations such as implementation. There is a high risk of being exposed to multiple viruses and hacking attacks. Unauthorized APs for information protection needs to be detected. Any malicious attacks against these networks, Like Sybil Attack leads to breach of security by enacting as a node that illegitimately declares several false identities at the same time. This misleads valid nodes, and they presume each of those identifiers as actual independent nodes by accident. Thus we proposed a machine learning model to detect Sybil attack in network where rawtraffic data has been collected and is used identify authorized and unauthorized APs in an integrated wired/wireless environment.

Keywords: Wireless Sensor Network, Machine Learning, Sybil attack, NSL-KDD Dataset.

1. Introduction
Since Smart gadgets are constantly utilizing wireless sensor networks, it is difficult without Wi-Fi to find positions in our lives. Wi-Fi is used in offices, bars, military stations, schools and public institutions. The creation of low-power, low-cost, small multifunctional sensor nodes has been enabled by numerous advances made in the field of wireless communication and electronics research. A wireless sensor
network consists hundreds of thousands lightweight, inexpensive sensor nodes operate together to provide the capacity for data collection and environmental monitoring as shown in Fig 1. In other words, sensor nodes transfer them, step by step, to sink node(s), after sensing information from the environment[27].

![Figure 1 Wireless Sensor Network System](image)

There is a risk of hooligans, interference, and modification of data packets due to the existence of transmitted communication. It is also important to include protection in this area to protect the network from these threats in order to safely route the data in the network[28].

The most harmful attack for wireless sensor network is Sybil attack which oughts to cause security breach. Sybil Attack is type of attack in peer-to-peer networks where several identities are successfully run at the same time by a node in the network and compromises the authority / power in credibility schemes as shown in Fig 2. The key goal of the assault is to obtain the majority of the network in order to carry out unlawful acts on the infrastructure (in compliance with laws and regulations laid down in the network). A single entity (computer) can establish and maintain several identities (user accounts, accounts on an IP address). These numerous false identities tend to be valid, identical identities for outside observers.

![Figure 2 Sybil Attack Occurrence Wireless Sensor Network Systems](image)

1.1. Types of Sybil attack

- In direct attack, truthful nodes directly affected by node(s) of Sybil.
The truthful node(s) is targeted in an indirect assault by node that connects directly with Sybil node(s). As it under the destructive control of Sybil node(s), this middle node corrupted.

![Figure 3 Sybil Attack Nodes](image)

Figure 3 depicts types of nodes in Sybil attack

- Malicious hub/Sybil Attacker: hub that parodies characters of different hubs.
- Sybil hubs: Additional characters are made pernicious hubs known Sybil hubs.

2. Related Work

Wireless sensor networks are distinct from conventional networks that need creative energy-sensitive and real-time routing solutions, reliability, fault identification, data integrity. Machine Learning aims to solve functional problems as well as non-functional requirements.[1] Mohammad Abu Alsheikh et al. information about WSN 's functional problems such as routing, location, data aggregation, data aggregation Attacks are rapidly rising and become lethal threats to Networks. [2] Recommended monitoring method that assists in the identification of Attack traffic. Attacks such as Botnet Assault can assault IoT machines and can allow them to be more easily hacked than desktop computers. Network-based IoTBotnet Attacks Identification was introduced in [3] Yair Meidan, Michael Bohadana et al. They classified advantages by using their method to detecting infected IoT such as resistance to heterogeneity, open world, performance. Sybil attack is extremely dangerous against sensor and impromptu structures where multiple characters are claimed illegitimately by a node. R's suggested a Random Password Evaluation system [RPC]. Amuthavalli et al. [4] which encourage the deployment and control of a node’s location, thus preventing the attack on Sybil. In defining the Sybil threat, the RPC approach is complex and precise. This approach increases the transfer of data in the network and can increase the throughput as well. Sybil Attack's Methods and Materials are provided at [5] by Udaya Surya et al. To configure, energy-efficient, promising nodes in the network, they graded the Network Model for Sybil attack. A WSN subsystem is separated by means of services that would satisfy WSN specifications. [6] Palak et al. introduced the Sybil Attack. They divided Sybil attacks into multiple types of fake or compromised images, direct or indirect communications, concurrent or non-simultaneous communications. Various methods of Sybil attack have been reviewed. [7] The key management protocol is intended to have a secure communication framework that uses computationally cheaper symmetric cryptography than asymmetric cryptography, which allows the energy-efficient protocol. A decentralized technique is proposed in [8] by Ehsan-Ullah Warriach et al to find errors in WSNs. Secret Markov Models (HMMs) are used to base this methodology on a statistical approach. The collected data was broken down into two forms as a supervised machine learning proposal: a training set and a test set. In actual cases where faults are basically offset faults, stuck-at fault and benefit fault, the suggested approach has worked well. [9] The authors suggested a classification strategy by SVM. It splits down the data into two classes: one for normal measurement and one for inaccurate measurement. To identify the data, the decision function is then implemented in the cluster head.

