



Research Article

Vampire Attack Mitigation and Network Performance Improvement Using Probabilistic Fuzzy Chain Set with Authentication Routing Protocol and Hybrid Clustering-Based Optimization in Wireless Sensor Network

Lulwah M. Alkwai,¹ Arwa Naser Mohammed Aledaily,¹ Shahad Almansour ,¹
Shoayee Dlam Alotaibi,¹ Kusum Yadav,¹ and Velmurugan Lingamuthu ²

¹College of Computer Science and Engineering, University of Ha'il, Hail, Saudi Arabia

²Ambo University, Ambo, Ethiopia

Correspondence should be addressed to Velmurugan Lingamuthu; velmurugan.lingamuthu@ambou.edu.et

Received 21 April 2022; Revised 17 May 2022; Accepted 25 May 2022; Published 14 June 2022

Academic Editor: Mukesh Soni

Copyright © 2022 Lulwah M. Alkwai et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The most effective threat for wireless sensor networks (WSN) is Vampire attacks on sensor nodes as they can stretch the network connectivity among them and influence the network's energy, which can drain the network. Vampire attack has particular malicious nature of sensor nodes in which they can widely exploit features of combined routing protocol. Fuzzy rules and fuzzy sets are highly optimal techniques in mitigating the vampire attacks of the network, which can quantify the uncertain behaviour of sensor nodes. This study aims to propose a novel technique using a probabilistic fuzzy chain set with authentication-based routing protocol and hybrid clustering technique for data optimization of the network. The suggested approach here employs a fuzzy-based chain rule set to combat growing types of vampire assaults using probability formulas. The authentication routing protocol has increased network routing security. The proposed technique (PFCS-ARP_HC) has optimized the energy consumption of network. Simulation for this technique has been carried out using NS2 and experimental results show the performance of the proposed model in terms of throughput of 98%, packet delivery ratio of 89%, energy consumption of 67%, latency of 46% control overhead of 53%, and attack detection ratio of 87.9%.

1. Introduction

Wireless network is a physical infrastructure that allows computers, mobile phones, printers, and other devices to communicate with each other via a router. Ad hoc sensor networks are being organized in numerous areas such as the military, health care, and defence as a result of technical advancements [1]. These sensors measure environmental elements such as humidity, temperature, traffic surveillance, movement, noise, military, and management of agricultural land. These sensors are vulnerable to DoS assaults such as the vampire, directional, black hole, and selective forwarding attacks because they are battery-powered. Because vampire

attacks are not protocol-specific, they're difficult to spot. Security is a significant study topic in WSNs (wireless sensor networks) [2]. Because routing is a trust-based operation among nodes, attackers have a good possibility of interfering with it. As a result, actions to safeguard WSN from security threats must be deployed. Security studies of these networks are undertaken separately because they are typically built without prior planning and are only used for a short period of time. DoS attacks are one of the most well-known types of network sensor attacks. DoS prevents radio from going into sleep mode, which would drain the battery completely [3].

Because of their distributed structure and positioning in remote places, these networks are exposed to a variety of

security vulnerabilities that can jeopardise their correct operation. WSNs with resource-constrained nodes are extremely vulnerable to a number of attacks due to their simplicity. Sensor devices' high resource constraints present significant hurdles to resource-hungry security systems. Because of the hardware limits, security methods must be exceedingly efficient. This is no trivial task [4]. Sensor networks' most valuable resource is energy. In terms of power, communication is very costly [5, 6]. The available communication channels for coordinating their attack. As a result, WSN is vulnerable to a number of attacks that could obstruct its operations and negate the benefits of using its services. If a sensor node is compromised, all vital material, data and code stored on that node can be retrieved. An attacker can quickly recover valuable information from packets that are sent. Finally, attacker can send bogus data into network [7, 8], possibly impersonating one of sensors, with goal of altering sensor readings or interrupting internal control data (Message Injection). Attackers may collaborate on a system attack by using a few MNs with similar or greater hardware capacity than genuine nodes [9]. These rogue nodes can be obtained either individually or by capturing and physically overwriting the memory of a few legitimate nodes. In rare cases, participating nodes may have high-quality communications links available to coordinate their attack. As a result, WSN is susceptible to a variety of assaults that might disrupt its operations and nullify the benefits of using its services [10–12].

Vampire attacks are tough to identify and avoid because they use protocol-compliant messages. Vampire attacks are not protocol-specific in the sense that they do not rely on individual routing protocols' design or implementation flaws. Effects of a vampire attack: (a) Vampire attacks are protocol-independent. (b) They do not cause any interruptions in instant availability. (c) Protocol-compliant communications are used by vampires. (d) Send a small amount of data while consuming the most energy. (g) Vampires do not alter or disturb established courses. Vampire assaults can be divided into two categories. There are two types of attacks: Carousel and Stretch [13–15].

The contribution of this study is as follows.

- (i) To develop the novel technique in mitigating vampire attacks and improve the network performance using security-based routing protocol and clustering-based data optimization.
- (ii) Here the data optimization has been carried out using hybrid clustering technique and vampire attack is mitigated using probabilistic fuzzy chain set with authentication-based routing protocol.
- (iii) Simulation for this technique has been carried out using NS2 and experimental results shows the performance of the suggested model in terms of throughput, packet delivery ratio, energy consumption, control overhead, and attack detection ratio.

