Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 3548607, 14 pages
https://doi.org/10.1155/2017/3548607

Research Article

Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks

Rupinder Singh, Jatinder Singh, and Ravinder Singh

I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India

Correspondence should be addressed to Rupinder Singh; rupi_singh76@yahoo.com

Received 4 October 2016; Revised 2 February 2017; Accepted 7 February 2017; Published 3 April 2017

Academic Editor: Paolo Barsocchi

In this paper, an Advanced Hybrid Intrusion Detection System (AHIDS) that automatically detects the WSNs attacks is proposed. AHIDS makes use of cluster-based architecture with enhanced LEACH protocol that intends to reduce the level of energy consumption by the sensor nodes. AHIDS uses anomaly detection and misuse detection based on fuzzy rule sets along with the Multilayer Perceptron Neural Network. The Feed Forward Neural Network along with the Backpropagation Neural Network are utilized to integrate the detection results and indicate the different types of attackers (i.e., Sybil attack, wormhole attack, and hello flood attack). For detection of Sybil attack, Advanced Sybil Attack Detection Algorithm is developed while the detection of wormhole attack is done by Wormhole Resistant Hybrid Technique. The detection of hello flood attack is done by using signal strength and distance. An experimental analysis is carried out in a set of nodes; 13.33% of the nodes are determined as misbehaving nodes, which classified attackers along with a detection rate of the true positive rate and false positive rate. Sybil attack is detected at a rate of 99,40%; hello flood attack has a detection rate of 98, 20%; and wormhole attack has a detection rate of 99, 20%.

1. Introduction

Wireless sensor networks (WSNs) are a recent technology and have received huge attention among researchers. Normally, the WSN environment comprises low power, low cost, and a huge number of sensors that are distributed arbitrarily over the target location or are redeployed manually. Wireless sensor networks have become a powerful and familiar technology due to their potential features and applications such as healthcare, monitoring, domestic applications, surveillance systems, and disaster management [1]. Wireless sensor nodes have poor capacities in terms of communication, computation, and energy. In wireless sensor networks, broadcast message is an effective and a popular prototype that permits multiple users to combine and distribute message packets throughout the network effectively in order to get data of their interest. An example diagram of WSN is demonstrated in Figure 1.

Wireless sensor network is a self-organizing network with a huge number of sensor nodes which consumes less power and is of low cost. Wireless sensor networks are utilized for several applications like civil and military applications that encounter detection, security, identifying environmental conditions, and weather monitoring, that is, sunray detection, particle movement, sound, temperature, object identification, prediction, disaster sensing, and so on [2]. This sort of network has restricted battery storage for the nodes, and thus efficient and proper utilization of the energy in WSN nodes is very essential to improve the network lifespan.

These sensor nodes are termed lightweight and transferable devices having the capacities of communicating, sensing, and processing the data from one node to the destination node in a larger network. They have a restricted transmission range and hence send the data directly to the desired user with a transmission range limit. Data transmission in longer distances can be performed through intermediate nodes, since WSNs are vulnerable to internal and external outbreaks. Most commonly, they do not have the capacity to handle a tough attacker owing to their resource restricted nature [3]. In this condition, a secondary stage of defence, mostly called Intrusion Detection System (IDS), is needed to protect the system from the attackers. The vast attacking techniques developed by the attackers can be detected by making use of efficient IDS [4]. Unfortunately, majority of the sensor

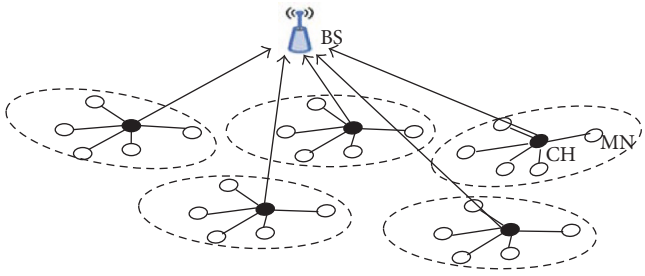

Figure 1: Cluster-based WSN architecture.

networks are very sensitive towards attacks because of WSN characteristics, and antagonists can simply create network traffic, which can also cause heavy packet drop during broadcasting of the packets or change the original content of the message in the packets [5]. Thus, authentication strategies are implemented in the network for ensuring secure communication between the nodes. In WSNs, it is very essential to carry out secure data transmission between the nodes.

For instance, if WSNs are employed in battlefield applications, sensor nodes are intruded upon by the attackers and destroyed. Hence, security plays a significant role. A prevention technique is utilized to counteract the well-established attacks. Moreover, a prevention scheme cannot defend against all the attacks. Thus, these attackers should be identified, so the IDS are utilized commonly to identify the packets in a network and estimate which packet is damaged by the attackers. Furthermore, IDS can help the prevention system through the developed nature of attacks [6].

The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol functions on the Medium Access Control (MAC) protocol based on the clustering algorithm for data collection in the WSN [7]. The LEACH protocol formed as cluster architecture using WSN nodes, to reduce the energy consumption level. To maintain the minimal energy consumption throughout the WSN, the cluster-group heads are selected rotationally among the sensor nodes within the cluster, if the present cluster-group head has lower available energy resources than other sensor nodes.

Therefore, the energy load connected with being a cluster head is evenly distributed with nodes for increasing the lifetime of the entire network. In each cluster, the sensor nodes can communicate using Direct Sequence Spread Spectrum (DSSS) to limit the interference with other clusters. Each cluster applies a spreading sequence which does not match nearby clusters, and cluster heads apply a reserved sequence method for making communication with the sink node. Eventually, the information would be sensed in the WSN in which nodes can transfer the data to a control center or sink node so that each end-user can access the data. LEACH depends on the following two assumptions: the sink node is fixed and located within the area of deployed sensors and all nodes in the network are homogeneous and energy constrained. Thus, communication between the sensor nodes and the sink node is expensive [8]. Media access in LEACH was selected to minimize energy consumption in the non-cluster head nodes. As the cluster members know their own cluster head, they can form a new TDMA schedule that describes to each node exactly when to transmit its data. This allows the nodes to remain in the sleep state with internal modules powered down as long as possible. Furthermore, by utilizing a TDMA schedule, it is possible to stop the collision happening in the intracluster while transferring the data. LEACH is classified into circles. Each circle starts at an initialization process and forms the cluster structure, which is later continued by a steady state phase. It forms different frames of data for transferring the data from node to cluster head; moreover, aggregated data is only transmitted to the sink node. The nodes must contain time synchronized stamp to start the initialization process at the same time. So, to minimize initialization overhead, the steady state phase is also equated to the initialization process.

There are modified versions of LEACH that attempt to add secure features [8], although they still have their own drawbacks as highlighted in the previous section and they do not consider the impact of radio range while electing a secure cluster head upon energy consumption. To identify the attackers, they make use of the network monitor and provide the alarm to the remaining nodes. They protect the system from the attacker's destruction by raising an alarm before the intruder initiates the attack. The two important modules in the IDS are misuse detection and anomaly detection [2]. Generally, anomaly detection develops a prototype to identify the abnormal and normal behavior of the nodes, by carrying out the analysis and comparison of the nodes behavior. It has the highest detection rate, and at the same time it has the highest false positive rate. The misuse detection identifies the various types of attackers by equating or comparing the present attack behavior and the past attack behavior [9]. It has the highest accuracy but with low detection rate. Particularly, it cannot detect unknown attackers, which are not in the base of the model. Various researchers have analyzed a module of hybrid detection to utilize the merits of both misuse detection and anomaly detection. This hybrid detection methodology can identify unknown attacks with the greatest accuracy of the misuse detection and the greatest detection rate of anomaly detection. The Hybrid Intrusion Detection System (HIDS) accomplishes the aim of obtaining the highest detection rate with low false positive rate [1].

This paper describes the Advanced Hybrid Intrusion Detection System (AHIDS); it utilizes a Multilayer Perceptron Neural Network (MPNN), which contains Feed Forward Neutral Network (FFNN) and Backpropagation Neural Network (BPNN) of the supervised learning approach based on the fuzzy logic mechanism with anomaly and misuse detection technique to detect the hello flooding, wormhole, and Sybil attacks with higher detection ratio and lower false alarm.

