THE COOPERATIVE-BASED FUZZY ARTIFICIAL IMMUNE SYSTEM USING WIRELESS SENSOR NETWORK

Bharathi Kannan B
Research Scholar
School of Computing Science and Engineering, Galgotias University
Greater Noida, Uttar Pradesh
bbharathikannan@gmail.com

Srinivasan Sriramulu
Professor
School of Computing Science and Engineering, Galgotias University
Greater Noida, Uttar Pradesh
ramuluvasan@gmail.com

Abstract:

Wireless Sensor Networks are used in favour of a extensive diversity of data collecting and transmission applications using wireless networks. Because of the WSN's weaknesses nodes are exposed towards the majority of cyber attacks. A denial of service attacks is the for the most part typical kind of assail in addition with those IoT devices. Certain assault protection strategies be obliged to exist utilized to combat attacks. Readily available are several ways for combating DoS attacks in a sensible nodes. During this learning, an anti-dos innate immune assaults on wireless sensor network is presented, that also would enhance attack prevention exactness, reduce false alarm rates, and discriminate between distinct DoS attacks. A identification of incursions in the earlier system in Wireless Sensor Networks (WSNs) fail to identify such malicious activity because of the scattered scenery of DoS. The cooperative-based fuzzy artificial immune system (Co-FAIS) is used as a bio-inspired technique in this article. It's a modular-oriented defense approach based on the danger hypothesis of the innate immune.

Keywords: Dos Attack, Co-FAIS, WSN, DDOS

Introduction:

WSNs are versatile, straightforward, and simple to execute. They're getting progressively regular because of their minimal effort and viability. For information assortment and handling, it has a wide assortment of utilization in the military and medical services. Because of safety dangers and restricted asset energy, they are helpless against security dangers. As a result, effective protection measures are needed. Among the most serious risks to WSN is a denial-of-service assault. Rather than compromising a service, the primary goal of DoS is to cause disruption by limiting access to the computer or service. This type of attack aims to disrupt a network unable to supply normal service by focusing on both the network's throughput or the network's security. The purpose of these attacks is to overwhelm a victim's connection or processing capacity with packets, preventing him from accessing his regular customers. Delicate figuring, game hypothesis, computerized reasoning, and multi-specialist strategies are utilized in most assault counteraction procedures. The fluffy Q-learning calculation, Decision tree, is utilized in delicate registering-based methodologies [1]. A system is characterized in-game hypothesis for every conceivable situation, and Nash balance is the arrangement. Dendritic cells are utilized by man-made reasoning, depending on the threat guideline. Every specialist in a multi-specialist invulnerable framework has explicit obligations and objectives2. The game hypothesis design dependent on Convenience Energy Aware Relaying (CEAR), which is gotten from Dynamic Source Routing (DSR), is utilized as a stable routing protocol, and Watch-list is utilized to recognize malevolent hubs. To pick a protected way, the utility worth is utilized. Hub bad conduct is determined utilizing participation and believability. Because of vindictive hubs, CEAR loses fewer parts of bundles, while standard DSR loses more parcels. When contrasted with EAR, CEAR endures less misfortune because EAR doesn't react to hub terrible conduct, though CEAR and Watch-list seclude the hub by stamping it as vindictive [2]. Subsequently, the organization hub can be disregarded and won't harm the organization. Non-cooperative nodes are identified using auction theory. The CEAR protocol is

used in this process. Instead of determining a safe path depending on utility value, the bid price is employed. Safe Auction-based Routing is the name of this protocol (SAR). The destination uses a timer to recognize malicious nodes. On the off chance that the clock terminates before the bundle arrives at its objective, the base station will get an awful course code and all hubs will be put on a watch list. On the off chance that a hub shows up the base station will put the hub to a disregard list if it is ignored more than a predetermined number of times., which will at that point be communicated. Since hubs with a terrible standing are overlooked by the large hubs in SAR, the normal number of dropped bundles stays consistent. Since it reacts to awful conduct, SAR loses fewer parts of parcels because of vindictive hubs. It experiences similar issues as the CEAR, for example, bogus marking and edge values4.

The rehashed game hypothesis approach depends on the game hypothesis, which recognizes hubs that consent to advance bundles but don't. It classifies nodes according to their dynamically evaluated behavior. This system encourages node cooperation while also punishing non-cooperative actions. The credibility of sensor nodes helps them to trust each other [3]. Each node can participate equally in packet transmission to improve the network's credibility. Otherwise, the IDS can identify malicious nodes and detach them from network operations, resulting in lower credibility. The strength of this method is that while the base station maintains account of past games, and when a game is over, the base station notifies the players, hub becomes cancerous, it receives a poor ranking. As the aggregate standing amasses, the way with the least malevolent hubs is picked as the victor. As an outcome, malevolent hubs are disconnected. It misses more malevolent hubs to lessen the pace of bogus positives and bogus negatives discovery.