2. Related Works

Numerous works have been carried out in this area and enormous data are available on DoS attacks and their effects

on ad hoc networks. At the routing protocol layer, the author [16] investigates resource depletion assaults, often known as "Vampire Attacks," which permanently disable networks by rapidly draining node battery power [17, 18]. They've included information on numerous vampire assaults and how they affect ad hoc networks. They've also listed a number of ways to protect the network from these threats. Our previous work [19] provides a quick overview of these two procedures as well as the consequences of vampire attacks on them. Some recent study in this topic includes numerous implementations and theoretical work, such as [20], which shows how to tolerate attack by using CH. In the event of a vampire assault, the Cluster Head intervenes and distributes the packet to its target without dropping it. As a result, even in the event of a vampire assault, the message is delivered successfully and reliably. The authors of [21] suggested how to use PLGP, an identifying malicious assault to lessen the vampire attack. The next study [22] looks into the energy issues and assaults that Ad Hoc WSNs and, eventually, future IoT face. It also provides a strategic method to dealing with energy threats that is resilient. The proposed approach in [23] aims to give a method that may be utilized to find vampire attack in WSN. A new trust routing motif is proposed in [24]. Multiagents gather multifactor data and come together to decide on the trust path. The degree of belief in the long-term conduct of alternative entities that is based on the nodes' previous experience is referred to as trust. CAWS and MES-1, a collection of algorithms put together by a researcher [25], were examined. CAWS (cellular automata-based security algorithms) entails key management and secure digital communication under cellular automata rules, requiring minimal memory and simple calculation. The author of [26] first aims to assess these vulnerabilities in terms of router layer battery reduction attacks. Second, it focuses on making changes to current routing protocols in order to prevent packet loss due to vampire attacks during packet forwarding. To protect wireless sensor networks from wormhole attacks, they propose a trust aware distance vector routing protocol (TAODV) in [27]. Their proposed approach was tested utilising experimental results in terms of enhanced PDR, end-to-end delay and node to destination variation. Ariadne, an on-demand routing system, and the LEACH protocol, intended to reduce battery use, are among the approaches and protocols used to resist these assaults. The LEACH methodology involves two phases: steady state and startup. The cluster is established in the steady-state phase based on threshold value, with each node calculating its value by picking a random number between 0 and 1 and broadcasting it to its neighbours. A node with a value less than threshold limit is nominated as CH and rest of nodes join as member nodes. Although the LEACH protocol helps to save energy, it does not ensure secure routing against vampire attacks. There are two phases to EWMA (Energy Weighted Monitoring Algorithm) [28]. The cryptographic keys can guard against active attacks from the outside, but they are unreliable in the case of passive attacks that compromise service quality as well as reliability. Optimization techniques based on the behaviour of lions during territorial defence and

takeover [29, 30], such as the Lion algorithm, were devised to minimise passive attacks and to optimise path selection. The nonlinear system identification solution is implemented. However, solutions to difficult situations are not taken into account. As a consequence, the authors in [31] presented the WOA, which is also an optimization system based on the behaviour of humpback whales. Because the location of the prey is unknown at beginning, the current solution, or prey, is treated as the best response and position is updated in each iteration, despite the fact that network nodes use more energy for calculation.

3. System Model

This section discusses the proposed design in mitigating vampire attacks of the sensor networks. Here the proposed module has been divided as three parts: first is hybrid clustering in which the nodes has been clustered based on energy level of energy; secondly analysing for vampire attacks by authenticating data transmission path through routing protocol and probabilistic fuzzy chain set with fuzzy rule sets. The overall proposed flow diagram is shown in Figure 1.

3.1. Hybrid Clustering of Nodes Based on the Energy Level. Consider n nodes in a field. Lifetime of node i is denoted by L_i . Let the network lifetime, L , be time it takes for first node in network to exhaust its energy. The main goal is to increase L , which necessitates uniformly utilising the energy of all nodes. To avoid drawbacks of both static and dynamic clustering methods, designed hybrid method so that clustering is not done every round. To do so, CHs save their residual energy in their memory at the end of each setup step after clusters have formed. When a CH detects that its residual has fallen below ECH, it sets a specific bit in a data packet ready to be forwarded to BS.

3.1.1. Cluster Setup Phase. Nodes that will become CH will be chosen during the clustering setup step. CH is chosen based on delay duration of processing. The primary CH will be chosen when the delay time approaches zero. If a node's delay time is assessed to be lower, it has a better chance of becoming a CH and sending a broadcast packet. Packet size, node ID, node location, residual energy, and packet type are all included in the content of the packet. If a node gets packet type 2 from other nodes before delay timer expires, it will become a normal node "N." Additionally, the candidate CH will send messages to sensor nodes through broadcast. Messages from the CH will be verified by the sensor nodes [32–34]. If the CH has a limited amount of residual energy and is likely to expire soon, the nodes in the network will advise their neighbours to modify path and deliver data to another CH. Several nodes having the same number of neighbours play a vital role in ensuring that each node has a diverse number of neighbours. Each node delay time is estimated using

$$D_t(i) = \left(1 - \frac{E_{rem(i)}}{E_{avg}(i)}\right) * W_t + R_v, \quad (1)$$

where $D_t(i)$ is node i 's delay time, $E_{rem(i)}$ is node i 's residual energy, W_t is primary CH's competition time, and R_v is the random value. When nodes have same residual energy, random value can help to reduce communication conflicts.

Algorithm for cluster setup phase (Algorithm 1):

3.1.2. Cluster Formation (CF). The CF function chooses best non-CH candidate to join CH. After selecting principal CH, it will broadcast packet type 3 to node S_i while waiting for the packet to arrive. If node S_i receives a message from node S_j , add it to CH_list of potential nodes and alter it to a non-CH state. In this situation, it will calculate distance between non-CHs and CH to select best nodes as its CH. The best CH selection is determined by a small number of neighbour nodes, a short distance, and a high residual energy. Furthermore, more number of nodes in every cluster has an impact on the network's performance.

Algorithm for CF (cluster formation) (Algorithm 2):

3.1.3. Transmission Phase. This phase transfers data over the network between CHs and CMs. A CH rotation technique and stacking implementation make up the transmission phase. In the following part, we'll go over the CH rotation approach and the layered implementation design in more detail. After selecting the principal CH, the transmission procedure is used to create a TDMA schedule that transmits a broadcast schedule to all CMs. Data will be sent from the CMs to primary CH, which will aggregate it. Aggregation operations are forwarded to BS after that.