At first, the Sybil attack detection is based on the Advanced Sybil Attack Detection Algorithm (ASADA) with fuzzification method along MPNN; it is utilized to separate the Sybil node and legitimate node even if it has the highest mobility through the verification process using RSSI (Received Signal Strength Indicator). Then, to identify the wormhole attack, we propose the Wormhole Resistant Hybrid Technique (WRHT) with fuzzification method along

FFNN. The proposed WRHT allows the source node in the sensor network to calculate the wormhole presence probability (WPP) for a path in addition to HC (Hop Count) information. WRHT makes use of dual mode detection by calculation of PLP (Packet Loss Probability) and TDP (Time Delay Probability); if it finds out packet loss at the receiving end, then it is concluded that the wormhole attacker is working in encapsulation mode (hidden mode). Finally, for detecting hello flooding attack, sensor nodes of RSS and distance along with their threshold values are moved to the BPNN. The fuzzy interface in the fuzzy based detector module uses both anomaly and misuse detector in order to estimate the hello flooding attack in the adversary model in AHIDS. Here, the trusted neighbor nodes are instructed to flood a fixed number of fake packets into the sensor network at the same time. If the suspicious node passes this test, then it is directed to send-received check. If it fails this test, then the node is considered as malicious and stored as blacklisted.

2. Literature Review

In recent years, the research about the WSNs had concentrated on the security of the sensor networks. Due to the resource limited environment of the WSN, conventional security strategies had not been employed, as they required too much energy as discussed by Zhu et al. [10]. Therefore, researchers were aiming to provide lightweight security schemes for all the security aspects of WSNs (such as routing protocol, IDS, and secure data aggregation). In this paper, we concentrate on identifying the three different attackers: hello flooding, wormhole, and Sybil attacks; some related security schemes are discussed below.

Zhu et al. [10] had demonstrated a scheme, LEAP+, which is a development of the LEAP protocol. LEAP+ utilizes 4 categories of keys as per the node requirement: (i) a single key shared with the sink node, (ii) an individual key shared with another node, (iii) a group key shared with nearby nodes in the same cluster, and (iv) a cluster key shared with all the nodes in the entire networks. In the key management system, it produced a master key and stored it in the nodes' memory before node deployment. Later on, during deployment, each node was produced from the original master key and forwarded the hello packet, which has its own identifiers to its neighbor. After it received an acknowledgement from its neighbor, verification took place in the MAC layer.

Y. Lee and S. Lee [11] illustrated the authentication and key management scheme to produce the secure communication channel in the WSN. The base station was utilized to store the public key of all the nodes before making deployment in the WSN. It is very essential to enhance the security of the networks; the authors incorporated their technique in two classes of authentication (handshake). The first class of authentication took place between the sink node and the sensor node. The node produced a symmetric key that used a public key for the encryption process in the sink node. It transmitted the encrypted key to the sink node without being decrypted, as the desired node does not know the secret key of the sink node. The next category of authentication was performed between the sink node and a pair of nodes in the networks so that it can authenticate the nodes.

Turkanović et al. [12] illustrated a new protocol that handled various types of keys like the LEAP protocol. The major difference was that group keys were estimated by each and every node inside the specified cluster. Despite this modification, it cannot produce a solution due to the lack of rekeying solution. An extensive survey on protocols and techniques used to detect the hello flooding attack has been presented in [12]. The authors have distinguished methods used in the noncryptographic and cryptographic techniques. However, because of the time, higher energy, and memory demands of the cryptographic methods, it is preferable to utilize the noncryptographic method. Hongbin et al. [13] presented cluster key management for hierarchical sensor networks. This mechanism estimated the cluster key utilizing the partial key in the sink node. By utilizing the random technique, the child node of the partial key was produced and then it was moved to the group head to estimate its partial key, so that the cluster key was estimated at last.

Pires et al. [14] introduced signal strength based detection of hello flooding attack. The proposed mechanism identified the attackers based on the Received Signal Strength (RSS); if a node seems to be distrusted in the network, then it is considered as an adversary; nodes are tested with their transmission range with the help of RSS. Hence, the nodes are detected as either malicious nodes or nonmalicious nodes. Whenever the malicious nodes are detected, they are labelled as "suspicious." Singh et al. [15] proposed a signal strength based detection approach for the suspicious node. Nodes would be represented as a stranger or a friend depending on the signal strength of hello messages sent by them. Nodes classified as strangers are further validated by sending a simple test packet; if the reply of the test packet comes back in a predefined time, then it is regarded as valid; otherwise, it is treated as malicious. However, the major demerit of this method is the bit overhead problem. Magotra and Kumar [7] enhanced this mechanism and depended on the identification of the malicious node using the signal strength along with distance between the nodes. Nevertheless, when both of these parameters exhibit a certain threshold value, then the test packet will increase the communication overhead, which affects the transmission time.

Oliveira et al. [16] introduced FLEACH, a protocol which is designed to provide security for node-to-node communication in LEACH-based WSNs. It utilized random-key predistribution technique to enhance the transmission security in the LEACH protocol along with symmetric-key cryptography in this protocol. FLEACH provides integrity, authenticity, confidentiality, and freshness in node-to-node transmission communication, but it is dangerous to node identifying attack. The authors of [17] proposed SLEACH, which is the first modified version of LEACH in regard to improving the security. They analyzed the security related problem while adding a cluster-based communication protocol for the WSN with various restricted resources. SLEACH gives security with the use of security protocol for WSN, message authentication code, and symmetric-key methods in the LEACH protocol. The proposed SLEACH defends against

hello flooding attacks and sinkhole and selective forwarding attacks. It prevents attackers from transmitting bogus sensor information to the cluster head and prevents the cluster head from transmitting a bogus message; meanwhile, SLEACH would forbid the crowded cluster in the time slot schedule, leading to DoS attack. Moreover, it reduces the throughput of the cluster head and does not provide data confidentiality.

Ibriq and Mahgoub [18] illustrated the secure hierarchical energy efficient routing protocol (SHEER), which provides secure communication in the network layer. It utilizes the probabilistic broadcast scheme and higher level hierarchical clustering to develop the network performance by creating efficient energy consumption which improves the network lifetime. To provide the security, the SHEER implements symmetric-key cryptography and a secure key transmission protocol called HIKES. The authors have analyzed the performances with the LEACH protocol and proved that the proposed SLEACH is efficient and significant. This protocol is dependent on the LEACH protocol, marked as authentication confidentiality cluster-based secure routing protocol. It employs both private and public key encryption using the digital signature cryptography. This protocol handles interior antagonists or attackers or compromised nodes. As a result of the greater computational demand with the use of public key cryptography, it is not significant for WSNs.

Sec-LEACH [19] is furnished as a significant solution for providing secure communication in LEACH. It utilizes TESLA and random-key predistribution for providing the dynamic cluster formation in the secure hierarchical WSN. Sec-LEACH utilizes random-key dispersion to LEACH with proposed symmetric key while one-way hash claims to give freshness and confidentiality. Sec-LEACH gives integrity, authenticity, confidentiality, and freshness to transmission communication. Sec-LEACH enhances the technique for selecting cluster heads and makes dynamic stochastic multidirectional cluster heads forms to transmit to the sink node. In this same mechanism, it would minimize the power efficiency and therefore the network lifetime has been improved. It utilized self-localization and key predistribution to transmit the data securely to the LEACH protocol. It prevented the compromised node from taking place in the WSN and maintained the secrecy of the data packet.

In [20], the author proposed RLEACH for secure transmission in the LEACH protocol, in which the clustering data have been organized dynamically and sporadically. In RLEACH, the orphan node issues arose as a result of random pairwise key mechanism so the authors have utilized enhanced random pairwise key mechanism to detect the attackers. RLEACH utilized symmetric, hash chain, and asymmetric cryptography to develop security in the LEACH hierarchical routing protocol. RLEACH resists multiple attacks such as sinkhole attack, Sybil attack, hello flooding attack, and wormhole attack.

3. Advanced Hybrid Intrusion Detection System

The proposed work aims to detect the hello flooding, wormhole, and Sybil attacks in the WSN by using the AHIDS. We utilize the enhanced LEACH protocol (with fuzzy rules) to identify the attackers of different types. AHIDS makes benefits from both anomaly detection and misuse detection models for the detection of the above said attacks. The proposed AHIDS can obtain a greater detection rate and low positive rate value. Meanwhile, it can find and include new instances by machine learning strategy of MPNN practically through enduring the unknown attacks. AHIDS proposed in this research contains two important elements as represented in Figure 5: the FFNN and the BPNN.

AHIDS first makes use of anomaly detection block in order to recognize the data packets as abnormal or normal. Later on, the misuse detection block covers the abnormal data packets to recognize the several types of attack detection [21]. Eventually, the effects of the two detection blocks are combined by the fuzzy block with MPNN in order to make a decision for identifying any intrusion and the different kinds of intrusion and bring back the same to the authority to protect the system from the attackers.

The anomaly detection models are generally utilized to recognize the abnormal packets for further detection of malicious nodes. Due to this, anomaly detection utilizes a standard method to detect the normal behavior of the nodes; a data packet is identified to be abnormal in the network once the present behavior changes from that of normal behavior. As an outcome, the anomaly detection generally identifies the common transmission as well as abnormal transmission of data packets, which forms the issues of classifying the erroneous nodes in the network. Nevertheless, it rarely considers an abnormal transmission as the normal transmission. Hence, the anomaly detection method is utilized to sort a huge number of data packets records first and make further detection analysis with the misuse detection method, whenever the amount of data is minimized.

