Identifying Nodes with Maladaptive Behavior in WSN's by Using Hybrid Incursion Identification Approach for Secure Wireless

G. Amudha (amudhaguna1161@gmail.com)
RMD Engineering College

Research Article

Keywords: WSN, Security, EC, HIIA, Attack detection

Posted Date: October 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-1009882/v1

Identifying Nodes with Maladaptive Behavior in WSN's by Using Hybrid Incursion Identification Approach for secure wireless communciation

Dr.G.AMUDHA, B.E, M.E, Ph.D.,

Associate Professor, R.M.D Engineering College, R.S.M Nagar, Kavaraipettai, Gummidipoondi Taluk,

Tiruvallur District, Tamil Nadu Pin code: 601 206.

Corresponding author mail id: amudhaguna1161@gmail.com

ABSTRACT

In this study, to detect attacks of WSNs, a Hybrid Incursion Identification Approach (HIIA) is proposed. To reduce the amount of Energy Consumption (EC) of the sensor nodes, the HIIA mechanism utilizes a cluster-oriented approach with the LEACH protocol. For misuse observation and anomaly recognition, with MPNN (Multilayer Perceptron Neural Network) depended on fuzzy rule sets, HIIA structure is utilized. To refer to various varieties of attackers and to harmonize the identification results, with appendicle NN, FFNN (Feed Forward Neural Network) is utilized, that means Sybil Attack (SA), Hello Flood Attack (HFA) and Wormhole Attack (WA). To detect a SA, Improved SA Algorithm developed. Similarly, to detect a WA, that particular method is developed by Wormhole Anti-Hybrid Technique. Using the distance and power of the signal, HFA is detected. An exploratory research is conveyed out in a group of nodes. The nodes that misbehave in them are all determined. This proposed method, detects the performance of the accuracy, precision-recall and EC. This proposed method also finds the WA Detection Rate, HFA detection rate and the SA Detection Rate, respectively.

Keywords: *WSN, Security, EC, HIIA, Attack detection*

I. INTRODUCTION

Researchers and technologies are heavily involved in research of Wireless Sensor Network (WSN). Usually the WSN is low-cost, with plenty of sensors and low power. They are reused manually, or are distributed arbitrarily, depending on the destination location. WSN have become a familiar mechanization and strong due to their possible characteristics & applications

such as healthcare, monitoring, catastrophe management, interior applications, and superintendence systems [1]. WSN have poor capabilities in terms of calculation, power, and communication. In WSNs, broadcasting news is an effective and popular role model. For many consumers, to obtain data of their attraction, sanction to distribute and merge details packets across the net, the public formation of WSN is shown in Fig. 1.

WSN has a huge no. of sensor nodes, and it is smaller expensive and consumes smaller energy, it is a self-arranging network. WSN is utilized for a no. of applications, such as civil and military utilities which faces observation of environmental conditions, meteorology monitoring, identification, and dependability. That means, sunray determination, calamity sensing, sound, temperature, particle motion, object recognition, prognostication, and so on [2]. Battery storage for these kinds of network nodes is for bided. Thus, to boost the lifespan of the network, the power in the WSN nodes should be utilized systematically and efficiently.

All of these sensor nodes are exclaimed replaceable devices. They are proficient of interfacing data from one junction to the station node on a big web. They have a minimal shift limit. The data is therefore sent straightly to the desired customer with the changer limit. WSNs are vulnerable to external and internal eruptions, thus over long distances, data transmission can be done through intermediate nodes. Most commonly, because of their resource constraints, they don't have the ability to handle serious attacks [3]. At this stage, to preserve the strategy from assailants, the IDS (Intrusion Detection System) is utilized. By employing these well organized IDS, it is possible to observe attack mechanisms maintained by the attackers [4].

Most WSNs have the ability to sense attacks very easily. Thus, attackers can easily create network traffic. Thus, when broadcasting in packets, alters the original content of the data in the packet, and much of packet, to come-down [5]. So, middle the nodes, to ensure secure transmission, authentication schemes are executed over the network. It is therefore necessary to secure data inter-exchange between nodes in the WSN.

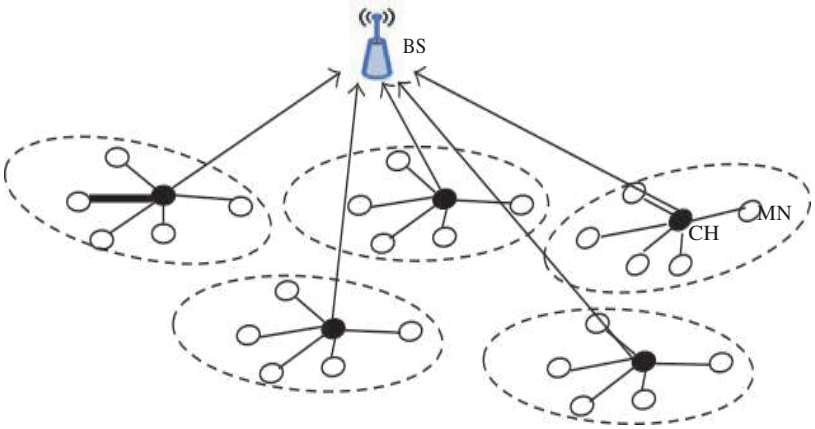

Fig.1: Architecture of cluster based WSN

In battlefield applications, If WSNs is used; sensor nodes are damaged by attackers. To counter the most powerful attacks, a powerful prevention technique is required. Moreover, by a blocking mechanism, not all types of attacks can be countered. So we need to identify the attacker. So IDS is, identify data packets in a network, and by attackers, it is utilized to identify which packet is mutilated. In addition, IDS can help prevent attacks by exploiting the growing nature of attacks. To reduce the amount of EC, the LEACH approach was developed using WSN nodes.