3.1.4. Analysing the Malicious Activities of the Network. The network's nodes are responsible for not only delivering precise data, but also for updating new data in received data packet and sending it to next node. As a result, it is critical to confirm that data exchanged between nodes is secure. When a node is subjected to an aggressive or passive attack, it loses its trustworthiness. A carousal attack occurs when a rogue node causes a data packet to loop continuously, preventing it from reaching the BS or the destination node. The energy of the node depletes dramatically in a short amount of time as a result of this anomalous behaviour, resulting in a vampire attack. If BS does not receive requested data packet within specified time interval, BS requests that CH evaluate trust value of all its member nodes given by (2)

$$T^d(t) = \frac{P_{n1}(t)}{P_{n2}(t)}. \quad (2)$$

$T^d(t)$ is computed direct trust between $n1$ and $n2$ nodes. $P_{n1}(t)$ denotes packets that have been received. The total number of packets sent is $P_{n2}(t)$. The surrounding nodes' estimated trust are represented in (3)

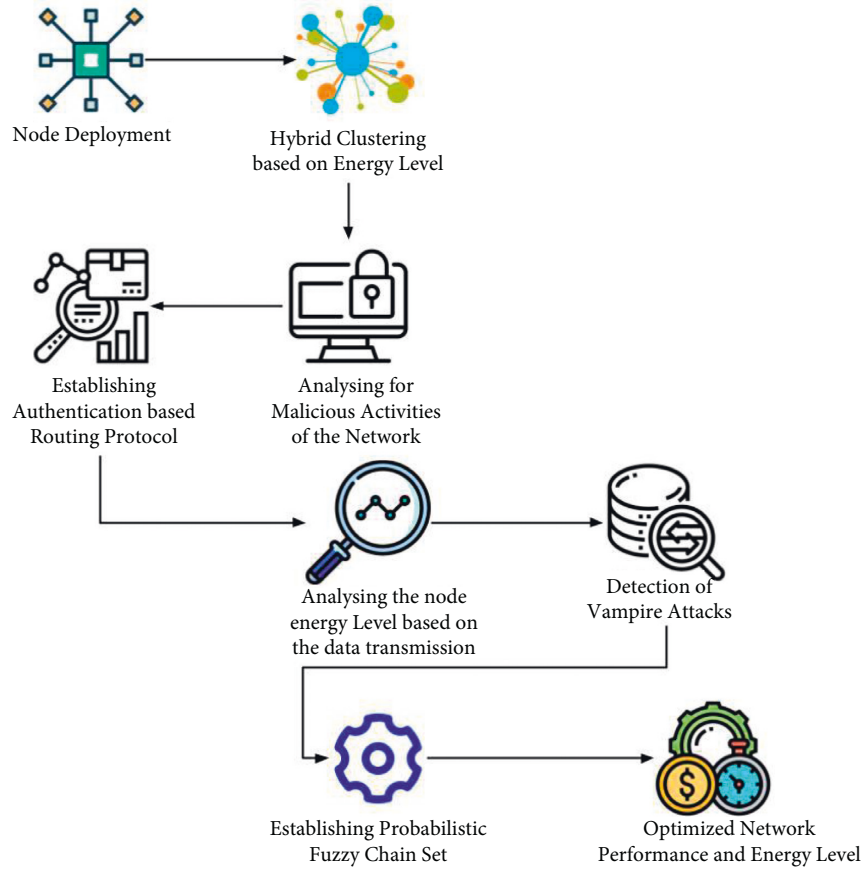


FIGURE 1: Overall proposed flow diagram.

$$T^t(t) = \frac{1}{k} \sum_{d=1}^k T^d(t), \quad (3)$$

$$T = \alpha T^d(t) + \beta T^l(t), \quad (4)$$

α, β values range from 0 to 1 such that $\alpha + \beta = 1$. Trust threshold is 0.99–1. If estimated value falls below this threshold, sensor is classified as an MN, as it experiences higher packet loss during transmission. For effective transmission of data to send packet along chosen path, the trust criteria are taken into account. If BS identifies an MN based on the trust degree calculation after the verification procedure, it sends an alarm message to CH with ID and location of detected MN. CHs have now blacklisted and isolated rogue node, as well as broadcasting its ID to all of its members.

3.1.5. Authentication-Based Routing Protocol. The sink is ready to receive a data packet from source/intermediate node k . It uses the selective authentication algorithm to determine whether or not to inspect the data packet. As a result, timer on the higher priority node is shorter. It would put up its own forwarder network and get ready to send data. The process is repeated by subsequent sensor nodes until data packet reaches sink.

Algorithm for Authentication-based routing protocol (Algorithm 3):

3.1.6. Probabilistic Fuzzy Chain Set. Three factors are chosen in the suggested work while considering the concept of vampire assault. Three trust factors, such as node's packet drop rate, percentage of battery drain, and the number of link requests initiated by the node, can be used to detect the vampire node. These are described as follows.