In [10], the authors separated the faults into two categories: (1) Persistent and (2) intermittent faults. Persistent errors are persistent errors while intermittent mistakes are temporary mistakes The paper [11] contains a comprehensive bibliography of and implementations of computer algorithms. Supervised and unsupervised learning frameworks were discussed in the report. Sunil Ghildiyal et al [12] addressed small
processing capacities and fewer resources to render WSN nodes very vulnerable to a range of attacks. [13] Nodes conserve scarce resources and, like any strong system inside the network like BS, they have to be covered by any outside support. Only sophisticated security processing and security algorithms for the whole network can be executed by BS. [14] The proposed solution to Sybil’s attack based redistributed sensor node keys, embedded at the time of development. Imran Makhdoom et al. [15] identifies various defences proposed against Sybil Attack and Proposed epic One Way Code Attestation Protocol (OWCAP) for remote sensor organizations, a financially savvy and secure code certification scheme that protects against Sybil Attack [16][17][18]. The statistical test and the neural network are merged by Manikopoulos and Papavassiliou. To get similarity measures, first run the Klomogrov-Smirnov test and classify network packets using 5 neural networks. [19]. By identifying and defining consistencies and trends in training data [20], the adoption of statistical methods to boost computer performance. [21] Suggested a stable neighbour authentication protocol on HB adaptation, validation convention for RFID gadgets. The utility of HB shared-key, unidirectional verification conventions permits them hypothetically ideal for asset confined gadgets as RFID labels. Suggested approach in [22] defined Sybil attacks via the positioning of anchor nodes. The main idea behind this method was that two nodes cannot be present at same location at same time and [23] uses received signal strength indication (RSSI) based methodologies. They all used the nodes signal strength to judge whether a node is Sybil in nature or not. C. Komar et al [24] developed the notion of preferred routes for Trespassers (TFP) and given method can estimate possibility of detecting surveillance network. Both computational approaches and simulation findings confirm the precision of the suggested consistency measure. S. A variety of current methodologies for detecting Sybil attacks have been reviewed by Sharmila et al [25] and algorithm suggested detecting Sybil assaults in remote Sensor Network. It is observed after identification, the ratio of throughput and packet transmission has increased. Sunil Ghildiyal et al [26] addressed reduced capability and less control WSN nodes to render vulnerable to a range of attacks.

3. Proposed System

This research is aimed at creating system that detects Sybil and other threats, using a machine learning model trained for efficiency and accuracy in detection by machine learning algorithms varies details in system Architecture as shown in Fig 4. It’s hard to spot an intrusion because it appears close to the victim-end’s legitimate network traffic. In the meantime, Sybil and other attacks on victim systems (ddos, u2r, and probe) must be produced over time. Otherwise, the network / system services would not be malicious. Therefore, the designed Machine learning approach used to identify Sybil attack based on the raw traffic internet data. We practise our machine learning model with a broad dataset, NSLKDD 2017 Dataset (We use NSLKDD short in rest paper). Our monitoring strategy uses a series continuous network packets and capable of learning subtle distinction between threats and legal ones. Historical information fed the machine learning model classify Sybil and other attacks (ddos, probe, u2r). It helps to identify recurring patterns of Sybil, DDoS, U2R, Probe attacks and locate in long-term traffic chain.