In each cluster, to control the sensor nodes for other clusters, the direct sequence diffusion spectrum approach (DSDS) is used. It can thus communicate with other clusters. Each cluster consists of a sequence of mismatches with adjacent clusters. And to cluster heads interact with other nodes, the allocated queue method is used. In the end, information will be realized in WSN. The nodes in it can move data to a Sink Node (SN); this permits each consumer to access the data. The LEACH protocol depends on 2 suppositions:

1. The SN is located within the borders of the sensor nodes that have been fixed and used.
2. All junctions in the network are uniform.

Thus, the relationship between the SN and the sensor junctions is costly [8]. In non-clump head nodes, to lessen EC, in LEACH, access is choosing through the channel. Because clump members know their own clump head, they can produce a new TDMA table. For each nook of it, designate when to transfer its data. This, by the modules in, this permits the nodes

driven by the blocks to stay in sleep mode. And by using a TDMA table, when changing data, conflict in intra-cluster can be prevented. LEACH is classified as circles. Each circuit starts with a boot process. Then builds the masonry structure, this then continues to be a steady phase. This is to the cluster head, from the node generates various frames for transporting data. And the assembled data is only sent to the SN. To start the boot process at once, time synchronization is kept.

II. LITERATURE REVIEW

In researching the WSNs, the safety of the sensor networks became known. However, it does not use conventional techniques. This is because in the research by Joe et al, these conventional techniques required more energy [10]. Thus the goal of researchers is providing security plans for all security aspects of WSN. In this paper, the objective is to identify three different attackers. SA, WA, and HFA; below, about other researches on safety plans is shown:

Zhu et al has demonstrated the LEAP scheme. Thus, this is a development for the LEAP Project. LEAP uses four types of keys for node needs.

1) With sink-end, a shared key.

2) A private key shared with other junction.

3) A shared keys with whole the nodes in the complete Networks.

4) In the identical clump, the shared set key with adjacent junctions.

In the key management procedure, it generates an initial key, before key arrangement, store nodes in memory. Then, throughout the categorization, every node, prepare from the authentic key and dispatch hello packet.

S. Lee and Y. Lee [11] Authorization to create a secure transmission channel in WSN, and described the prime management scheme. In WSN, before arranging, to save the general key of every nodes, base station utilized. It is exceedingly supreme to raise the safety of the Networks. The authors amalgamate their technique into two types of recognition. First Class Accreditation happened between the sensor nozzle and the SN. The node generated a steady key. It in the SN, for the encryption operation, utilized the public key.

Durganovic et al [12] explained a new protocol for handling different types of keys, such

as the LEAP protocol. Despite this change, lack of restoration it is not possible to create a solution. The sharp distinction is that set keys were estimated by every-one node within the identified clump. Some security protocols have been used in paper [12] to detect hello attacks. An author describes the unique methods used in cryptographic and non-cryptographic techniques. However, this method is more difficult because of the high power, memory and high time of cryptographic methods.

Hankbin et al [13] provided clump key management for ranking sensors. This machine is at the SN, utilizing the area key, approximated Masonry Key. By trying the jumbled manner, the child node of the incomplete key is made. Then to estimate its area key, passed to set leader. Thus the clump key was last computed.

Pires et al [14] initiated the recognition of HFA by signal power. Oriented on the RSS (Received Signal Strength), the advanced procedure recognizes the attackers. If a node doesn't rely on network, it is regarded an opponent. With the support of RSS, nodes are checked in their transference scope. So it distinguish whether the junctions are malevolent or not. Whenever malevolent nodes are discovered, are described.

Singh et al [15] for the disbelieving tip advanced a signal-depended discovering approach. Hello messages they sent, regarding on the signal power, nodes will be noticeable as good or bad. Nodes categorized as bad, by dispatching a plain check packet, are also verified. However, the main drawback of this method is that the piece suspended is the problem.

Kumar and Magotra [7] ameliorate this manner, with the length between the ends, utilizing signal energy; recognize the malicious node, however, when these two parameters express a certain value, increase test packet communication.

Oliveira et al [16], for information transmission on Node-to-Node, to produce reliability, in LEACH-oriented WSNs, they have established FLEACH protocol. In this protocol, with steady key cryptography, to upgrade transferred security, it utilized an erratic and careful manner. In node-to-node transferences communications, this FLEACH process provides friendliness, integrity, freshness, and confidentiality. But it is threatening for the node to identify the offensive.

III. PROPOSED METHODOLOGY

The purpose of the proposed method is using HIIA means detecting attacks like WA, HFA, and SA. To recognize various categories of attackers, this paper uses the advanced LEACH protocol. To detect the above attacks, HIIA gives that the ability to do so. With this HIIA you can get lower positive rate and higher detection value. In the meantime, by at staying unknown attacks; we can discover and add new instances through the MPNN learning of machine learning. In this study, the formation of the proposed HIIA method is presented in figure 4.

To run data packets as normal, the closest method was, first of all, to find anomaly. To recognize multiple types of attack detection, the fault detection module then contains unusual data packets [21]. Finally, to find any intruders and they are enclosed in fuzzy blocks with MPNN to protect the computer from attackers.

Also, to detect malicious nodes, should detect unusual packets, anomaly detection methods are used. Because of this, to detect normal behavior in nodes, this paper uses a standard method. When current behavior has changed from normal behavior, a data packet can be identified as abnormal in a network. Because of this, detection of anomaly usually, data transfers abnormal transfer and, identifies common exchange as well. In classify the fault node in the network, creating problems. However, it rarely refers to an abnormal exchange as a normal exchange. So when the amount of data is reduced, first order a large number of data packet records.