- (1) **Packet Drop Rate (PDR):** Malicious nodes lose a substantial percentage of packets, whereas trustworthy nodes forward all of the packets they receive. The ratio of number of packets dropped to total number of packets is used to calculate this value.
- (2) **Battery Discharge Rate (BDR):** This node parameter is dependent on the network's operation. An active node appears to be in use and uses more energy. Nodes with a malignant or selfish aim, on the other hand, are observed to be more active than other nodes.
- (3) **Number of link requests (NLR):** The vampire node tries to connect to numerous nodes at the same time. As a result, the node will generate an unusually large number of link requests. The i th node initial position is given by (5)

```

(1) Input ( $S_i, W_t, A, B, Th_v, RL_{max}, a, b, R_v$ )
(2) Output
(3) For each node  $S_i$  do
(4) Evaluate  $R_c(i)$ 
(5) Nodes known their neighbours
(6) Broadcast packet type_1
(7) Evaluate number of neighbour nodes  $NN(i, r)$ 
(8) Every node evaluates delay time  $D_t(i)$ 
(9) Evaluate average energy of neighbour nodes  $E_{avg}(i)$ 
(10)  $S_i$ . Type = "N".
(11) If  $S_i.D_t(i)$  = close to 0
(12) CountCH = countCH + 1
(13)  $S_i$ . Type = "CH."
(14) End
(15) While  $S_i.D_t(i) \neq$  close to
(16) Broadcast packet type_2
(17) If  $S_i.D_t > S_j.D_t$ 
(18) End
(19)  $S_i$ . Type = "N."
(20) While  $S_i.W_t \neq 0$ 
(21) If  $S_i.D_t < S_j.D_t$ 
(22) If  $S_i$ . Type = "CH."
(23) If  $S_i.E < S_j.E$ 
(24)  $S_i$ . Type = N.
(25) Else  $S_i$ . Type = "CH."
(26) End While

```

ALGORITHM 1: Cluster setup phase.

```

(1) Input ( $S_i, S_j$ )
(2) Output (CH_list)
(3) For each node  $S_i$  do
(4) If  $S_i$ . Head =  $S_j$ . Head
(5) If  $S_i$ . Type = "N" &&  $S_i.E > 0$  &&  $S_i$ . Type =* "Awake."
(6) Evaluate less distance from non-CH to CHs
(7) If  $S_i.E > av\_energy$  &&  $S_i$ . Neighbour  $< S_j$ . Neighbour
(8)  $S_i$ . Type = "CH."
(9) CH_list store  $S_i$ 
(10) Broadcast packet type 3
(11) Else  $S_i$ . Type = "CH."
(12) End for

```

ALGORITHM 2: CF (cluster formation).

$$f(x_i), x_i = (x_i^1, \dots, x_i^D). \quad (5)$$

The matrices' dimension is D . For example, the position of node 1 is given by $x_{1D} = x_{1D} = (x_{11}, y_{12}, z_{13}, w_{14})$, position of node 2 is given by $Sx_{2D} = (x_{21}, y_{22}, z_{23}, w_{24})$, and so on. Fitness value is given by (6)

$$f(x) = \frac{1}{4} [T + E + D + d(i, j)]. \quad (6)$$

After determining the fitness of all nodes, the fitness with the lowest value, f_{best} , is regarded the best, and the fitness with the highest value, f_{worst} , is measured worst. Masses of all surrounding nodes are determined in molecular dynamics. The atoms with the greatest mass have best fitness value, while atoms with smallest mass have poorest.

$$m_{i(t)} = \frac{M_i(t)}{\sum_{j=1}^N M_j(t)}, \quad (7)$$

where $M_i(t)$ and $M_j(t)$ signify the mass of i th and j th atoms (node); $f_{best}(t)$ indicates the least fitness value; and $f_{worst}(t)$ denotes the highest fitness value. PFCS is denoted as a collection of four tuples $PFCS = (F_H, F_\kappa, F_n, F_d)$ with various encouragement factors of vampire attack as $FI = f1, fe, f3, \dots, fm$. The following steps make it easier to mitigate a vampire attack with PFCS.

- (1) For removing the discrepancy that exists between generalisation and quality of approximations.
- (2) Evaluate probability-oriented fuzzy membership value " $F_n(\lambda_{F_n(j)}(f_i))$ " from matrix F_d using the

```

Vector<nsaddr.t>ARP:multi_shortest_path(nsaddr_t_sourfe_node,int packet.energy);
Bool exchange;
If (high ≥ low){
While(time ≥ TIME_MAX&& listening (ACK = false){
If (exchange){
Int high, low, path.amount
Exchange = false
Path_amount
Multi_shortest_path(nsaddr.t source_node, int packet_energy)
High = path_amount, low = 1
Count(int timer); exchange = true
Send(route[high--]source_node)
}
}
Else
{
Path_amount
Send(route[low++] source_node)
Exchange = true
}
}
Else{
Int packet_energy)
High = path_amount;low = 1
Multi_shortest_path(nsaddr_t souce_node
exchange = true
}
}
Return
}

```

ALGORITHM 3: Authentication-based routing protocol.

uncertainty factor' $F_n(\chi_{i,j}^g)$ and fuzzy associativity factor $\lambda_{F_{n(i)}}(f_i)$ as

$$F_n(\lambda_{F_{n(i)}}(f_i)) = \sum_{k=1}^{S_{ij}} \lambda_{F_{n(j)}}(f_i) * F_n(\chi_{i,j}^g). \quad (8)$$

(3) Finding of equivalent classes based on union and intersection operations utilising a probabilistic fuzzy theory technique, as shown in (2) and (3).

$$\text{Union}(F_{n(i)} \in F_{n(i)}(j) = \max_j \left\{ F_N \left(\left(\lambda_{F_{n(j)}} f_i \right) \right) \right\}_{i=1}^m,$$

$$\text{Intersect}(F_{n(i)} \in F_{n(i)}(j) = \min_j \left\{ F_N \left(\left(\lambda_{F_{n(j)}} f_i \right) \right) \right\}_{i=1}^m \quad (9)$$

(4) Mean, higher, and lower degrees of approximations (π_M, π_G, π_L) evaluated for quantifying the degree of conformation that is estimated:

$$\begin{aligned} \pi_M &= \min(\pi_L, \pi_G), \\ \pi_L &= \kappa(F_d, \text{Interect } F_{n(i)}), \\ \pi_G &= \kappa(\text{Union } F_{n(i)}, F_d). \end{aligned} \quad (10)$$

Finally, the crisp factor of PFCS is calculated using (7) as the ratio of divergence between lower as well as

greater approximations to increasing count of entities inspected in universe utilized for decision making.

$$\beta = 1 - \frac{\sum \pi_G - \lambda_L}{|F_u|}. \quad (11)$$

(5) Then evaluation of inclusion degree is enabled using

$$\beta(M_a, M_b) = \frac{|\phi(M_a, M_b)|}{|\text{Supp}(M_b)|}. \quad (12)$$

3.1.7. Fuzzification. For FCS, three variables are used as input. The maximum and minimum values of the fuzzifier crisp input variable for calculating the eligibility index. Euclidean distance between each SN and BS is called distance to BS. The overall power accessible with the SN at that moment is known as Remnant Energy. The count of neighbouring nodes in vicinity of node under consideration for CH candidacy is known as node density. The FIS receives these crisp values (discrete values).