Machine learning is typically defined by sensor network programmers set of techniques and algorithms used to construct prediction models. Machine learning professionals consider it rich area with very wide themes and trends. Among those want to add machine learning WSNs, knowing certain themes would be helpful. Machine learning algorithms have enormous versatility advantages applicable to various WSNs implementations. An access point in WSN base station which transmits and receives data (sometimes called a transceiver). An access point links users inside the network to other users and can also act as an interconnection point between the WSN fixed wire network.
Figure 4: System Architecture

Gathering data
Raw network traffic data involves the analysis of many attributes that emphasize for prediction of target variable. This module involves gathering data from mass amount of internet traffic records that collected and bundled into dataset for real-time analysis. The study involves the detection of attacks in dataset records.

Pre-processing data
Data pre-processing is a vigorous technique in the machine learning process. The categorical data is converted to binary data by clearing the missing values, null values, and inaccurate values, data polishing. The dummy values are added for different attributes to form a dataset and are sent to the training and testing phase.

Feature Extraction and Transformation
First concentrate network traffic fields from NSLKDD informational index. Table I a few models and kinds of fields. We use preparing highlights. Unlike in relation to other AI strategies applied on Sybil, Probe, U2RDDoS location, we don't have to choose measurable highlights in model.

| Field                  | Field Example | Field Type |
|------------------------|---------------|------------|
| duration               | 5607          | Continuous |
| src_bytes              | 232           | Continuous |
| Protocol_type          | tcp           | Nominal    |
| Num_failed_logins      | 5             | Continuous |
| Num_file_creations     | 1             | Continuous |
| Num_shells             | 0             | Continuous |
| Su_attempted           | 0             | Binary     |
| Count                  | 1             | Discrete   |
| srv_count              | 1             | Discrete   |
| Serror_Rate            | 0.5           | Discrete   |
| dst_host_serror_rate   | 0.01          | Discrete   |
Table I classifies three types of fields: Binary fields, nominal fields, continuous fields. For substance of most text and trivial areas, we turn the representation. We convert them to binary Boolean fields like TCP / UDP port number. After element change, we get $m \times n'$ network, where $m$ shows number of parcels and $n'$ demonstrates number of new highlights For e.g., we encode TCP and UDP port number to 16-digit paired rundown.

3.1. Machine Learning based Approach

Algorithms are crucial in the analysis of hidden data knowledge. Because of their precision and speed, machine learning is commonly used in attack detection. We have suggested a framework where machine learning algorithms are applied to effectively detect the attacks with performance. The data collected is that there is no raw traffic internet data in the necessary format to collect the data and bring it into the required format using different data processing techniques to train the model, so the user only has to upload data after developing the system. There are four different machine algorithms in this project it is a comparison study of the algorithms and comparison study of the heart disease data set and real-time dataset. The machine learning algorithm incorporates three different types of learning.

**Supervised Learning**

Here the algorithm uses the set of variables to generate a method were it maps inserted query to the desired outputs. It consists of the target which is projected from the set of independent variables; the training come to an end till the desired accuracy is attained on the training dataset shown in Fig 5. Various examples of Supervised Learning are Strategic Regression, Decision Tree, Support vector machine and Random Forest, and so on.

![Figure 5: Supervised learning model](image)

**Unsupervised Learning**

Here the technique makes use of clustering the population in distinct clusters. It is used for segmenting the all given population into the desired groups that are specified as shown in Fig 6. Some of the unsupervised learning is Apriori algorithm, k-means clustering, etc.
Reinforcement Learning

Using this technique was the mechanism is trained to make choices by itself. The machine is put in an environment where it itself trains using the trial and error method where it learns from the previously experienced encounters to gather the best knowledge and to make appropriate decisions. Example is Markov decision process.

A. Logistic Regression

Strategic relapse is a calculation utilized for arrangement. It is utilized to estimate discrete values such as yes, no, 0, 1, true and false. It studies the relationship between the binary response variable from the set of the predictors. This method is a statistical technique for evaluating a dataset where there are one or more independent attributes that define the effect; the outcome is measured using discrete values. The objective of the logistic regression is to obtain the optimal fitting model which determines the relation between the explanatory and the response variable. It generates the coefficient of the formula to predict logit transformation of the presences of the probability of the characteristics of the interest.

\[ s(z) = \frac{1}{1 + e^{-z}} \]

The values predicted are mapped to probabilities, the above sigmoid function is used. Using the sigmoid function and decision boundaries the prediction function is made.

\[ z = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots \]

The above expression is of the multiple explanatory variables.