A. Probe of the Attackers

a) *Observation of SA:*

In the SA, in 2 ways, the attackers can be recognized. First, it has the capacity to generate its own specification. That means in WSN, cheats the markings of legitimate nodes. To recognize the new identity created by the Sybil attacker, a preprogrammed algorithm is created. Malicious terminal, with a sign of it, enters the network. Misbehaving nodes don't caste everyone other. Likewise, nodes don't reduce or raise their transferring power. In SA-WSNs, the effects are as follows.

1. The value of the routing table is elaborated in one WSN. This can produce skepticism in data routing packets.
2. By growing or diminishing the truth value of the node; SA pre-check a truth-

depended manner in WSN.

3. In SA-WSN, between systematic nodes creates confusion.
4. For requests on different fronts, because of the reaction of a single node reduces the life of the WSN.

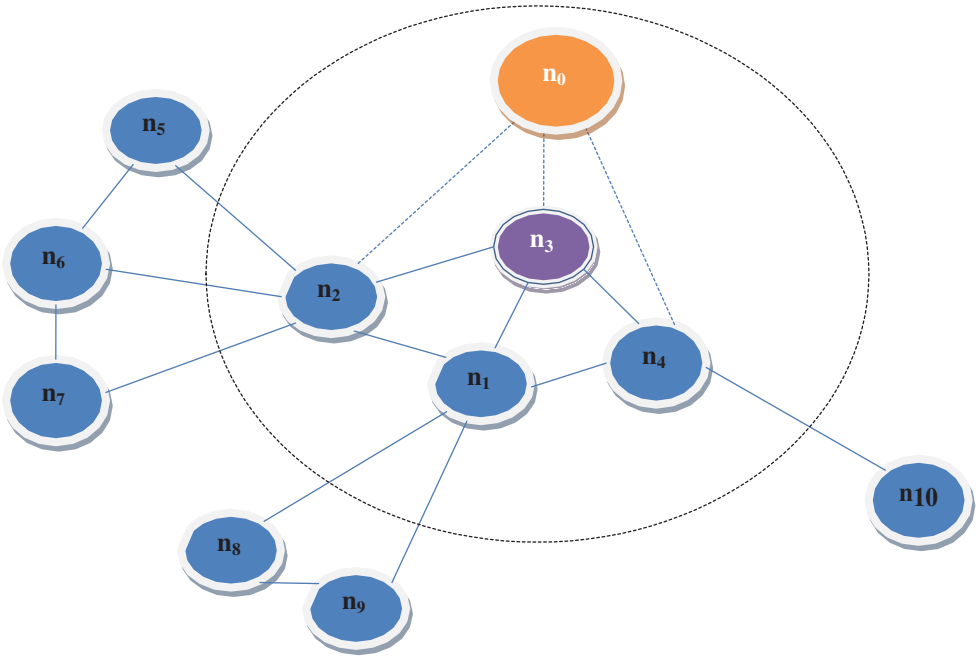

Fig.2: Detection of SA

To identify the SA, with the manner of explaining with MPNN, Improved SA Identification Algorithm (ISAIA) is suggested. Through the validation operation, despite the excessive-mobility, it is utilized to separate the SA and the proper node.

Each node internally creates a table that includes a calculated range estimate. First of all, it was identified, from each neighboring node, calculating distance. Here, as the node is calculated, between the nodes n_x and n_y, calculates the estimated distance d^n_{xy}. However,

distance detection may be inaccurate. And this will be denoted as e error units; there may be a range error. It has unlimited communications, wireless networking is caused by the underlying PHY deficiencies and misbehavior. The node will decrease or increase the distance. So, by the d^e_{xy}, specifies the exact distance between node n_x and node n_y. It concerns that $(d^n_{xy}-\frac{n}{2}) < d^n_{xy} < (d^n_{xy}+\frac{n}{2})$ at median for every node, n_x, n_y.

Every node in WSN performs multiple distance compatibility checks. Node nx with its potential, range of measurements for each pair of nodes denotes equalization. n_x and n_y are represented in its neighbor node list. That means, for all y, z ≠ x, 1 ≤ y,

If $\{\left|d^n_{xy} - d^n_{xy}\right| > e$, then increase an alarm

If $\{\left|d^n_{xy} - d^n_{xy}\right| \geq e$, else continue usual operation.

With the above conditions, except for the quiet node mean by n_y and n_z 2 other nodes they have a minor length contrast than metric units. Then the length testing node, a SA is in action. And a blacklist of nodes with the process of identification continues.

b) Identification of WA:

In WSNs, through the routing process, the specific attack is referred to as the WA. When the attack is in working, in the context of a bad node WSN, sucking a data packet from 1 place, at a certain point, mining can make way for some other attacking node. It reproduces, locally. The subway will be demonstrated on a variety of routes. This has been advanced in the opportunity of ad-hoc natures.

c) *Discover the HFA:*

By utilizing a robust receiver sooner than the usual sensor nodes, the HFA works as hello packets widen. WSN such as these hello packets inaccurately assume that they are inner the transmitter's RSS by their misbehavior, trying to hijack. In this paper, based on the distance threshold of RSS and choose cluster head junctions, regards a cluster-oriented WSN. The length to the nodes is judged by the following equations.