IHIDS (Intelligent Hybrid Intrusion Detection System) and AIHIDS (Artificial Immune based Hybrid Intrusion Detection System) are similar, but the important difference between them is that IHIDS does not support artificial neutral network [22]. Hence, it cannot analyze and distinguish new intruders immediately while it suffers from the unknown assaults, whereas AIHIDS detects the attackers with the use of MPNN. The difficulty with the LEACH-based implementation is that the resources of the cluster head are less than the base nodes. Due to the higher number of resources in the base nodes, it does not have any restrictions while utilizing the resources. In case cluster heads take a lot of resources of performing and energy to identify intrusion, then the overall network lifespan becomes lesser. Hence, to minimize the workload of AIHIDS, there is no supervised learning of neutral network mechanism between the base node and cluster heads. The feedback mechanism is used for feeding the information of new assaults which is used for the learning process of AIHIDS. This corresponds to the misuse detection scheme of the proposed AHIDS for training the dataset.

This procedure not only obtains the AIHIDS but also gets the same performance of IHIDS which consumes some additional resources to detect the new attacks. When AHIDS

gets the feedback message from the learning mechanism of AIHIDS, the misuse detection model of IHIDS is retrained using the data of new attacks at the next training for adding new detection classes. Because the anomaly detection model, misuse detection model, and decision-making model in AHIDS are the same as those in IHIDS, the details of system structure are not described again.

3.1. Analysis on the Attackers

3.1.1. Detection of Sybil Attack. In Sybil attack, the attackers can get identities by two ways. At first, it has the ability to forge its own identities, for instance, forming an arbitrary identifier. Then, it applies stolen identities, which means spoofing the identities of legitimate nodes (masquerading) in the WSN. The proposed mechanism is developed for recognizing new identity formed by a Sybil attacker. We consider that the malicious node enters the network with its one identity and that the misbehaving nodes do not conspire with one another. We also considered that nodes do not increase or decrease their transmit power. The Sybil attack has the following effects on the WSNs [23]:

(i) The routing table size is elaborated in a WSN and it causes confusion in the data routing packets.

(ii) The Sybil attack interrupts the trust based mechanism in WSNs by decreasing or increasing the node's trust value.

(iii) Sybil attack produces confusion between illegitimate node and legitimate node in the WSN.

(iv) The wireless sensor network's life gets decreased due to the single node's reaction to the various nodes requests.

(v) The performance and throughput of the network are reduced significantly because of the Sybil attack.

To identify the Sybil attack, we propose the Advanced Sybil Attack Detection Algorithm (ASADA) with fuzzification method along MPNN; it is utilized to separate the Sybil node and the legitimate node even if it has the highest mobility through the verification process. The AHIDS absorbs each node RSSI value in the table with respect to the time period, and it analyzes whether the first RSSI value is lesser than threshold or not. If not, AHIDS includes it to the attacker list and updates its neighbors' list. Due to the battery restrictions, every sensor node maintains only 5 lists. Figure 2 shows a scenario of Sybil attack in WSN.

The proposed ASADA is combined with the rule based anomaly detection module. In this mechanism, the anomaly detector utilizes fuzzy rules set to differentiate data units as normality or anomalies. While supervising the WSN, these fuzzy rules sets are chosen appropriately and employed to the supervised data. If the fuzzy rules are satisfied in determining, an anomaly is announced. The ASADA, the underlying detector, is compiled into four processes, towards observing Sybil attacks in the wireless sensor networks. In this first process, nearby nodes identify the path for the data transmission, utilizing the range-enabled scheme [3] which

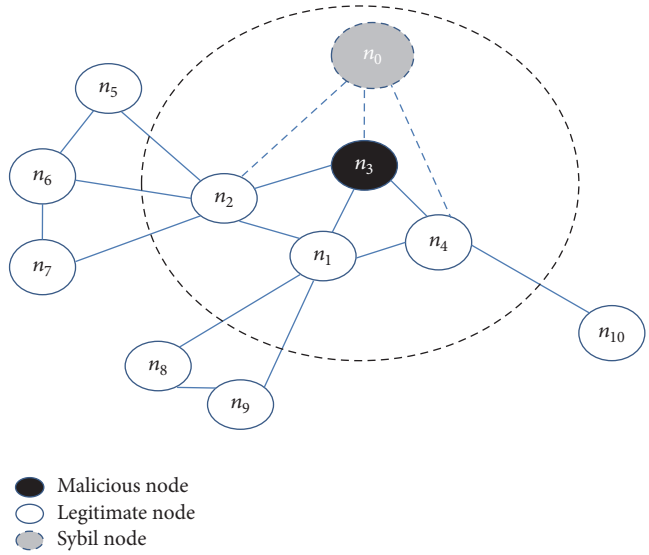

Figure 2: Sybil node detection analysis.

sends hello packets to the neighbor nodes (which are also called beacons). The data packets are utilized within the particular range in order to receive the effective RSSI signal; if they cross a certain distance or range, then the signal strength becomes weaker which has the possibility of getting affected by the malicious nodes, so we include the ranging estimation scheme. In this scheme, each packet has the PHY header (PHR) with particular bit which is called the ranging bit; moreover, each packet broadcasts the PHY for the frames sets meant for ranging [3].

In the next phase, each node develops the table comprising the locally calculated ranging estimation; that is, at first, it calculates the distance d_{ab}^n from every neighboring node it identified. Here, we consider that d_{ab}^n represents the detected distance between the node n_a and the node n_b as calculated by the node n_a. Nevertheless, the distance detection may not be error-free, and it may contain ranging error, which is indicated as e error units, which happens because of the wireless network of the ranging communication and the imperfections of the fundamental PHY and because of the misbehavior node performing a distance increasing or decreasing attack. Therefore, by d_{ab}^e, we represent the exact distance between the node n_a and the node n_b. Evidently, it applies that $(d_{ab}^n - n/2) < d_{ab}^n < (d_{ab}^n + n/2)$ at average for each node, n_a, n_b.

In this next process, every node in the WSN severally executes multiple distance matching verification. This indicates that node n_a equates the ranging measurements of every possible pair of nodes n_a and n_b, represented in its neighbor node list; that is, for all $b, c \neq a$, $1 \leq b$,

$$\text{If } \begin{cases} |d_{ab}^n - d_{ac}^n| < e, & \text{then rasie an alarm} \\ |d_{ab}^n - d_{ac}^n| \geq e, & \text{else continue normal operation.} \end{cases} \quad (1)$$

With the above conditions, the rules set that in case node n_a determines that two nodes other than trenchant node, represented by n_b and n_c, have a difference in distance smaller

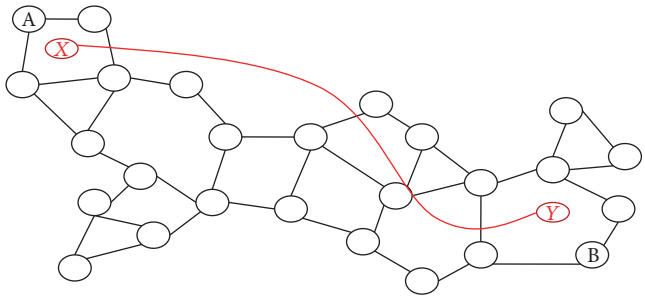

Figure 3: Construction of wormhole tunnel.

than e quadratic metric units, then the node performing the distance verification considers that a Sybil attack is active and continues with the procedure of identifying the blacklisting of nodes n_b and n_c. As evident, this premise could produce a false (positive) value in the fuzzy table set 1; the two distance matching nodes, n_b and n_c, are legitimate sensor nodes. Accordingly, the network performance and the applicability are based on the false probability [24]. Therefore, the analytic framework has been developed to enhance the accuracy of the detection mechanism.

Under this condition, it is very essential to describe that the third process of the proposed algorithm is a repeating process, intending that distance checks are performed sporadically. The time period in which each node runs circular based Sybil attack detection algorithm is based on the fuzzy set rules with neural network. Each sensor node moves to the neighbor route discovery seeking for the fresh neighbors in its locality. Each time a wireless sensor node finds older or fresh neighbors, it rejoins the distance checks. This process also sets the requirements to ensure that distance verifications are invariably upgraded between the freshly added neighbor and every other older node in the neighbor list, based upon the distance, and the threshold point of the fuzzification is used to determine the percentage of the Sybil attackers.

3.1.2. Detection of Wormhole Attack. The specific attack during the routing functionality in the wireless networks, referred to as the wormhole attack, has been proposed in the context of ad hoc networks [25]. When the attack is active, a misbehavior node can absorb one data packet from one location in the wireless network and "tunnel" it to some other assaults node at a particular point, which reproduces it locally. The tunnel would be demonstrated in various manner paths, such as through an out-of-band hidden channel (e.g., wired link), high powered transmission, or data packet encapsulation [26]. This channel tunnel builds the tunneled data packet that would come either faster or with minimum number of hops while equating to the data packets carried over pattern multihop routes. This produces the delusion that the two end points of the tunnel are very near to each other. The wormhole attack is shown in Figure 3.