B. Random forest (RF)

This approach forms a combination of the decision trees with every feature provided into every decision tree. It is very simple and flexible to use algorithm avoiding tuning hyper parameter it always gives the best results. It provides both classification and regression tasks. It uses the supervised learning technique. It creates decision trees by randomly choosing the different attributes present in the dataset available and then gets the predictions from the trees and chooses the best solution. It also indicates the attribute importance. It is considered as the highly accurate and strong method it does not have an over fitting problem because it takes the average of all the predictions made. It handles missing values very efficiently by median replacement and proximity weighted average. It provides with importance of the relative feature which helps in picking the feature contributing most in the classification.

C. Support vector machine

This regulated calculation for AI utilized for issues like arrangement or relapse. To change over the information, it utilizes method called portion stunt and afterward finds suitable limit between the potential
yields based changes [29]. Predictive analysis data classification algorithm that assigns one of the labeled categories to new data components. In certain instances, a binary classifier implies that two potential goal values are present in the data in question. In specific, it is widely used in the classification of support vector machines. On two samples \( x \) and \( x' \), the RBF kernel, expressed feature vectors in some input space specified:

\[
K(x, x') = \exp \left( -\frac{||x - x'||^2}{2\sigma^2} \right)
\]

\( ||x - x'|| \) perceived as squared Euclidean separation between two component vectors between the two featurevectors \( \sigma \). An equivalent definition involves parameter.

\[
\gamma = \frac{1}{2\sigma^2}
\]

\[
K(x, x') = \exp (\gamma ||x - x'||^2)
\]

Since estimation of RBF bit diminishes with separation and reaches between zero (in the breaking point) and one (when \( x = x' \)), prepared understanding as similitude measure.

D. Decision Tree
Paradigm in which each option is centred on the constant time analysis of two numbers is called the Decision Tree Paradigm. The technical difficulty of sorting and searching has been added. The decision tree paradigm is computing model in terms of computational complexity in which algorithm is assumed effectively decision tree, i.e. series branching operations centred similarities such quantities, assigning unit computational expense to the similarities.

The "tests" or "queries" are considered branching activities. The algorithm in question can see Boolean function computation in this context.

\[
f: \{0, 1\}^2 \rightarrow \{0, 1\}
\]

Where the input is a set of questions and the final judgement is the result. Each question can rely on past queries Differing versions of decision tree models is applied on basis of complexity of operations allowed in determiningsingle contrast and way of branching.

Decision tree models help establish lower limits for the theory of complexity in certain forms of computational problems and algorithms. Decision tree complexity or query complexity of this issue or calculation communicated as far as choice tree model known as being computationally intricate.

3.2. Analysis of Algorithms
In the process of anomaly detection, machine learning algorithms are applied to the DDoS, Sybil, u2r, investigate.

- A distributed denial of service (DDoS) attack is deliberate effort to interrupt traffic of targeted website, or network by cascade of Internet traffic flooding the object or the surrounding networks.
- The Sybil assault is a major disruptive assault on the sensor network in which many genuine identities and forged identities are used to access a network illegally.
- User to Root (u2r): Intruder has local access to the victim computer and is attempting to obtain rights for super users.
- Probe: Intruder seeks to obtain details regarding the target host.
The most frequently used algorithms include Backing Vector Machine, Decision Tree, irregular timberland, calculated relapse are executed on dataset for identification of assaulted bundle.

3.3. Analysis of Performance
Eventually, to label each instance as benign or anomalous, we add the customised model to features derived from continuously observed packets. Marked instances are then used to assess if the whole accompanying stream is benign or anomalous. Consequently, where an anomalous stream is observed, a warning should be released, since it may suggest fraudulent behaviour on the provided dataset. Thus notifies each model accuracy shows how effectively detecting the attacks in dataset.