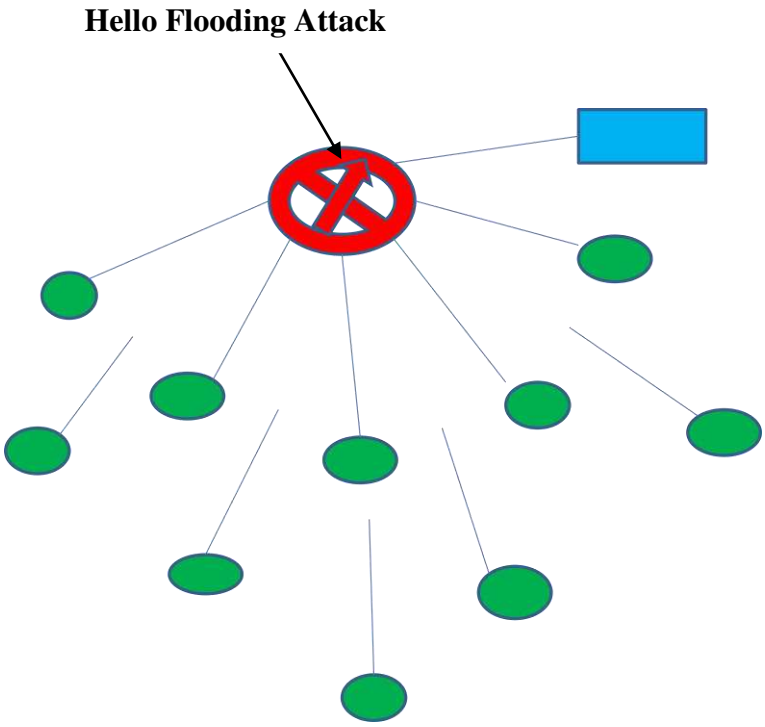

Fig.3: HFA in WSN.

$$\text{Distance} = \sqrt{\left\{\sqrt{(a2-a1)} + \sqrt{(b2-b1)}\right\}}$$

Here, (a1, b1) denotes the place correlates of the station node that is accepting packet. During (a2, b2) are the place correlates that are sent via broadcasting hello packet.

$$(RSS < T_R) \;\&\&\; (D < T_D)$$

Where,

T_R = Threshold RSS

D = Distance

T_D = Threshold Distance

B. Working of Proposed Structure

In this study, based on a cluster, has been proposed WSN. The first is to monitor the status of the data packets. Then there is require exhibiting the patterns of conventional node manners, this is one of the most foremost of data packets. The working flow model of this proposed method can be divided into three functions.

Function 1:

This allows the transaction history in the data packet to be fully evaluated. In clump based WSN, from the neighbors of the clump heads, motion data packets by the base junction, are sent to the MPNN. In that, they went to FFNN. So at the basic node communicating to evaluate previous data packets, are collected. Further data packets can be divided into two types, that is to say, usual and amazing.

Function 2:

This operation is utilized to choose attribute packages. To separate ordinary and unusual packets, the key elements are to search for authentication.

Function 3:

In the process, anomaly implements infiltration discover rules. And it only chooses the greatest features. It regards on the resolve in a representative data packet. Then fuzzy-based controls are made. Then, with a set of well-known rules like BPNN, is stored in Knowledgebase.

In clustered depend WSN, all cluster heads, when sending data to the base nodes, flowing through the base nodes, and complete data packets, detects if there are any unusual data packets. After detection, the anomaly detection system should be checked. If such unusual data packets are recognized, they must be passed to the 2^{nd} operation. This proposed MPNN method distinguishes attackers and their proportion of detection.