A wormhole tunnel can be generally practicable if utilized for transmission of all the data packets. Nevertheless, in its misbehavior incarnation, it can be utilized by the two misbehavior end points of the wormhole tunnel to enter traffic congestion during the routing which affects all routes through them. The misbehavior nodes end points may then introduce different types of attacks which results in the traffic congestion occurring in the wormhole. Therefore, the wormhole attack would influence the route established by protecting any two sensor nodes in the wireless network that are much bigger than two hop nodes away from exposing routes to each other. The wormhole attack may influence various applications and energy utilization in wireless ad hoc networks such as clustering protocols, data aggregation, and location based wireless network systems [25]. At last, the wormhole attack is regarded as especially pernicious as it can be established without experiencing access to any legitimate node in the network.

To identify the wormhole attack, we propose the Wormhole Resistant Hybrid Technique (WRHT) with fuzzification method along FFNN. The proposed technique WRHT is a hybrid technique based on the concept of watchdog [26] and Delphi [27]. Watchdog (packet drop) and RTT based technique Delphi are based on the assumption that the packet drop and RTT of a route in the network are very closely related to the value of its hop count (HC) and distance. WRHT makes use of the information about the packet drop, the delay per each hop, and the complete route in the sensor network. The foundation behind WRHT is to build up a wormhole detection methodology that is able to manage every category of wormholes, which is possible for every type of WSN device and scenarios of the network, without the earning of significant computational costs. WHRT is considered as an extension to routing protocol. The proposed WRHT allows the source node in the sensor network to calculate the wormhole presence probability (WPP) for a path in addition to HC information. During packet encapsulation in wormhole attack, the packets are transmitted via the legitimate path only; the packet that reaches a colluding node is encapsulated so that the nodes on the way are not able to increase the hop count. When the packet reaches the other colluding node at the receiving end, this node then decides whether to drop the packet or retransmit it in the network. Since WRHT makes use of dual mode detection by calculation of PLP and TDP, if it finds out packet loss at the receiving end, then it concludes that the wormhole attacker is working in encapsulation mode (hidden mode).

The following formulas are used for calculating the presence of the wormhole:

$$\mathrm{TDP}_{\mathrm{HTOTAL}} = \mathrm{TDP}_{\mathrm{HRREQ}} + \mathrm{TDP}_{\mathrm{HRREP}}, \tag{2}$$

where $\mathrm{TDP}_{\mathrm{HRREQ}}$ is the time delay probability of a node during RREQ and $\mathrm{TDP}_{\mathrm{HRREP}}$ is the time delay probability of a node during RREP,

$$\left(\mathrm{TDP}_P\right) = 1 - \left(\prod_{j=1}^{n}\left(1 - \mathrm{TDP}_j\right)\right), \tag{3}$$

where TDP_j is the time delay probability measured at node j,

$$\left(\mathrm{PLP}_P\right) = 1 - \left(\prod_{j=1}^{n}\left(1 - \mathrm{PLP}_j\right)\right), \tag{4}$$

where PLP_j is the packet loss probability measured at node j.

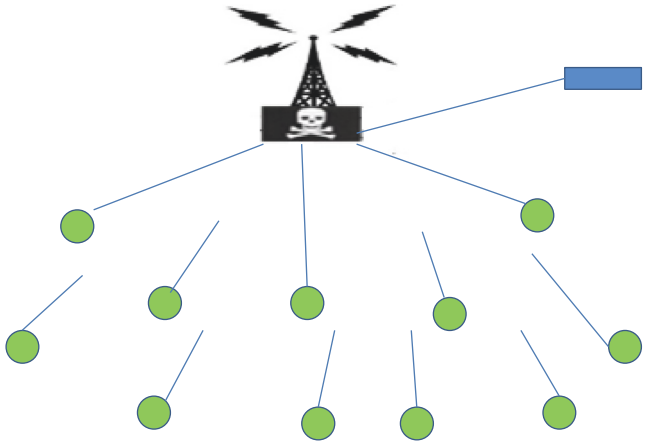

Figure 4: Hello flooding attack in WSN.

Since the two events, time delay and packet loss, are not mutually exclusive (as there may be loss of packets and time delay at the same time), the wormhole presence probability (WPP) for a path can be defined as

$$\text{WPPp} = \text{TDP}_P + \text{PLP}_P - (\text{TDP}_P \text{ and } \text{PLP}_P). \quad (5)$$

Here, the calculated values of (2)–(5) are moved to the FFNN. The fuzzy interface in the fuzzy based detector module uses both anomaly and misuse detectors in order to estimate the wormhole attack in the adversary model in AHIDS. Here, malicious nodes are detected and stored as blacklisted.

3.1.3. Detection of Hello Flooding Attack. The hello flooding attack works as an assaults node disseminates hello packets by applying a more powerful transceiver than common sensor nodes. The attack is shown in Figure 4. The wireless sensor nodes obtaining such hello packets may incorrectly consider that they are inside the RSS of the transmitter and attempt to transmit their data packets through the misbehavior nodes. These packets would be lost as they may not reach the destination sensor nodes. RSS can be estimated by the nearest neighbor of a misbehaving node as this RSS is effectively higher than the signal received from other neighbors [7].

To minimize the communication overhead of the data packet in the previous RSS established methodology, in this paper, we consider the clustered based wireless sensor network, based on the RSS and distance threshold of the elected cluster head nodes. The distance of nodes is estimated by the following:

$$\text{Dist} = \text{sqrt}\left[\text{sq}(x2 - x1) + \text{sq}(y2 - y1)\right]. \quad (6)$$

Here, $(x1, y1)$ represent the location coordinates of the destination node that is receiving packet, while $(x2, y2)$ are the CH location coordinates that are sent through advertising hello packet. Receiving nodes calculate RSS threshold value TRSS, which corresponds to each node radio range in WSN. Receiving nodes also calculate the value for distance threshold (TDIST), which corresponds to the radio range distance covered. Each sensor node joins a CH if

$$(\text{RSS} < \text{TRSS}) \;\&\&\; (\text{Distance} < \text{TDIST}). \quad (7)$$

Here, sensor nodes RSS and distance along with their threshold values are moved to the BPNN. The fuzzy interface in the fuzzy based detector module uses both anomaly and misuse detector in order to estimate the hello flooding attack in the adversary model in AHIDS. Here, the trusted neighbor nodes are instructed to flood a fixed number of fake packets into the sensor network at the same time. If the suspicious node passes this test, then it is directed to send-received check. If it fails this test, then the node is considered as malicious and stored as blacklisted. AHIDS utilize the fuzzy based MPNN, which contains the FFNN and BPNN of supervised learning approach in order to identify the all three attackers with the help of fuzziness rules set.

3.2. To Detect the Malicious Nodes in the Advanced Hybrid Intrusion Detection System. In this paper, we consider a clustered based WSN; it is very important for the data packets to demonstrate the common patterns of normal node behavior for supervising the condition of the data packets. Hence, in this paper, the fuzzy rule based analysis is utilized to develop the anomaly detection scheme and the representing rules are determined by the experts. The work flow model can be explained in three steps, which are represented below.

Process 1. It evaluates the data packet transmission history completely. In a cluster-based wireless sensor network, the data packets move through the base node and are forwarded from the neighbor of cluster heads to the MPNN, in which they moved to FFNN. Hence, the previous data packets that communicate on the base node are gathered to evaluate, and the data packet is classified into two types, that is, abnormal and normal.

Process 2. This process is used to select the feature set, looking for recognition of the key elements that emerged to separate the abnormal and the normal packets.

Process 3. This process includes the establishement of anomaly intrusion detection rules. It depends on the resolution of a common data packet and it chooses the best features, and then the fuzzy based rules are produced. Later on, the BPNN along with well-known rules sets is stored in the knowledge base.

In clustered based wireless sensor networks, when all clustered heads transmit the data to the base nodes, entire data packets which pass through the base nodes have to be checked by the anomaly detection method to find whether there are any abnormal data packets. In case such abnormal data packets are identified, they should be moved to the second process, in which the misuse detection method appears for any misjudgments that have occurred using the fuzzy based Multilayer Perceptron Neural Network which will distinguish the attackers and provide detection ratio.