4. Results

Figure 7: Result of Detecting Attacks in Uploaded Dataset

Dataset uploaded underwent through model for Detection processing each record indicates in predictions whether they are Normal, DdoS, Sybil or U2R attacks by classifiers as shown in Fig 7 by introduced machine learning model.

Figure 8: Accuracies in Algorithms
In proposed Machine Learning model, as mentioned in section-III four classifier algorithms ie., SVM, Random forest, Decision tree and logistic Regression algorithms as shown in Fig 8 used to determine how effectively does each classifier detect attacks in network data by accuracy performance.

5. Conclusion

It is apparent from doing the aforementioned analysis that the accuracy of the support vector machine algorithm is of the highest precision. The variables of Predictor are used from the dataset that was generated for the prediction of attacks (DDOs, R2L, Probe, Sybil, and Normal) from real-time data obtained from web sources. For the estimation of the outbreak, there were four main models used. The first model used was Random Forest, which gave 79 percent accuracy. Logistic regression was the second model developed, which gave 84 percent precision. The support vector machine’s third model gave 93 percent precision and the fourth Decision Tree model gave 83 percent precision. It is therefore assumed that the Support vector machine model with the highest precision obtained can be used effectively by 93 percent and also the best predictors of the Attack presence (DDOs, R2L, Probe, Sybil, and Normal) in the uploaded dataset from the variable significance graph.

Future studies will require device extension since data set attacks can be closely studied under networks that currently use construction models that have the potential to foresee future demands, preferences, requirements, and attack detection needs. For different attacks under consideration, there is an ability to achieve prediction method, since it is easy to terminate anything from happening until it alters the current state of nodes in networks by creating a real-time website where nodes go through detection and drop clean data packets.

REFERENCES:

1. Mohammad Abu Alsheikh, Shaowei Lin, DusithNiyato, and Hwee-PinkTan, "AI in Wireless Sensor Networks: Algorithms, Strategies, and Applications", in IEEE Communication Surveys and Tutorials, Vol. 16, No. 4, Fourth Quarter, 2014.
2. Xiaoyong Yuan, Chuanhuang Li, Xiaolin Li, "Profound Defense: Identifying DDoS Attack through Deep Learning", in IEEE International Conference, 2017.
3. YairMeidan, Michael Bohadana, Yael Mathov, YisroelMirsky, "N-BaIoT:Network-based Detection of IoTBotnet Attacks Using Deep Auto encoders", Published by the IEEE Computer Society, 2018.
4. R. Amuthavalli, Dr. R. S. Bhavaneswaran, "Recognition and Prevention of Sybil Attack in Wireless Sensor Network Employing Random Password Comparison Method", in Journal of Theoreticaland Applied Information Technology, 2014.
5. UdayaSuriya Raj Kumar Dhamodharan and RajamaniVayanaperumal, "Distinguishing and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method", in Hindawi Publishing Corporation e Scientific World Journal, 2015.
6. Palak, "Survey on the different Sybil Attack Detection Techniques in Wireless Sensor Network", in International Journal of Computer Applications, Volume 164 – No 1, April 2017.
7. SonaMalhotra, PankajRathee, "Avoidance of Sybil Attack utilizing Cryptography in Wireless Sensor Networks", IJIRST–International Journal for Innovative Research in Science& Technology, 2015.
8. EhsanUllahWarriach, Kenji Tei, "Flaw Detection in Wireless Sensor Networks: A Machine Learning Approach", 2013, distributed in 2013 IEEE sixteenth International Conference on Computational Science and Engineering.
9. SalahZidi, TarckMoulahi, and BechirAlaya, "Flaw Detection in Wireless Sensor Networks through SVM Classifier", distributed in IEEE Sensors Journal, Vol.18, No. 1, January 1, 2018.
10. ThahaMuhammed, Riaz Ahmed Shaikh, "An examination of deficiency recognition procedures in remote sensor organizations" distributed in the Journal of Network and Computer Applications.
11. Uday Shankar Shanthamallu, Andreas Spanias, Cihan Tepedelenlioglu, and Mike Stanley, "A Brief Survey of Machine Learning Methods and their Sensor and IoT Applications", distributed in eighth International Conference on Information, Intelligence, Systems and Applications, 2017.