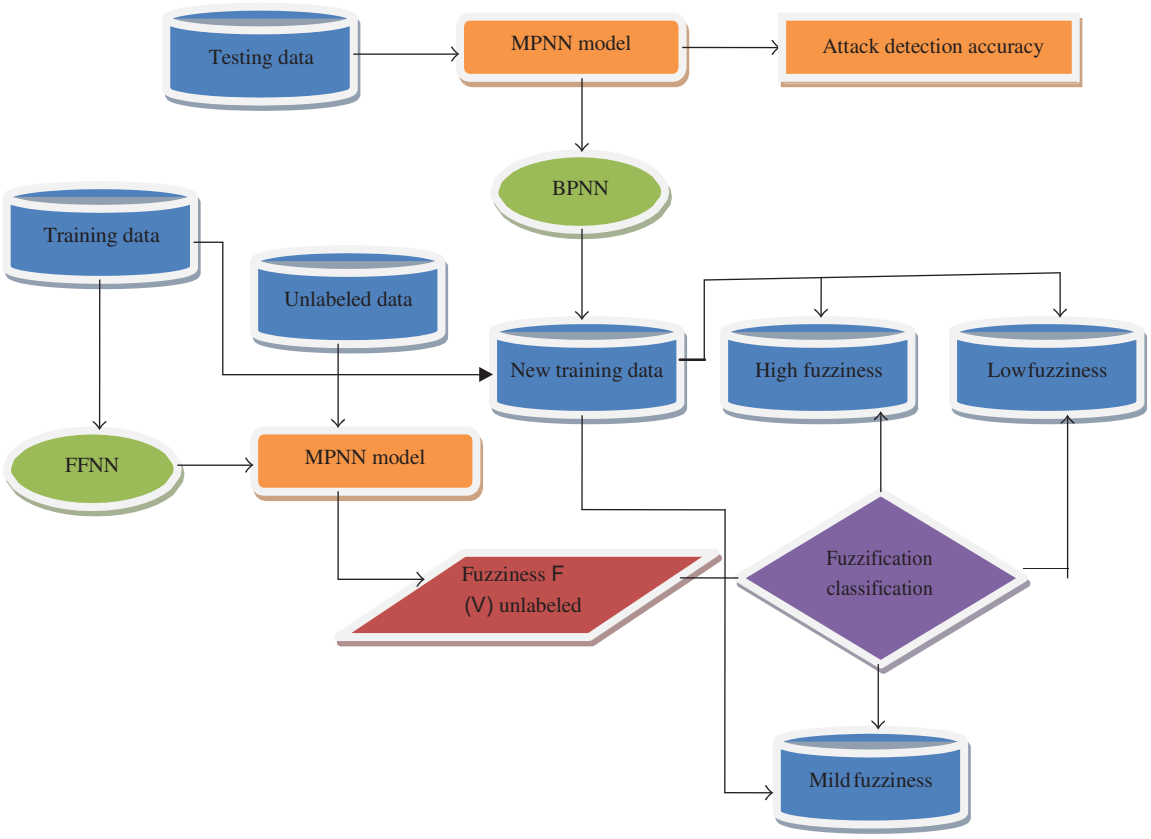

Fig.4: Structure for Proposed Methodology

1) Fuzziness

The term ambiguity concerns two important linguistic factors. It joins with vague boundary value limits. Also it depends on the member function and the obscure packages. Shannon Information Entropy has three important properties. These characteristics describe the ambiguity. For each attribute, since membership degrees are equal, the ambiguous degree should get its maximum value. And the minimum value of each attribute denotes ambiguous set. In this proposed paper, in a neutral network, is considered a kind of cognitive uncertainty.

2) Fuzzy Based Detector Model

In this case, fault detection and anomaly detection methods employ well-defined methods. Thus, to overcome these attacking behaviors, a new strategy has been developed, multiple penetration detection techniques through training data, promising to detect attacks. But they fail unsurely. The advanced manner is depending on MPNN. It also includes BPNN with FPNN. In a more supervised learning mode, this paper is used to bring about greater

accuracy of detection. The proposed HIIA method has demonstrated statistics outside the correlation between output and input variables. And with the weight associated with it, fits. This reduces the error in obtaining greater accuracy. So to get the highest accuracy the methods BPNN and FPNN are proposed.

In FFNN process, parameters are determined in all performance. And by applying the formula given below, the error rate is estimated.

$$e_r = d_o - a_o$$

Here,

d_o = the desired output

a_o = denotes the actual output

3) MPNN

Here, the model of MPNN is classified as BPNN and FPNN. In this paper, this method is presented for the above three types of attacks have been used to accurately identify. With the enlargement of technique, the no. of attackers is enlarging day by day. The previously intrusion discover way should therefore boost the effectiveness of the procedure. To control such difficulties, this present structure is extremely well-ordered. When the complex recognizes fresh kinds of attacks, the ML system has the capability to determine them and learn right aside. However, data packets can't be correctly characterized by misdiagnosis. These are said to be incalculable attacks. Therefore this proposed method is very useful for identifying different types of attacks. These data packets are sending to the MPNN method. The structure is shown in the figure 5.

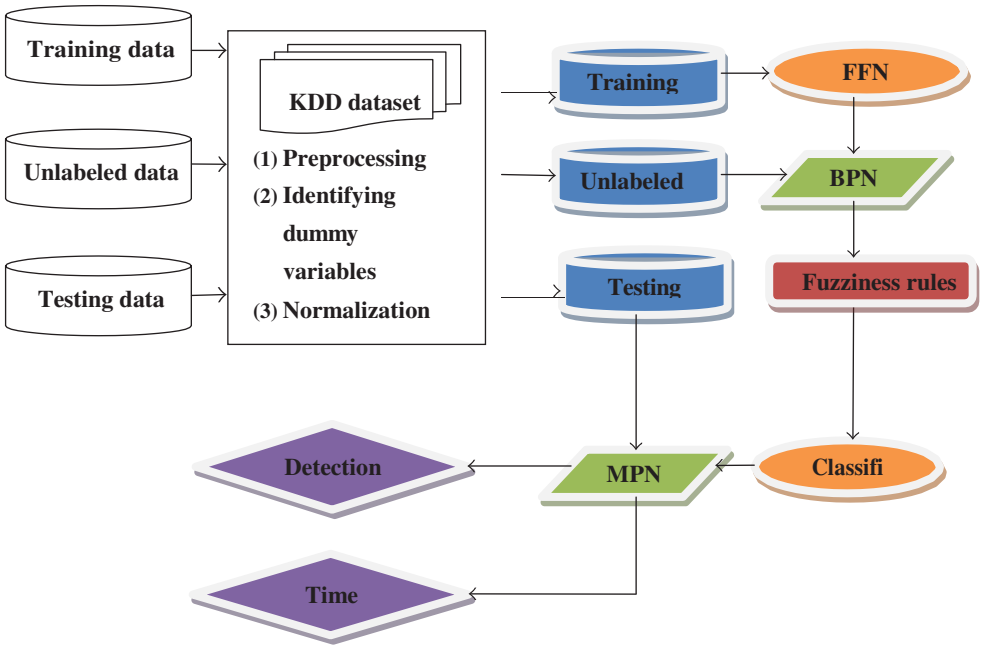

Fig.5: Fuzziness based MPPN

The value of fuzziness $F(V)$,

$$F[V] = -\frac{1}{n}\sum_{j=1}^{n}\left[\mu_j \log \mu_j + \left[1-\mu_j\right] \log\left[1-\mu_j\right]\right]$$

Here, $V = \{\mu 1, \mu 2, \ldots, \mu n\}$ is a fuzzy set. The value of fuzziness is split into 3 sets. That is, low fuzziness, neutral fuzziness, and high fuzziness.