3.1.8. Fuzzy Rule Base. After fuzzification, the membership values are given into the rule base for IF-THEN situations. A value is derived by applying the fuzzy AND and OR operators to inputs. The aggregation method unites all of the

```

Input:n_round, deployment area, p, sing_p, initial_e, c_range, n_node, t_node
Output:R_VALUE = [CHs,alive_n]
(1) Initialization;
(2) For r= 1 to n_round
(3) For I= 1 to n
(4) If(mod(r,3) == 1)
(5) If (S(i).energy ≤ 0)
(6) Alive = alive-1;
(7) SAY_HI_MESSAGE (ID,CR,SE)
(8) If r= 1
(9) Apply PFCS method to choose initial tentative CHs
(10) End if
(11) S(i).channel = evalfis([S(i).energy S(i).cound_tch],z)
(12) If r> 1
(13) End if
(14) If S(i) = best (channel])
(15) S(i).t_node = TCH;
(16) If (S(i).E < S(j).E)
(17) CONFIRM_TCH_MESSAGE(ID)
(18) S(i).type = N;
(19) MEMBER_JOIN_CH_MESSAGE(ID)
(20) Nodes with S(i).t_node = TCH will be confirmed final CH
(21) Transmit data ti the CH
(22) If (mod(r,3) == 2) and previous CHs are alive
(23) Else choose best chance CH
(24) If (mode(r,3) == 0)
(25) If (S(i).energy ≤ 0)
(26) For I= 1 to n
(27) Alive = alive-1;
(28) End if
(29) S(i).chance2 = evalfis([S(i).energy S(i).mch],z);
(30) SAY_HI_MESSAGE(ID,CR,SE)
(31) If (S(i).E < S(j).E)
(32) S(i).type = N;
(33) S(i).t.node = TCH;
(34) If (S(i) = best(chance2)
(35) AUTHORIZE_TCH_MESSAGE(ID)
(36) MEMBER_JOIN_CH_MESSAGE(ID)
(37) Nodes with S(i).t_node = TCH will be confirmed final CH
(38) End if
(39) Return R_VALUE

```

ALGORITHM 4: PFCS.

output after applying the 27 rules and a high value is determined from the gathered fuzzy set. Probabilistic chain rule was used, which is the most often used due of its properties, to generate the eligibility index using Fuzzy Logic.

3.1.9. *Defuzzification.* Center of area (Z^*) method is utilized for defuzzification by (13)

$$Z^* = \frac{\int \mu_A(x)xdx}{\int \mu_A(x)dx}. \quad (13)$$

After calculating the eligibility index for all nodes, the threshold (TH) is derived using the equation (9).

$$TH = \frac{\text{Node}(i) \cdot P \times \text{mean}[EI]}{1 - \text{Node}(i) \cdot P \times \text{mod}(r, (1/\text{Node}(i) \cdot P))}. \quad (14)$$

For indiscriminate CH selection, every node in network creates a randomised number. If that value is less than computed TH, node will be assigned to CH role. CH's role is critical to the network's energy efficiency and rotated after each round to balance load among organized SN. Popt clusters are created in this manner. If some nodes remain after CF, they will join the cluster that is closest to them following CH recognition. Once all of the SN have been bound to clusters, the topology configuration process is complete. This method of weightage calculation enables for accurate values of criteria weights with the highest possible membership grade

TABLE 1: Comparative analysis of the proposed and existing techniques in vampire attack mitigation.

Parameters	TAODV	LEACH	WOA	PFCS- ARP_HC
Throughput	93	95	97.8	98
PDR	87.8	88	88.5	89
Energy consumption	63	65	74.5	75.5
Attack detection ratio	81.5	82	87.8	88
Latency	58	56	53.5	46
Control overhead	50	52.8	53	62

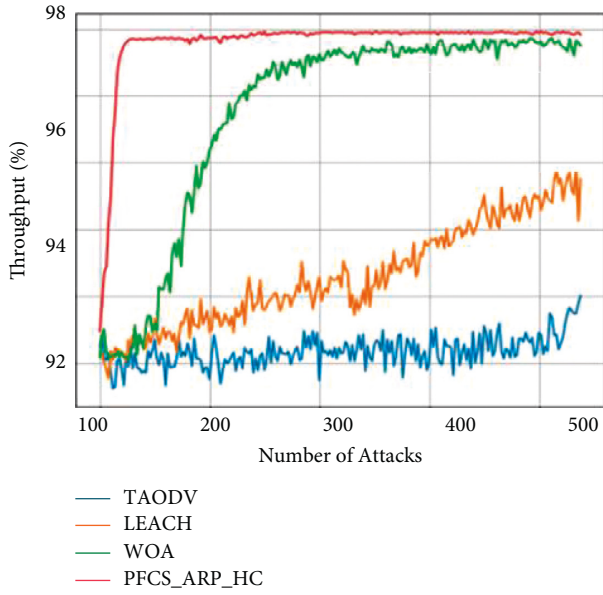


FIGURE 2: Comparative analysis of throughput.

for their membership function. Equation (10) is a linear programming model that enables the max–min weightage computation approach computationally.

$$z = \beta \longrightarrow \max,$$

$$\frac{w_i + \alpha_j^i - u_j}{\alpha_j^i} \geq \beta \text{ where } 1 \leq j \leq k,$$

$$\frac{\alpha_j^i + u_j - w_i}{\alpha_j^i} \geq \beta \text{ where } 1 \leq j \leq k, \quad (15)$$

$$\text{Such that } \sum_{j=1}^k w_i = 1, w_i \geq 0 \text{ with } \beta \in (0, 1).$$

The weightage set in question is made up of all strict and fuzzy sets with a separate high value intersected. The objective function is stated to be maximising in this scenario based on gain corresponding to result membership maximal grade. Furthermore, w_i is the weight value of the crisp parameter linked with the j th condition.