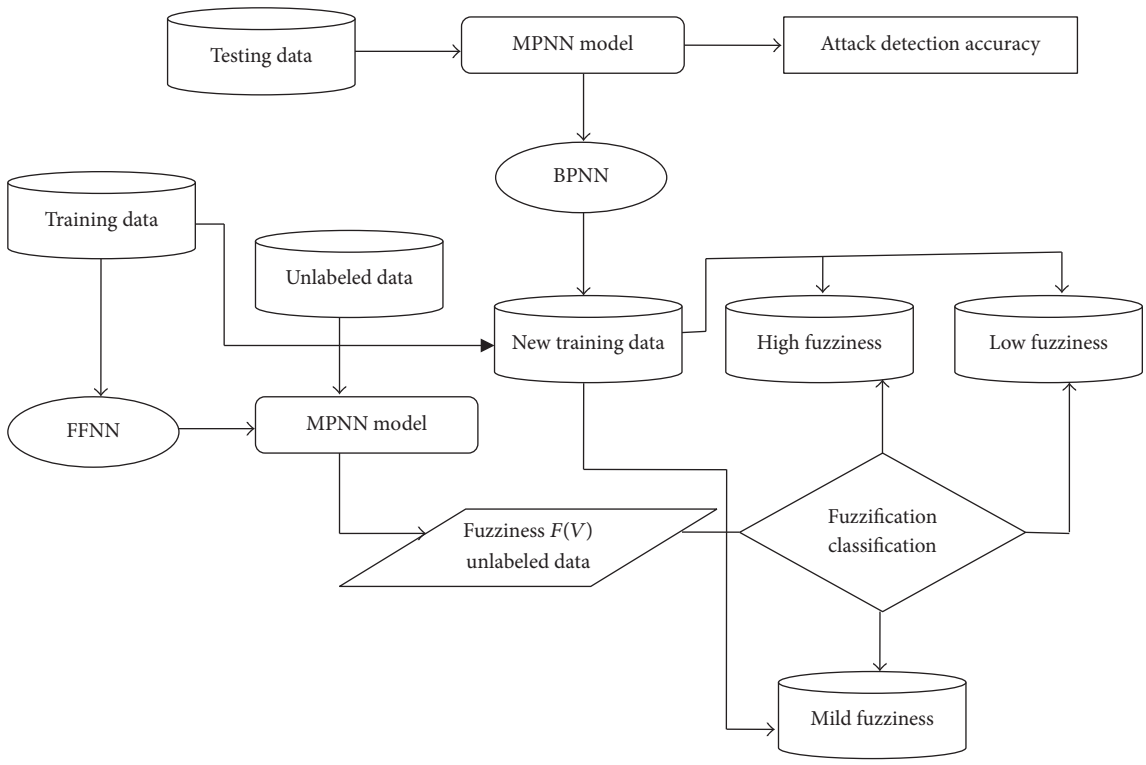

Figure 5: The proposed methodology.

3.2.1. Modules Description

(1) Fuzziness. The word fuzziness connects to the unclear boundary value limits considering two important linguistic factors and it is dependent on the fuzzy sets and membership function. It was first discovered by Zadeh [28] in 1965. Later on, fuzziness was defined as the quantitative measure of uncertainty with 1 nonprobabilistic entropy by the author Shannon (Shannon's information entropy). They also introduced three important properties that fuzziness should contain. These properties would describe the fuzziness; the fuzziness degree must reach its maximum value as the membership degrees of each and every attribute are equal and its minimum value as each and every attribute either denotes the fuzzy set or utterly not. In this proposed study, we consider fuzziness as a type of cognitive uncertainty in the neutral network, determining the transition of uncertainty from one linguistic condition to another, whereas a linguistic condition is defined as a fuzzy set in a certain universe of discourse. The fuzziness of a fuzzy set can be evaluated by a function $F \to [0,1]X$ satisfying the following axioms [29]:

(1) $F(\mu) = 0$ if and only if μ is a crisp set.

(2) $F(\mu)$ obtains its maximum value if and only if $\mu(x) = 0.5\ \forall x \in X$.

(3) If $\mu \leq s^{\sigma}$, then $F(\mu) \geq F(\sigma)$.

(4) $F(\mu) = F(\mu')$, where $\mu'(x) = 1 - \mu(x)\ \forall x \in X$.

(5) $F(\mu \cup \sigma) + F(\mu \cap \sigma) = F(\mu) + F(\sigma)$.

(2) Fuzzy Based Detector Model. The anomaly detector and misuse detection methods use several methodologies of well-established attack behaviors, so that we develop the new strategy to overcome or defend against these attacks behaviors [30]. Most of the intrusion detection techniques promise to detect the attacks through the training data, but they fail uncertainly. The proposed work is based on MPNN, consisting of FFNN along with BPNN, and is applied in this study in order to provide the highest detection rate in the supervised learning approach. The proposed methodology demonstrated figures outside the corresponding relationship between input and output variables, and that matches the corresponding weight. It can minimize the error rate that occurs in the interface for obtaining the greatest accuracy. Hence, we proposed fuzzy based FFNN and BPNN to obtain the highest accuracy level in the detection of the attacks for the clustered based AHIDS through massive training.

In this research, multiple-layer perception in the neutral network is utilized for the detection strategy mechanism of AHIDS that admits a hidden layer, an input layer, and an output layer. In the FFNN process, all the performances parameters are determined and the error rate is estimated by applying this formula

$$e_{r_i} = d_i - a_i. \tag{8}$$

Here, d_i denotes the desired output and a_i denotes the actual output which resulted from the MPNN. In the back propagation process, the error rate or signal is propagated

by the MLP network. Since the proposed methodology integrates the anomaly detection and misuse detection scheme, we use abnormal packets, which were determined by the anomaly detection scheme, as the input layer. The number of performing units in input vector is decided by the selected characteristics of the data packets. Furthermore, the number of performing units is included in the hidden layer which is developed by increasing the amount of output layers and the input layers. Performing units in the output layer provide various attacks and a single normal behavior of the node to decide whether the inserted packet is an attacker or intrusion that forms a classification.

The overall complete details of the data packets are gathered, which move towards the base nodes in clustered based wireless sensor networks, as the common data for training. The majority of the data packets are normal in clustered based wireless sensor networks, which makes the training data imbalanced. On the other hand, the abnormal data packets are eliminated by FFNN because of their minimum occurrence ratio. Therefore, to avoid such issue, the training data are percolated through the anomaly detection scheme at first; later on, the abnormal data are distinguished, which have been obtained from the training. Before forwarding to the training data to BPNN, the training data were generalized into an identical form of BPNN. On the other hand, the data packet records are converted into a stream binary value and then set to BPNN. To obtain good convergence, the detection rate is kept at 0.1 to 1.0. The actual learning ratio is obtained from the simulation. Furthermore, we allocate values from the range of 0 to 1 as the biases and weights haphazardly.

After the training data are incorporated into the BPNN, we equate the actual output results through the mechanism of the FFNN. The error and rectification value of hidden and output layers are estimated through the mechanism of the back propagation in the MPNN. To modify the biases and weights of networks, unless all the training data have been utilized, such duration is called the epoch. The training data would be discovered continuously and organize the weights according to the layers frequently with the help of the epochs, unless the output layer value is the same as the target value and then the training data is finished.

Hence, complete abnormal packets are identified by the anomaly detection scheme and then, for further verification, they are forwarded to misuse detection scheme. At first, we apply the preprocessing step to covert the abnormal packets into a binary value and then the binary value is forwarded to the misuse detection scheme to estimate the output value. At last, the outcome of the detection value is delivered to the fuzzy module with MPNN model in order to obtain the best integration.

The fuzzy module is utilized to make the best decision-making in order to identify the attackers and their different types of attack by integrating anomaly detection scheme and misuse detection module. The fuzzy rule based mechanism is utilized to support the decision-making model, by applying the rules to aggregate the outputs of the two detection schemes, and the major merit of this study is to obtain fast and accurate results. The fuzzy based rules are given in the tabulation. This mechanism operates using fuzzy logic controller; first, the input parameters (FPNN) are assigned in the fuzzification process and these parameters move to the Fuzzy Inference System (FIS). FIS performs based on the fuzzy membership (triangular) and the fuzzy rule that are applied on the input parameters to determine the suitable fuzziness to determine the attackers types. The fuzzy sets considered for the input parameters are very low, low, medium, high, and very high, and this is represented in Table 1, and the hidden layer input (BPNN) is given as very short, short, medium, long, and very long, and this is presented in Table 1. Thus, these parameters are analyzed in FIS that checks the fuzzy rules and functions for producing the results to defuzzification where the output parameters are extracted as low fuzziness (Sybil attack), mild fuzziness (wormhole attack), and high fuzziness (hello flooding attack).

Table 1: Fuzzy rules based MPNN.