IV. RESULTS AND DISCUSSION

To determine the cluster-based WSN, by reducing duplicate packets, to reduce energy use, efficient MPNN was used. So in the pre-processing phase, duplicate packets are deleted from the network. This improves the strength of data usage. To lessen power utilize, the amount of the fake packet differ under or above the conventional packet. Eventually, it splits the data packet in the middle of the duplicate packets and the legitimate packets. It doesn't produce data on genuine packets. The present HIIA manner is originated to lower the EC in WSNs and it can also be used to secure data packets.

The present HIIA method in this paper can be estimated using the following properties:

1) Accuracy

Generally, accuracy is the proposed method depends on how well overcomes of that algorithm are showed or estimated or calculated. The equation given below is very useful.

$$A = \frac{\sum_{j=1}^{c} PT_j}{N}$$

Where,

C = classes

N = No. of examples

PT_j = No. of true positive value of the j^{th} class

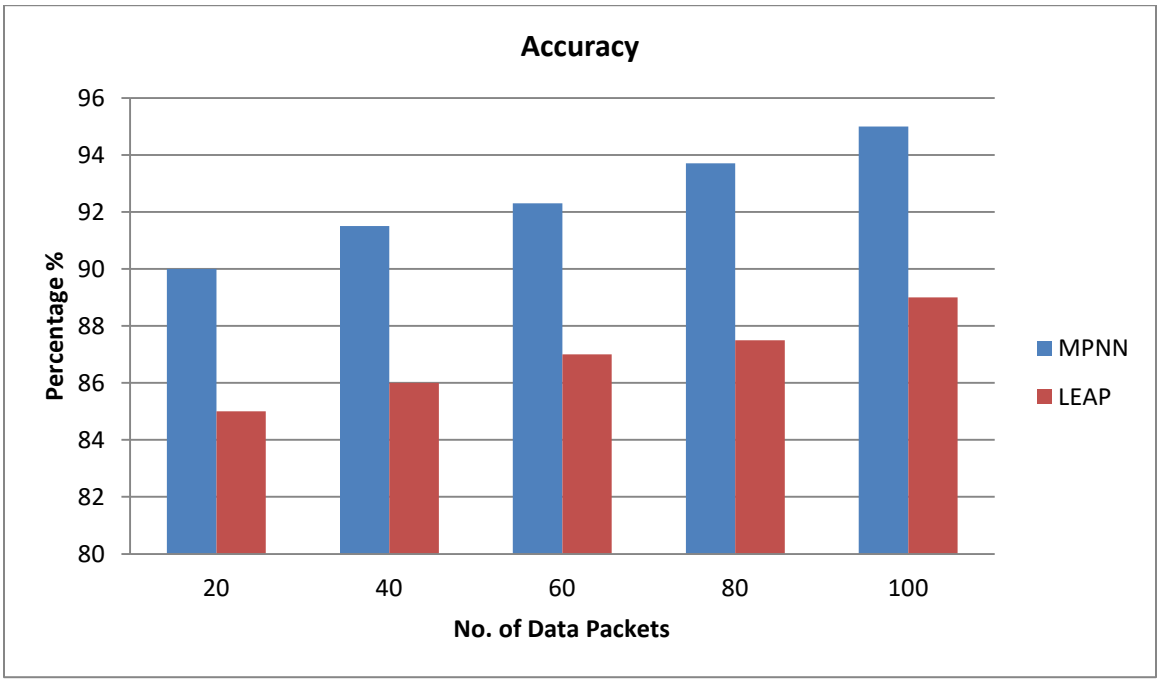

Fig.6: Accuracy Performance

As evaluated, in figure six, the use of specific data packets shows that the particular algorithm has such how much accuracy. In showing so, the MPNN method has much greater accuracy than the LEAP.

2) Rate for Attacker Detection

$$R_{ad} = \frac{\sum_{j=2}^{c} PT_j}{\sum_{j=2}^{c} PT_j + NF_j}$$

Attackers	Attack Detection rate
SA	99,30%
HFA	98,10%
WA	99,105%

3) Precision - Recall

When classes are so unbalanced, precision and recall of the success of forecasting is a good measure. In information retrieval, precision is depends on the relevance of the results of that method. Recall depends on how many results have been returned.

$$R = \frac{PT_j}{PT_j + NF_j}$$

$$P = \frac{PT_j}{PT_j + PF_j}$$

Where,

PFj = No. of false $+^{VE}$ values of the j^{th} class

NF_j = No. of false $-^{VE}$ values of the j^{th} class.