12. Sunil Ghildiyal1, Ashish Gupta2, Nitesh Tomar3, Anupam Semwal, "Examination of Sybil Attack in Wireless Sensor Networks", International Journal of Engineering Research and Technology (IJERT), Vol. 3 Issue 5, pp.845-848. May – 2014.

13. V. Sujatha, E.A. Mary Anita, "FEM-Hybrid Machine Learning Approach for the Detection of Sybil assaults in remote sensor organizations" distributed in International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol.8, May 7, 2019.

14. P. Raghuvanshi and Krishna Kant, "Sybil Attack Detection utilizing Sequential Hypothesis Testing in Wireless Sensor Networks," in IEEE, 2014.

15. Imran Makhdoom, Mehrreen Afzal, Imran Rashid, "A Novel Code Attestation Scheme Against Sybil Attack in Wireless Sensor Networks" in National Software Engineering Conference, 2014.

16. C. Manikopoulos and S. Papavassiliou, "Organization interruption and deficiency location: a measurable irregularity approach," IEEE Communications Magazine, vol. 40, no. 10, pp. 76–82, 2002.

17. S. Seufert and D. O'Brien, "AI for programmed safeguard against disseminated disavowal of administration assaults," in 2007 IEEE International Conference on Communications. IEEE, 2007, pp. 1217–1222.

18. P. A. R. Kumar and S. Selvakumar, "Circulated refusal of administration assault recognition utilizing a gathering of neural classifier," Computer Communications, vol. 34, no. 11, pp. 1328–1341, 2011.

19. A. H. Duffy, "The 'what' and 'how' of learning in plan," IEEE Expert, vol. 12, no. 3, pp. 71–76, May/Jun. 1997.

20. P. Langley and H. A. Simon, "Uses of AI and rule enlistment," Commun. ACM, vol. 38, no. 11, pp. 54–64, Nov. 1995.

21. Jasmine Norman, Paulraj Joseph "Secure Neighbor Authentication in Wireless Sensor Networks," in second International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronics Systems Technology, Chennai, Feb. 28, 2011-March 3, 2011.

22. Bin TIAN, Yizhan YAO, Lei SHI, Shuai SHAO, Zhao Hui LIU and Changxing XU "A Novel Sybil Attack Detection Scheme for Wireless Sensor Network," in fifth IEEE International Conference on Broadband Network and Multimedia Technology Guillin, Nov. 17–19, 2013.

23. Shanshan Chen, Geng Yang, Shengzhou Chen "A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks," in IEEE International Conference on Communications and Mobile Computing, Shenzhen, April 12-14, 2010.

24. C. Komar, M. Y. Donnez, and C. Ersoy, "Discovery nature of outskirt observation remote sensor networks in the presence of trespassers' favourite ways," Computer Communications, vol. 35, no. 10, pp. 1185–1199, 2012.

25. S. Sharmila and G. Umamaheswarji, "Discovery of Sybil assault in portable remote sensor organizations," International Journal of Engineering Science and Advanced Technology, vol. 2, pp. 256–262, 2012.

26. Sunil Ghildiyal1, Ashish Gupta2, Nitesh Tomar3, Anupam Semwal, "Investigation of Sybil Attack in Wireless Sensor Networks", International Journal of Engineering Research and Technology (IJERT), Vol. 3 Issue 5, pp.845-848. May – 2014.

27. R. V. Saraswathi, L. P. Sree and K. Anuradha, "Dynamic and probabilistic key administration for disseminated remote sensor organizations," 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai, 2016, pp. 1-6, doi: 10.1109/ICCIC.2016.7919666.
28. R.V.Saraswathi, L. P. Sree, and K. Anuradha, "Multi-stage Key Management Scheme for Cluster based WSN," International Journal of Communication Networks and Information Security, Vol. 10, No. 3, pp. 552, 2018.

29. R. VijayaSaraswathi, L. PadmaSree and K. Anuradha"Backing Vector Based Regression Model to Detect Sybil Attacks in WSN" distributed in International Journal of Advanced Trends in Computer Science and Engineering, Volume 9, no. 3, May-June 2020.