FFNN	BPNN	Fuzziness
Very high	Very long	Mid fuzziness
Very high	Long	Mid fuzziness
Very high	Medium	Low fuzziness
Very high	Short	Low fuzziness
Very high	Very short	Low fuzziness
High	Very long	Mid fuzziness
High	Long	Mid fuzziness
High	Medium	Mid fuzziness
High	Short	Low fuzziness
High	Very short	Low fuzziness
Medium	Very long	High fuzziness
Medium	Long	High fuzziness
Medium	Medium	Mid fuzziness
Medium	Short	Low fuzziness
Medium	Very short	Low fuzziness
Low	Very long	High fuzziness
Low	Long	High fuzziness
Low	Medium	Mid fuzziness
Low	Short	Mid fuzziness
Low	Very short	Mid fuzziness
Very low	Very long	High fuzziness
Very low	Long	High fuzziness
Very low	Medium	High fuzziness
Very low	Short	Medium
Very low	Very short	Medium

4. Multilayer Perceptron Neural Network (MPNN) Model Supervised Learning

The MPNN model is categorized into FFNN and BPNN and is used to estimate the detection accuracy of the three different attackers mentioned above in this paper. The attackers are improving day by day due to the development of advanced technology; hence, it is very necessary to improve the existing Intrusion Detection System as well as the system capacity. To overcome such issues, our proposed AHIDS is an advanced

intelligent detection system. When the system identifies the new types of attacks, machine learning mechanism has the capacity to identify and learn them. Nevertheless, the data packets cannot be accurately assorted by misuse detection model, which would be noticed as an unknown assault. Furthermore, these data packets would be transmitted to the MPNN to understand and introduce the new type of detection system for identifying the different types of attacks.

The proposed methodology is provided in Figure 5. We adopt the MPNN to develop the FFNN and BPNN mechanism of IHIDS, because these neutral networks could manage with a huge number of data to continue the system stability and they have the capacity to listen to different types of attackers. On the other hand, FFNN would progress with detection and estimate the new types of attacks simultaneously. The proposed BPNN is utilized to cluster unknown attacks for our MPNN supervised learning mechanism that incorporates an input layer, a hidden layer, and an output layer. The pattern of the supervised learning system is represented in Figure 6. In the misuse detection, a scheme cannot detect exact attacks from the data packets, because input layer and the number of input nodes are decided through the selected features for the data packets. The number of output nodes is found at the starting stage. Therefore, various kinds of clusters would be produced by using the proposed fuzzy based MPNN. Hence, the output nodes results are improved, when each output node establishes a fresh type method to detect the attackers.

Each data packet of unknown attackers is inserted to the artificial supervised learning mechanism in order to estimate the corresponding points for each output result. Later on, it detects the winning output node results to estimate the corresponding value of winning output node. If this value is higher than the vigilance value, this indicates that the inserted packets correspond to the output node; hence, it belongs to clusters and MPNN just has to modify the weights. On the other hand, when the corresponding value of the winning output node is lesser than the alertness value, this indicates that the inserted data packet is not equal to the connected weight; therefore, it does not match this cluster. It has to detect the next winning node results to check whether it can pass the alertness test or, else, it would produce a fresh output result node which means a fresh attack has been identified. Furthermore, to determine the desirable vigilance value, it is examined by the sample data through the experimental simulation. In order to include fresh detection classes, the information about cluster is carried to retrain the MPNN of the misuse detection scheme while the cluster member values obtain the defined threshold.

4.1. Fuzzy Rules Set Based Multilayer Perceptron Neural Network. The proposed methodology of the fuzzy based rules in the MPNN supervised learning is described in Table 1. From the given dataset of labeled examples, a dataset of unlabeled examples, and a testing dataset, the data are train using supervised FFNN classifier by applying the 223 hidden nodes. The hidden node is applied with BPNN supervised classifier in order to get the final output as the sigmoid activation algorithm. Then, as membership 223 vector V is achieved on every unlabeled sample by analyzing U applying MPNN supervised learning method, the membership vector of each 224 unlabeled sample that is produced throughout this process is further applied to get the fuzziness $F(V)$ by using

$$F(V) = -\frac{1}{n}\sum_{i=1}^{n}\left(\mu_i \log \mu_i + (1-\mu_i)\log(1-\mu_i)\right), \quad (9)$$

where $V = \{\mu_1, \mu_2, \ldots, \mu_n\}$ is a fuzzy set.

The fuzziness value is further classified into three different groups: low fuzziness group, high fuzziness group, and mid fuzziness group. Those samples which denote the high fuzziness and low fuzziness groups are extracted, and these groups are further included with T_r to get a revised dataset T_{r_new} for training the FFNN and testing it using BPNN. This is represented in Figures 5 and 6.

5. Results and Discussion

In this approach, we utilize the KDD datasets to coordinate the pattern. To determine the clustered based wireless sensor network, we have introduced an efficient training MPNN for minimizing the energy utilization by reducing the variable size dummy packets. Therefore, the dummy packets are removed from the network during the preprocessing stage, which can improve the strength of the data utility. Thus, the size of the dummy variable packet is varied below or above the normal data packets, to reduce the energy utilization. This will finally make the adversary model separate the data packets between the legitimate packets and a fake packet, and it does not provide the data about the actual size of the real packets; however, the proposed methodology provides several benefits to improve the data packets security and to minimize the energy consumption in the wireless sensor networks in the AHIDS.

The performance of the proposed AHIDS can be estimated by applying the following:

(1) Accuracy

$$\text{Acc} = \frac{\sum_{i=1}^{C} \text{TP}_i}{N}. \quad (10)$$

(2) Recall

$$\text{Recall} = \frac{\text{TP}_i}{\text{TP}_i + \text{FN}_i}. \quad (11)$$

(3) Average accuracy

$$\text{AAcc} = \frac{1}{C}\sum_{i=1}^{c} \text{Recall}_i. \quad (12)$$

(4) Precision

$$\text{Precision}_i = \frac{\text{TP}_i}{\text{TP}_i + \text{FP}_i}. \quad (13)$$

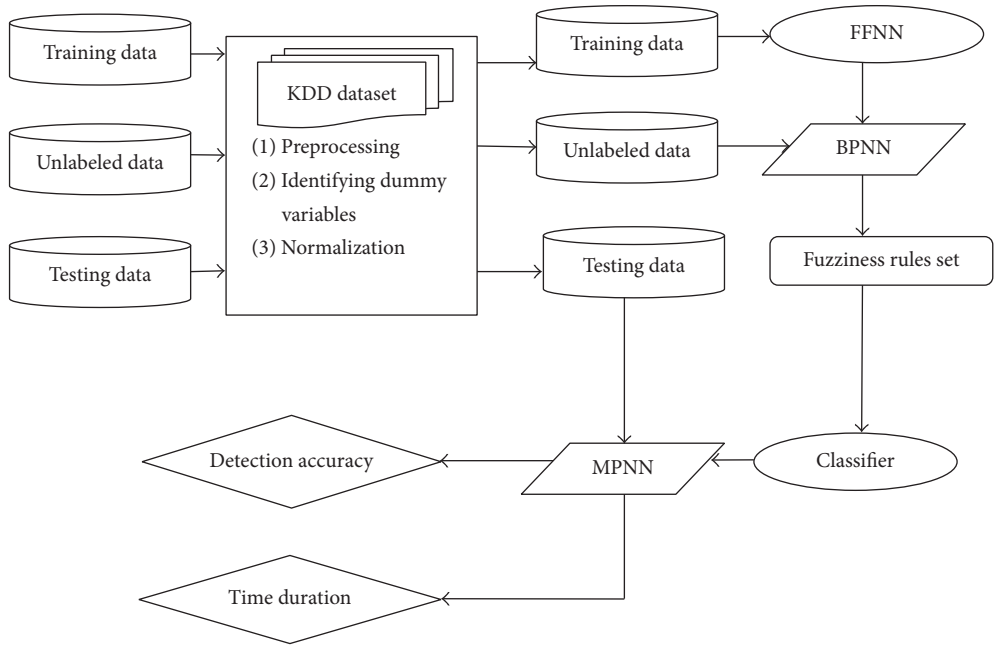

Figure 6: Fuzziness based MPPN.

(5) F-measure

$$\mathrm{FM}_i = \frac{2 \cdot \mathrm{Recall}_i \cdot \mathrm{Precision}_i}{\mathrm{Recall}_i + \mathrm{Precision}_i}. \tag{14}$$

(6) Attacker accuracy

$$\mathrm{Attacc} = \frac{1}{C-1} \sum_{i=2}^{c} \mathrm{Recall}_i. \tag{15}$$

(7) Attacker detection rate

$$\mathrm{Adr} = \frac{\sum_{i=2}^{c} \mathrm{TP}_i}{\sum_{i=2}^{c} \mathrm{TP}_i + \mathrm{FN}_i}. \tag{16}$$

Here, C denotes the number of classes, N stands for the number of examples, TP_i is the number of true positive values of the ith class, FP_i is the number of false positive values of the ith class, and FN_i is the number of false negative values of the ith class.