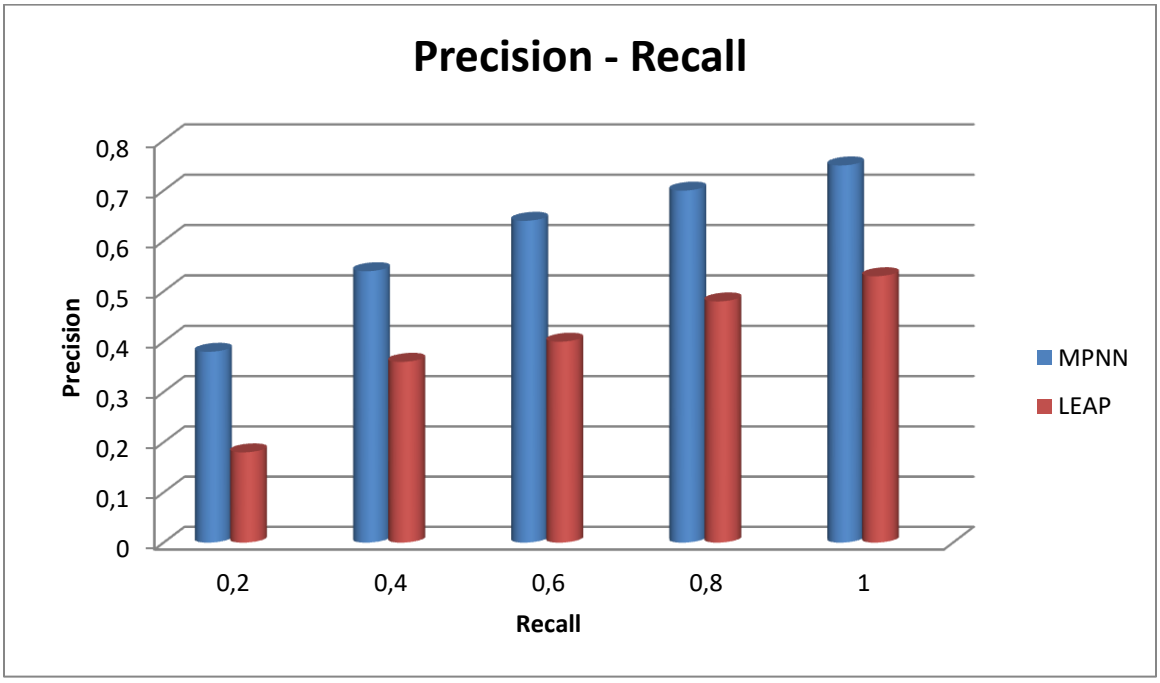

Fig.7: Precision – Recall Performance

4) EC

For the EC computation of nodes of the sensor, at the starting we assign the value of 10-joules. This power is called the beginning energy. At any disposed time, at the sensor end, to indicate power, variable power is utilized. The value of the starting power is mentioned to as the input explanation. To receive and transmit every-one packet, a sensor node drop a specific quantity of energy.

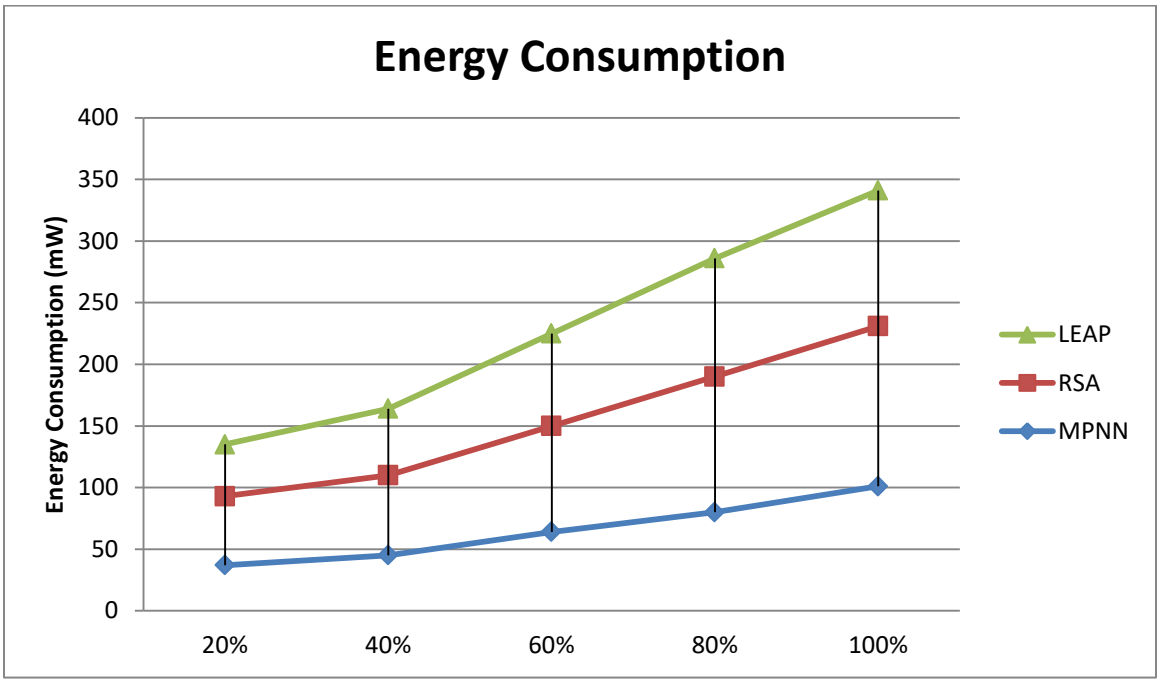

Fig.8: EC Performance

Since of this, at one sensor end, the value of radiation power lessens, the EC of the sensor node is constant, by obtain the deviation between the prime power value and the present power value, is established. If the power of the sensor node is 0, it can't receive or transmit the data packet. Therefore, HIIA's EC in Figure 8 is much lower than other methods.

V. CONCLUSION

In this paper, in WSNs, a protective mechanism was used against SA, WA and HFA. For that, a hybrid algorithm called HIIA is used. It was used to detect anomaly, to detect wrongdoing, and

to detect attacks. MPNN was used here as a hybrid method. In this case, BPNN and FPNN were used to detect the above attacks. A combination of these 2 structures, a excessive HIIA is provided with a low FPR. To reduce EC and communication costs, the cluster-based algorithm with the LEACH algorithm is combined. This enlarges the time of the longevity of the web. This proposed system has a lower FPR and also shows high TPR. The proposed system has proved to be efficient in parameters such as Packet loss, efficiency, PDR, EC, precision, recall and accuracy.