Algorithm for PFCS (Algorithm 4):

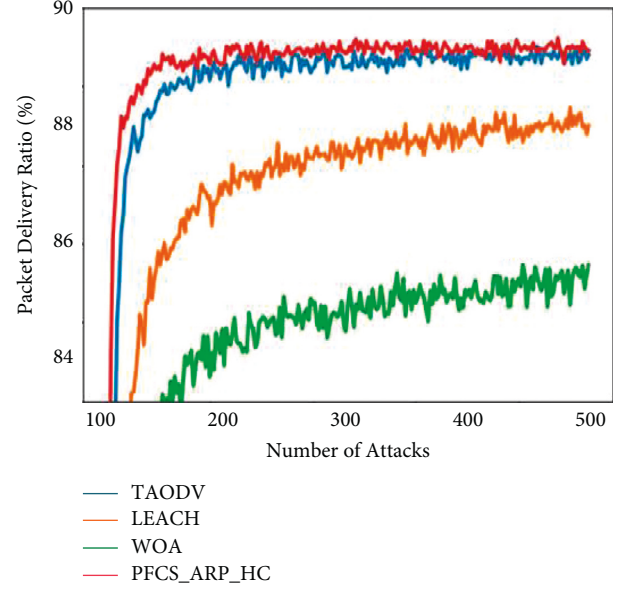


FIGURE 3: Comparative analysis of PDR.

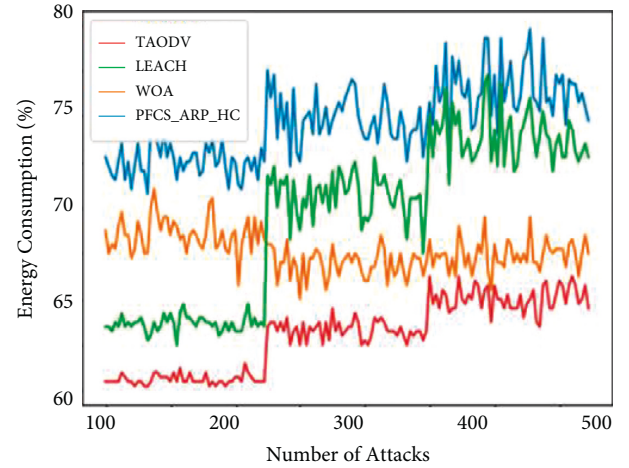


FIGURE 4: Comparative analysis of energy consumption.

4. Performance Analysis

The PFCS-ARP HC simulation configuration contains 100 mobile nodes that are randomly distributed within a terrain perimeter of 10001000 square metres. For validating the performance of PFCS-ARP HC, the pause period and simulation time were 20 seconds and 300 seconds, respectively. The PFCS-ARP HC simulation environment uses 802.11 as MAC protocol with 2 Mbps channel capacity of and Constant Bit Rate data source. Source and destination pairs of 20 and 50 mobile nodes are also used in the simulation investigation.

Table 1 shows comparative analysis for the proposed and existing techniques in minimizing the vampire attacks. Here the parameters compared are throughput, PDR, energy consumption, attack detection ratio, latency, and control overhead and compared with TAODV, LEACH, and WOA with the proposed PFCS-ARP_HC.

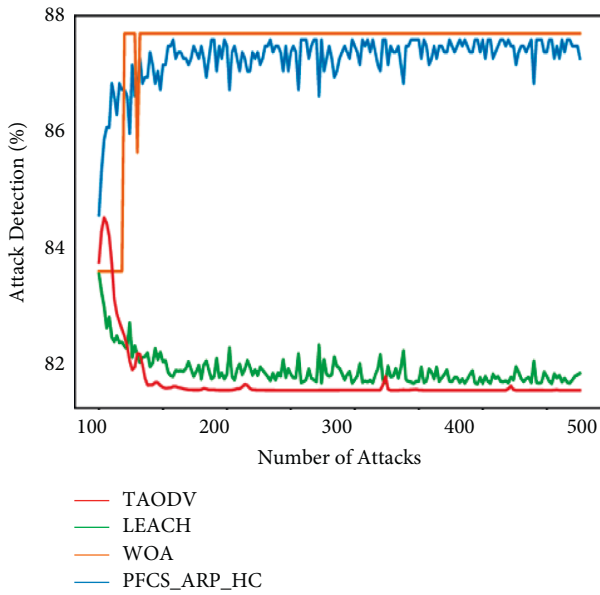


FIGURE 5: Comparative analysis of attack detection ratio.