6. Simulation-Based Implementation and Experimental Results

In this experimental setup, we evaluate the performance of the proposed AHIDS in the wireless sensor network by using the NS2 network simulator version 2.33 (NS2.33) with parameters of the simulation used defined in Table 2.

We estimate the different types of attackers such as hello flooding, wormhole, and Sybil attacks and their detection accuracy for the wireless sensor networks in the AHIDS with fuzzy rules based MPNN. In Table 3, the results demonstrated that the misbehavior nodes are detected in the true positive rate (TPR) and false positive rate (FPR), which is detected with the MPNN using fuzzy logic mechanism. For instance, out of 100 nodes, 23.33% of the nodes are determined as misbehaving nodes which have cut down the data passing through them. The obtained results have proved that the proposed fuzzy logic mechanism is able to identify the misbehavior nodes in the system with higher positive ratio and lower false positive rate. Table 3 illustrates detection rates under each level of node speed. Table 4 represents the detection rate and false negative for the attack of hello flooding, wormhole, and Sybil.

We first deploy WSN by defining the base station (BS) and clusters with each having a cluster head (CH). As shown

Table 2: Simulation parameters.

Parameter	Value
Simulator used	NS 2.3
Area (meters)	1600 × 900
Number of nodes	42
Routing protocol	DSDV
Channel type	Wireless
Packet size	512 bytes
Initial energy of nodes	10 joules

Table 3: Detection rate.

TPR	FPR
55% (mid fuzziness)	5% (low fuzziness)
57% (mid fuzziness)	12% (low fuzziness)
63% (high fuzziness)	17% (low fuzziness)
77% (high fuzziness)	20% (low fuzziness)

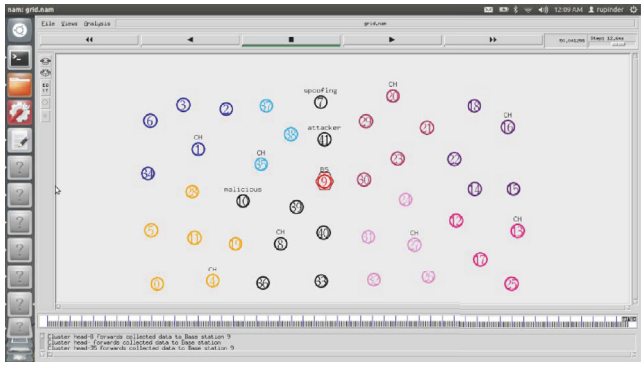

Figure 7: Detection of hello flooding, Sybil, and wormhole attacks.

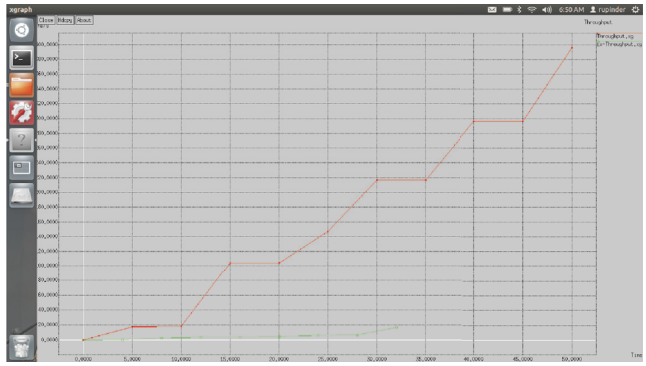

Figure 8: Throughput of WRHT.

Table 4: Detection ratio and false negative rate for three attackers.

Attack	Detection rate	False negative
Sybil attack	99,40%	4,12%
Hello flooding attack	98,20%	2,22%
Wormhole attack	99,205%	5,16%

in Figure 7, node 9 is the BS with nodes 1, 4, 8, 13, 16, 20, 27, and 35 as CH. Figure 7 provides a scenario of the sensor network having node 10 as selfish node (i.e., hello flooding node). Node 10 is dropping packets and is detected as the hello flooding attacker by the proposed AHIDS. Node 7 and node 41 as shown in Figure 7 are detected as Sybil and wormhole attacks by AHIDS. These malicious nodes 7, 10, and 41 are isolated from the network for the normal function of WSN by AHIDS.

6.1. Throughput of AHIDS. In the first experiment, we measure the sensor network throughput as this is one of the crucial network parameters. Network throughput is defined as the average successful rate of delivered packets. Throughput is calculated depending on the total number of received packets at the destination in sensor network per unit of time. Throughput is calculated as

$$\text{Throughput} = \frac{(\text{Total number of received packets at destination})}{(\text{simulation time})}. \quad (17)$$

Figure 8 shows the throughput analysis in the case of the sensor network under attack and after implementation of AHIDS. The figure clearly shows that the proposed technique after the isolation of the attacks results in the increase of throughput.

6.2. Packet Delivery Ratio of WRHT. Packet delivery ratio (PDR) is defined as ratio of the total received packets at the destination to the total packets generated by source node. PDR is calculated as

$$\text{PDR} = \left(\frac{\text{Packets received}}{\text{packets generated}}\right) * 100. \quad (18)$$

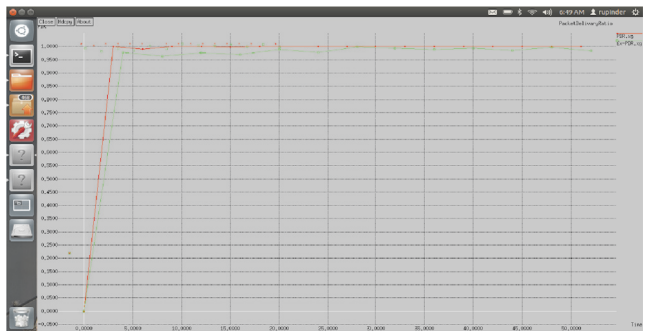

Figure 9: PDR of WRHT.

Figure 9 shows the PDR analysis in the case of the sensor network under attack and after implementation of AHIDS. The figure clearly shows that the proposed technique after the isolation of the attacks results in the increase of PDR. A high value of PDR is an indication that there is less packet loss in the sensor network.

6.3. Energy Consumption of AHIDS. For the energy computation of sensor nodes, we assign initial value of 10 joules at the beginning of the simulation. This energy is termed initial energy. In simulation, the variable energy is used to represent the energy level in a sensor node at any specified time. The value of initial energy is passed as an input argument. A sensor node loses a specific amount of energy for every packet being transmitted and received. As a result of this, the value of initial energy in a sensor node gets decreased. The energy consumption level of a sensor node at any time of the simulation is determined by finding the difference between the current energy value and initial energy value. If an energy level of a sensor node reaches zero, it cannot transmit or receive any more packets. Figure 10 shows that the AHIDS reduces the energy consumption as compared to the attacking scenario of the sensor network.

6.4. Packet Loss of AHIDS. Packet loss is defined as the difference between the packets generated by the source node

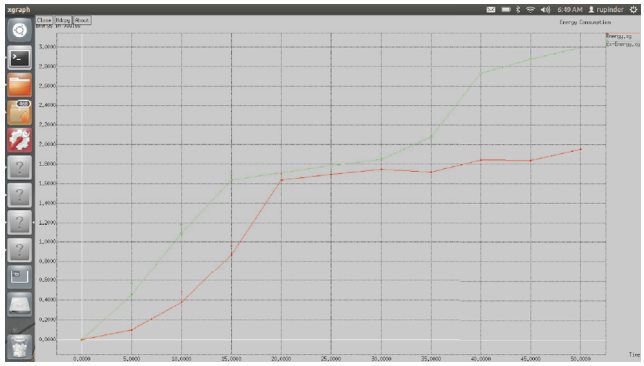

Figure 10: Energy consumption of AHIDS.

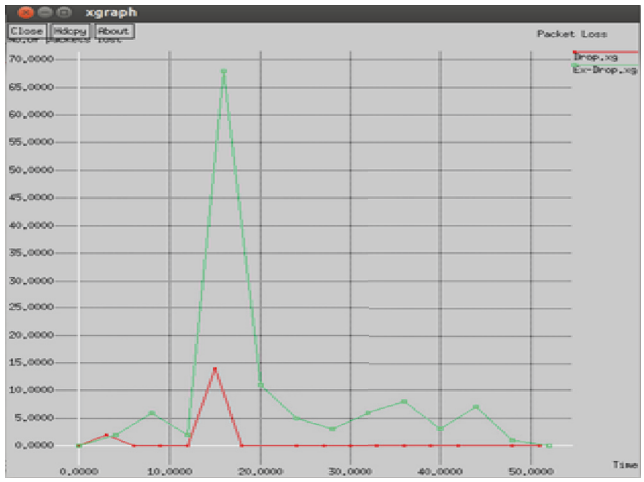

Figure 11: Packet loss of AHIDS.

and the number of packets received by the destination node. Packet loss is calculated as

$$\text{Packet Loss} = \text{Generated Packets} - \text{Received Packets}. \quad (19)$$

Figure 11 shows the packet loss analysis in the case of the sensor network under attack and after implementation of AHIDS. The figure clearly shows that the proposed technique after the isolation of the attacks results in the decrease in packet loss. A smaller value of packet loss is an indication that there is high PDR in the sensor network.