Declarations

1. **Funding**
   Not Applicable
2. **Conflicts of interest/Competing interests**
   There is no conflict of interest from all the authors in the manuscript.
3. ***Availability of data and material**
   Not Applicable
4. ***Code availability** (software application or custom code)
   Not Applicable
5. ***Authors' contributions**
   G Amudha – Overall concepts, literature survey, Working and ideology, Results development, Proof editing

REFERENCES

1) Sunil Ghildiyal, and Ashish Gupta, "Analysis of Sybil Attack in Wireless Sensor Networks", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 5, pp.845-848. May – 2014.

2) Udaya Suriya, and Raj Kumar Dhamodharan, "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method", The Scientific World Journal, Volume 2015, pp.192-195, 2015.

3) S. Abbas, and M. Merabti, "Signal strength based Sybil attack detection in wireless Ad Hoc networks," in Proceedings of the 2nd International Conference on Developments in systems Engineering (DESE '09), pp. 190–195, Abu Dhabi, UAE, December 2009.

4) K.-F. Ssu, and W.-T.Wang, "Detecting Sybil attacks in wireless sensor networks using neighboring information," Computer Networks, vol. 53, no. 18, pp. 3042–3056, 2009.

5) S. Sharmila, G. Umamaheswari, “Detection of Sybil attack in mobile wireless sensor networks,” International Journal of Engineering Science & Advanced Technology, vol. 2, pp. 256–262, 2012.

6) A.Vasudeva, M. Sood, “Sybil attack on lowest id clustering algorithm in mobile ad hoc network,” International Journal of Network Security & Its Applications, vol. 4, no. 5, pp. 135–147, 2012.

7) G. Padmavathi, D. Shanmugapriya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” International Journal of Computer Science and Information Security, vol. 4, pp. 1–9, 2009.

8) N. Balachandaran, S. Sanyal, “A review of techniques to mitigate Sybil attacks,” International Journal of Advanced Networking and Applications, vol. 4, pp. 1–6, 2012.

9) L. Xiao, L. J. Greenstein, “Channel-based detection of Sybil attacks in wireless networks,” IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 492–503, 2009.

10) G. Jing-Jing, and W. Jin-Shuang, “Formal threat analysis for ad-hoc routing protocol: modeling and checking the Sybil attack,” Intelligent Automation & Soft Computing, vol. 17, no. 8, pp. 1035–1047, 2011.

11) H. Yu, and P. B. Gibbons, “Sybil Limit: a near-optimal social network defense against Sybil attacks,” IEEE/ACM Transactions on Networking, vol. 18, no. 3, pp. 885–898, 2010.

12) C. Komar, and M. Y. Donmez, “Detection quality of border surveillance wireless sensor networks in the existence of trespassers' favorite paths,” Computer Communications, vol. 35, no. 10, pp. 1185–1199, 2012.

13) V. Rathod and M. Mehta, “Security in wireless sensor network: a survey,” Ganpat University Journal of Engineering & Technology, vol. 1, pp. 35–44, 2011.

14) R. Amuthavalli, R. S. Bhuvaneswaran, “Detection and prevention of Sybil attack in wireless sensor network employing random password comparison method,” Journal of Theoretical and Applied Information Technology, vol. 67, pp. 236–246, 2013.

15) W. Niu, J. Lei, E. Tong et al., “Context-aware service ranking in wireless sensor networks,” Journal of Network and Systems Management, vol. 22, no. 1, pp. 50–74, 2014.

16) M. Sa, A. K. Rath, “A simple agent based model for detecting abnormal event patterns in distributed wireless sensor networks”, in Proceedings of the ACM International Conference on Communication, Computing & Security, 2011, pp. 67–70.

17) S. Kaplantzis, and A. Shilton, “Detecting selective forwarding attacks in wireless sensor networks using support vector machines”, in 3rd IEEE International Conference on Intelligent Sensors, Sensor Networks and Information, 2007, pp. 335–340.

18) E. U. Warriach, K. Tei, “Fault detection in wireless sensor networks: A machine learning approach,” in 16th IEEE International Conference on Computational Science and Engineering (CSE), 2013, pp. 758–765.

19) B. J. Culpepper, H. C. Tseng, “Sinkhole intrusion indicators in MANETs,” in Proc. First IEEE International Conference on Broadband Networks, 2004, pp. 681–688.

20) G. Kaur, M. Singh, “Detection of black hole in wireless sensor network based on data mining,” in Proc. 5th IEEE International Conference Confluence The Next Generation Information Technology Summit, 2014, pp. 457–461.

Dr.G.AMUDHA, B.E, M.E, Ph.D., pursued her Bachelors of Engineering (CSE) in the year 2002 from Periyar University and Master of Engineering in Computer Science and Engineering in the year 2007 from Anna University, Chennai. She bagged Ninth University Rank in M.E(CSE). She has completed her Ph.D., in the area of Wireless Sensor Networks from Anna University, Chennai in the year 2019. She has 18 years of working experience in the teaching profession. She is coordinating Cyber Security Centre of Excellence activities. She obtained IBM - DB2, Tivoli, and RAD value added certifications. She bagged more than ten NPTEL certificates in the domain of Internet of

Things and Network Security. Her areas of interest are Cryptography and Network Security, Compiler Design, and Sensor Networks. She has guided eight Master of Engineering projects. She was associated as Co-coordinator with AICTE Sponsored Faculty Development Programme on “Provision of Urban Amenities in Rural Areas” and National Level Conference RING 2015. She has published eleven research papers in journals and conferences. She was invited as a Guest Speaker in Anna University Sponsored Faculty Development Training Programme. She is been awarded as Motivational Learner by NPTEL. She also bagged CEH certification.