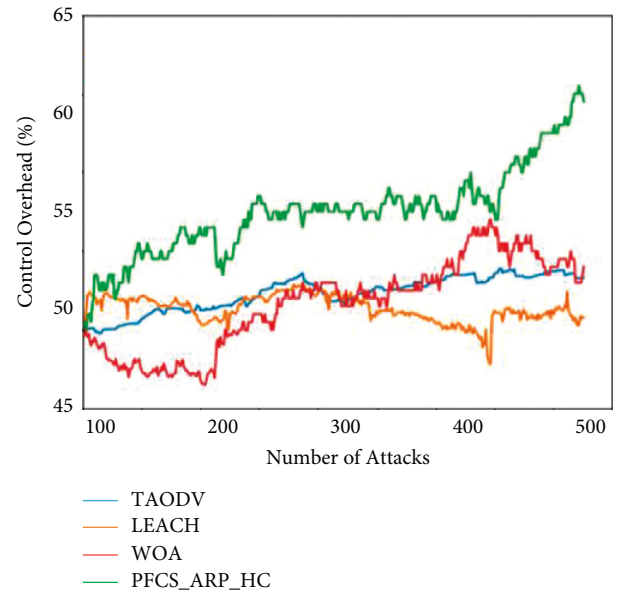


FIGURE 7: Comparative analysis of control overhead.

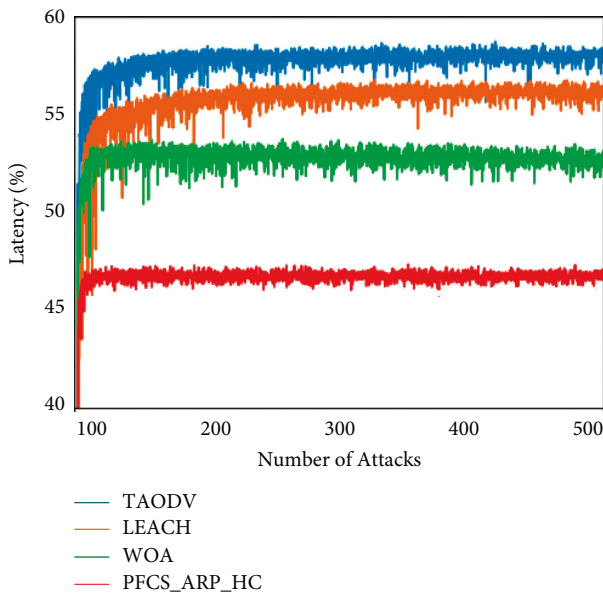


FIGURE 6: Comparative analysis of latency.

Figures 2–7 show comparative analysis of the proposed and existing techniques in vampire attack mitigation and improving the network performance. Comparative analysis has been carried out for throughput, PDR, energy consumption, attack detection ratio, latency, and control overhead. Here throughput attained by the proposed technique is 98% which enhanced when compared with TADOV, LEACH, and WOA. In terms of PDR, 89% has been obtained by the proposed technique; energy consumption by the proposed protocol is 75.5%, which is optimized when compared with existing protocol while data

transmission. Since their energy consumption is high, the mitigation of vampire attacks by existing protocol is not efficient. Vampire attack detection ratio obtained by the proposed technique is 88% which is optimal than the existing techniques. Latency of the proposed technique in network is 46% and control overhead is 62% which is enhanced based on this comparative analysis.

5. Conclusion

This research offered a unique design strategy for minimizing vampire attacks and improving network performance by utilising a security-based routing protocol and clustering-based data optimization. The data was optimised using a hybrid clustering approach, and the vampire attack was neutralised using a probabilistic fuzzy chain paired with an authentication-based routing protocol. The routing security of the network has been improved by authentication routing protocol. The performance can be improved by optimizing the data and network by hybrid-based sensor nodes clustering. Simulation for this technique has been carried out using NS2 and experimental results show that the performance of the proposed model in terms of throughput of 98%, packet delivery ratio of 89%, energy consumption of 67%, latency of 46% control overhead of 53%, and attack detection ratio of 87.9% [35].