6.5. Intrusion versus Membership. Figure 12 represents the relationship between the intrusion detection in the network and the membership function of AHIDS.

7. Conclusion and Future Works

In this paper, we provide a combined defence mechanism against hello flooding, wormhole, and Sybil attacks in wireless sensor networks. An Advanced Hybrid Intrusion Detection model is proposed for wireless sensor networks which makes use of both anomaly detection and misuse detection for the

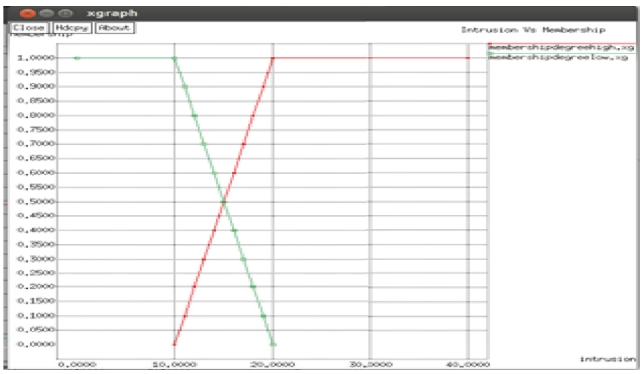

Figure 12: Intrusion versus membership of AHIDS.

detection of attacks. The proposed Advanced Hybrid Intrusion Detection System utilizes a Multilayer Perceptron Neural Network, which contains Feed Forward Neural Network and Backpropagation Neural Network of the supervised learning approach based on the fuzzy logic mechanism with anomaly and misuse detection technique to detect the hello flooding, wormhole, and Sybil attacks. The combination of these two techniques is used to provide an Advanced Hybrid Intrusion Detection System with a high detection rate and low false positive rate. The detection mechanism is incorporated in a cluster-based topology with LEACH protocol, to decrease communication costs and energy consumption, which leads to an increase in the network lifespan, improving the lifetime of the network. The simulation results show that the proposed Intrusion Detection System is capable of attaining high true positive rate and low false positive rate. The results also prove that the proposed system is highly efficient for the parameters of throughput, packet loss, energy consumption, PDR, and so forth. For the future work, more analysis on this topic is required to be undertaken with detailed simulation of different attack scenarios to evaluate the performance of the proposed work.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Acknowledgments

The authors are highly thankful to the Department of RIC, I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India, for providing the opportunity to conduct this research work.

References

[1] Y. Maleh, A. Ezzatib, Y. Qasmaouic, and M. Mbidac, "A global hybrid intrusion detection system for wireless sensor networks," *Procedia Computer Science*, vol. 52, pp. 1047–1052, 2015.

[2] S. Shamshirband, N. B. Anuar, M. L. M. Kiah et al., "Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 42, pp. 102–117, 2014.

[3] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information," *Expert Systems with Applications*, vol. 42, no. 21, pp. 7560–7572, 2015.

[4] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," *Expert Systems with Applications*, vol. 29, no. 4, pp. 713–722, 2005.

[5] Y. Shen, S. Liu, and Z. Zhang, "Detection of hello flood attack caused by malicious cluster heads on LEACH protocol," *International Journal of Advancements in Computing Technology*, vol. 7, no. 2, pp. 40–47, 2015.

[6] S. K. Saini and M. Gupta, "Detection of malicious cluster head causing hello flood attack in LEACH protocol in wireless sensor networks," *International Journal of Application or Innovation in Engineering & Management*, vol. 3, no. 5, pp. 384–391, 2014.

[7] S. Magotra and K. Kumar, "Detection of HELLO flood attack on LEACH protocol," in *Proceedings of the IEEE International Advance Computing Conference (IACC '14)*, pp. 193–198, Gurgaon, India, February 2014.

[8] V. K. Arora, "A survey on LEACH and other's routing protocols in wireless sensor network," *International Journal for Light and Electron Optics*, vol. 127, no. 16, 2016.

[9] T. M. Rahayu, S.-G. Lee, and H.-J. Lee, "Security analysis of secure data aggregation protocols in wireless sensor networks," in *Proceedings of the 16th International Conference on Advanced Communication Technology*, pp. 471–474, February 2014.

[10] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks*, vol. 2, no. 4, pp. 500–528, 2006.

[11] Y. Lee and S. Lee, "A new efficient key management protocol for wireless sensor and actor networks," *International Journal of Computer Science and Information Security*, vol. 6, no. 2, 2009.

[12] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[13] M. Hongbin, W. Yingli, Y. Shuang, Y. Hai, and L. Zhenhai, "Hybrid key management mechanism based on double cluster head structure," in *Proceedings of the IEEE 2nd International Conference on Instrumentation, Measurement, Computer, Communication and Control*, pp. 164–167, Harbin City, China, December 2012.

[14] W. R. Pires, J. T. H. de Paula Figueiredo, H. C. Wong, and A. A. F. Loureiro, "Malicious node detection in wireless sensor networks," in *Proceedings of the IEEE 18th International Parallel Distributed Processing Symposium*, vol. 1, p. 24, Santa Fe, NM, USA, April 2004.

[15] V. P. Singh, A. S. A. Ukey, and S. Jain, "Signal strength based hello flood attack detection and prevention in wireless sensor networks," *International Journal of Computer Applications*, vol. 62, no. 15, pp. 1–6, 2013.

[16] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro, "SecLeach—a random key distribution solution for securing clustered sensor networks," in *Proceedings of the 5th IEEE International Symposium on Network Computing and Applications*, pp. 145–154, Washington, DC, USA, 2006.

[17] A. C. Ferreira, M. A. Vilaça, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. Loureiro, "On the security of cluster-based communication protocols for wireless sensor networks," in *Proceedings of the 4th IEEE International Conference on Networking*, vol. 3420 of *Lecture Notes in Computer Science*, pp. 449–458, 2005.

[18] J. Ibriq and I. Mahgoub, "A Secure Hierarchical Routing protocol for wireless sensor networks," in *Proceedings of the 10th IEEE Singapore International Conference on Communications Systems (ICCS '06)*, pp. 1–6, IEEE, Singapore, November 2006.

[19] L. B. Oliveira, A. Ferreira, M. A. Vilaça et al., "SecLEACH—on the security of clustered sensor networks," *Signal Processing*, vol. 87, no. 12, pp. 2882–2895, 2007.

[20] K. Zhang, C. Wang, and C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management," in *Proceedings of the 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–5, October 2008.

[21] R. Alcalá, Y. Nojima, H. Ishibuchi, and F. Herrera, "Special issue on evolutionary fuzzy systems," *International Journal of Computational Intelligence Systems*, vol. 5, no. 2, pp. 209–211, 2012.

[22] Y. Y. Chung and N. Wahid, "A hybrid network intrusion detection system using simplified swarm optimization (SSO)," *Applied Soft Computing*, vol. 12, no. 9, pp. 3014–3022, 2012.

[23] P. Rathee and S. Malhotra, "Preventing sybil attack in wireless sensor networks," *International Journal for Innovative Research in Science & Technology*, vol. 1, no. 12, 2015.

[24] F. Cao, H. Ye, and D. Wang, "A probabilistic learning algorithm for robust modeling using neural networks with random weights," *Information Sciences*, vol. 313, pp. 62–78, 2015.

[25] V. Obada, K. Djouani, and Y. Hamam, "Hidden Markov model for shortest paths testing to detect a wormhole attack in a localized wireless sensor network," *Procedia Computer Science*, vol. 10, pp. 1010–1017, 2012.

[26] J. Rupareliya, S. Vithlani, and C. Gohel, "Securing VANET by preventing attacker node using watchdog and Bayesian network theory," in *Proceedings of the International Conference on Communication, Computing and Virtualization*, vol. 79, pp. 649–656, Mumbai, India, February 2016.

[27] P. Amish and V. B. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol," in *Proceedings of the 7th International Conference on Communication, Computing and Virtualization (ICCCV '16)*, vol. 79, pp. 700–707, February 2016.

[28] A. Zadeh, "Fuzzy rule sets," in *Information and Control*, Department of Electrical Engineering and Electronics Research Laboratory, University of California, Berkeley, Calif, USA, 1965.

[29] A. Zadeh, "Fuzzy sets and information granularity," in *Fuzzy Sets, Fuzzy Logic and Fuzzy Systems*, pp. 433–448, World Scientific, 1996.

[30] K. Q. Yan, S. C. Wang, S. S. Wang, and C. W. Liu, "Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network," in *Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT '10)*, pp. 114–118, Chengdu, China, July 2010.