Data Availability

The data used to support the findings of this study are available from the author upon request (kusumasyadav0@gmail.com).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] C. Wang, R. S. Batth, P. Zhang, G. S. Aujla, Y. Duan, and L. Ren, "VNE solution for network differentiated QoS and security requirements: from the perspective of deep reinforcement learning," *Computing*, vol. 103, no. 6, pp. 1061–1083, 2021.
- [2] B. Gao, T. Maekawa, D. Amagata, and T. Hara, "Detecting reinforcement learning-based Grey hole attack in Mobile wireless sensor networks," *IEICE - Transactions on Communications*, vol. E103.B, no. 5, pp. 504–516, 2020.
- [3] D. Zhang, T. Zhang, and X. Liu, "Novel self-adaptive routing service algorithm for application in VANET," *Applied Intelligence*, vol. 49, no. 5, pp. 1866–1879, 2019.
- [4] M. K. Shahzad, L. Nkenyereye, and S. M. R. Islam, "A fuzzy system based approach to extend network lifetime for en-route filtering schemes in WSNs," in *Proceedings of the 2019 11th International Conference on Computer and Automation Engineering - ICCAE 2019*, Perth, Australia, February 2019.
- [5] G. Dhiman, K. K. Singh, A. Slowik et al., "EMoSOA: a new evolutionary multi-objective seagull optimization algorithm for global optimization," *International Journal of Machine Learning and Cybernetics*, vol. 12, no. 2, pp. 571–596, 2021.
- [6] R. Kumar and G. Dhiman, "A comparative study of fuzzy optimization through fuzzy number," *International Journal of Modern Research*, vol. 1, no. 1, pp. 1–14, 2021.
- [7] P. K. Vaishnav, S. Sharma, and P. Sharma, "Analytical review analysis for screening COVID-19 disease," *International Journal of Modern Research*, vol. 1, no. 1, pp. 22–29, 2021.
- [8] V. K. Gupta, S. K. Shukla, and R. S. Rawat, "Crime tracking system and people's safety in India using machine learning approaches," *International Journal of Modern Research*, vol. 2, no. 1, pp. 1–7, 2022.
- [9] C. Nalini and G. L. V. Prasad, "Secure routing protocol in WSN against vampire attacks," *International Journal of Modern Agriculture*, vol. 9, no. 4, pp. 1247–1253, 2020.
- [10] V. Verma and V. K. Jha, "Detection and prevention of vampire attack for MANET," in *Nanoelectronics, Circuits and Communication Systems*, pp. 81–90, Springer, Singapore, 2021.
- [11] T. Sharma, R. Nair, and S. Gomathi, "Breast cancer image classification using transfer learning and convolutional neural network," *International Journal of Modern Research*, vol. 2, no. 1, pp. 8–16, 2022.
- [12] S. K. Shukla, V. K. Gupta, K. Joshi, A. Gupta, and M. K. Singh, "Self-aware execution environment model (SAE2) for the performance improvement of multicore systems," *International Journal of Modern Research*, vol. 2, no. 1, pp. 17–27, 2022.
- [13] P. B. Srikanth and V. Nagarajan, "Fuzzy rough set derived probabilistic variable precision-based mitigation technique for vampire attack in MANETs," *Wireless Personal Communications*, vol. 121, no. 1, pp. 1085–1101, 2021.
- [14] M. S. Mekala, G. Dhiman, G. Srivastava et al., "A DRL-based service offloading approach using DAG for edge computational orchestration," *IEEE Transactions on Computational Social Systems*, 2022, in Press.
- [15] B. Sumathy, A. Chakrabarty, S. Gupta et al., "Prediction of diabetic retinopathy using health records with machine learning classifiers and data science," *International Journal of Reliable and Quality E-Healthcare*, vol. 11, no. 2, pp. 1–16, 2022.
- [16] I. S. R and J. J., "A secure routing scheme to mitigate attack in wireless adhoc sensor network," *Computers & Security*, vol. 103, Article ID 102197, 2021.
- [17] W. Viriyasitavat, L. D. Xu, A. Sapsomboon, G. Dhiman, and D. Hoonsopon, "Building trust of Blockchain-based Internet-of-Thing services using public key infrastructure," *Enterprise Information Systems*, pp. 1–24, 2022, in Press.
- [18] G. Dhiman, J. Rashid, J. Kim, S. Juneja, W. Viriyasitavat, and K. Gulati, "Privacy for healthcare data using the byzantine consensus method," *IETE Journal of Research*, pp. 1–12, 2022, in Press.
- [19] A. A. Jasim, M. Y. I. Idris, S. Razalli Bin Azzuhri, N. R. Issa, M. T. Rahman, and M. F. b. Khyasudeen, "Energy-Efficient wireless sensor network with an unequal clustering protocol based on a balanced energy method (EEUCB)," *Sensors*, vol. 21, no. 3, p. 784, 2021.
- [20] C. Lyu, X. Zhang, Z. Liu, and C.-H. Chi, "Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks," *IEEE Access*, vol. 7, pp. 31068–31082, 2019.
- [21] J. Zhou, "Efficient and secure routing protocol based on encryption and authentication for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, Article ID 108968, 2013.
- [22] P. K. Mishra and S. K. Verma, "FFMCP: feed-forward multi-clustering protocol using fuzzy logic for wireless sensor networks (WSNs)," *Energies*, vol. 14, no. 10, p. 2866, 2021.
- [23] P. S. Mehra, M. N. Doja, and B. Alam, "Fuzzy based enhanced cluster head selection (FB ECS) for WSN," *Journal of King Saud University Science*, vol. 32, no. 1, pp. 390–401, 2020.
- [24] R. Isaac Sajan and J. Jasper, "Trust-based secure routing and the prevention of vampire attack in wireless ad hoc sensor network," *International Journal of Communication Systems*, vol. 33, no. 8, Article ID e4341, 2020.
- [25] P. B. Srikanth and V. Nagarajan, "Semi-Markov chain-based grey prediction-based mitigation scheme for vampire attacks in MANETs," *Cluster Computing*, vol. 22, no. 6, pp. 15541–15549, 2019.
- [26] A. M. Desai and R. H. Jhaveri, "Secure routing in mobile ad hoc networks: a predictive approach," *International Journal of Information Technology*, vol. 11, no. 2, pp. 345–356, 2019.
- [27] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors*, vol. 19, no. 4, p. 970, 2019.
- [28] J. Jiang, X. Zhu, G. Han, M. Guizani, and L. Shu, "A dynamic trust evaluation and update mechanism based on C4.5 decision tree in underwater wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9031–9040, 2020.
- [29] S. Swain, B. Bhushan, G. Dhiman, and W. Viriyasitavat, "Appositeness of optimized and reliable machine learning for healthcare: a survey," *Archives of Computational Methods in Engineering*, vol. 1, 2022.
- [30] R. Bharti, A. Khamparia, M. Shabaz, G. Dhiman, S. Pande, and P. Singh, "Prediction of heart disease using a combination of machine learning and deep learning," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 8387680, 2021.
- [31] G. Sanjay Gandhi, K. Vikas, V. Ratnam, and K. Suresh Babu, "Grid clustering and fuzzy reinforcement-learning based energy-efficient data aggregation scheme for distributed WSN," *IET Communications*, vol. 14, no. 16, pp. 2840–2848, 2020.

- [32] H. Upadhyay, S. Juneja, A. Juneja, G. Dhiman, and S. Kautish, "Evaluation of ergonomics-related disorders in online education using fuzzy AHP," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 2214971, 2021.
- [33] G. Dhiman, K. K. Singh, M. Soni et al., "MOSOA: a new multi-objective seagull optimization algorithm," *Expert Systems with Applications*, vol. 167, Article ID 114150, 2021.
- [34] H. Kaur, A. Rai, S. S. Bhatia, and G. Dhiman, "MOEPO: a novel multi-objective emperor penguin optimizer for global optimization: special application in ranking of cloud service providers," *Engineering Applications of Artificial Intelligence*, vol. 96, Article ID 104008, 2020.