A Bayesian game known as S-LEACH is used to protect the LEACH protocol. S-LEACH is partitioned into adjusts, every one of which starts with an arrangement stage and gets done with a consistent state stage. Bunch heads (CHs) are chosen during the setup process. In the second step, the cluster heads use TDMA (Time Division Multiple Access) ways for setting a time for sensor nodes in their network to submit data to them The central intrusion detection system (IDS) will be notified of malicious nodes [4]. The central IDS then warns the entire network about malicious nodes. As a consequence, local IDSs will be warned that selfish nodes should not be assigned any time, reducing device resource waste. The number of bytes lost is lower in a secure network than in a non-secure network. Throughput is high because CHs can check their component hubs more often in an all-discovered thinking proposes and feel the kind of them. 6. To identify hubs that launch high flood assaults, the AODV-HFDP (Ad-hoc On-Demand Distance Routing with Hello Flood Detection and Prevention) routing algorithm is utilized. The hello flood attack is a network layer attack. A hello message tells that a node exists. When a Hello message arrives, each swelling modifies its neighbor table, displaying the route to the base station node. A approach based on a short test packet is used to discriminate between a friend and a stranger. The Hello message receiving node sends a basic test packet to the Hello message sending node; if the response is received within the specified time threshold, the Hello message sending node is labeled as a friend; if it is not received within the specified time threshold, the Hello message sending node is labeled as an enemy. When a node is marked as malicious, the hello distribution node is disconnected from the direction-finding table, and this information is disseminated across the network [5]. All network nodes delete malicious node information from the routing database. AODV-HFDP outperforms AODV in terms of packet delivery ratio. However, it works for harmonized sensors with constant indication power [6].

An ant-based system takes advantage of the difference between stateless and attractive signatures, keeping only the valid packets while discarding the contaminated ones. The Ant-Based Routing Algorithm is used in this application. If the reliability grows or the buffer size exceeds a certain amount, DDA (DDOS Detecting Ants) detects the assault. DDA [7] detects a sudden increase in system transfer. Because this increase might be due to flooding, it's important to see whether a sample packet is transmitted to a DPA adjunct node (DDOS Preventing Ants). The discrepancy between the current number of incoming packets on the network and the sample packets is detected by DPA. By keeping genuine packets unaffected by the assault, false tagging may be avoided. The quantity of energy used has decreased. It may also help with traffic source detection [8].

The spatiotemporal association underpins the message observation mechanism (MoM). The similarity feature is used by MoM to detect both the content and frequency attacks. The MoM then employs countermeasures such as rekeying and rerouting to isolate the malicious node. Because of CH's sink feature, the MoM is deployed there. The normal message list (NML), abnormal message list (AML), and observation mechanism make up the MoM. (OM). The number of messages sent and the quality of those messages are also taken into account when detecting a DoS attack. If a new message is associated with AML, it is classified as a bogus message. If CH receives a message more than a certain number of times, it is considered a replayed message. CH declares the malicious node's ID and refuses to forward its messages after finding the malicious node. The cluster keys, as well as pair-wise key’s session keys, are

also changed. The key is sent to cluster members through filters that want to block out the rogue node. New roads are being created to get to CH. As the number of rogue nodes grows, this strategy minimizes packet loss. In addition to detecting and guarding against DoS attacks, MoM may save energy by not transmitting packets from hostile nodes any farther [9].

A methodology for recognizing interruptions in WSNs' hubs utilizing a bunch of AI classifiers. These classifiers are SVM [12], credulous Bayesian (NB), DT, and RF. Four kinds of DoS assaults (flooding, gray hole, black hole, and booking assaults) were concentrated in this work. A WEKA information-digging instrument was utilized for carrying out their methodology. The outcomes were assessed in light of various measurements, like review (R), accuracy (P), genuine positive rate (TP), and bogus positive rate (FP). This review showed that the SVM accomplishes a high discovery pace of 96.7% contrasted with different classifiers.

To utilize the irregular backwoods random forest classifier for distinguishing the sort of DoS assaults in WSNs. The proposed classifier accomplishes the best F1-score results are 96%, close to 100%, 98%, 96%, and 100 percent for flooding, blackhole, gray hole, planning to Time Division Multiple Access (TDMA), and typical assaults, separately [13]. In any case, the aftereffect of this review was for a few cases in the testing stage, which around addresses 25% (94,042 occasions) of the information. As [14] proposed a strategy for interruption location utilizing arbitrary woodland classifier and manufactured minority oversampling procedure. They involved the SMOTE procedure for oversampling the minority tests. The test after-effects of the review showed that the exactness of utilizing an irregular woodland classifier was 92.39% and the precision of utilizing SMOTE has expanded the exactness to 92.57%.

The Evolutionary Algorithms (EA) is a heuristic flexible search computation that was inspired by the transformational ideas of hereditary traits. It addresses a canny abuse that involves an irregular quest for tackling both unconstrained and obliged enhancement issues [15]. The EA monotonously modifies individual arrangements of a populace and at each progression, it chooses haphazardly people from the populace that are right now in the cycle to be guardians; then, at that point, it uses them to produce the youngsters for the up and coming age of populace. Going through the advancement of these sequential ages; the arrangement is improved to optimality. The hereditary calculation is utilized to take care of an assortment of issues, including blended whole number programming issues or the issues in which their genuine capacity is stochastic, non-differentiable, intermittent, or exceptionally nonlinear.

Slope supporting is an outfit learning strategy, utilized for arrangement and relapse issues, proposed by Friedman [16]. It can deliver a successful model comprising of powerless students, generally choice trees. The essential thought of slope is to fabricate and sum up the gathering model in a phase savvy design by upgrading a genuine inconsistent misfortune work.

Literature Survey:

Filter convention embraces a progressive organizational structure, what's more, is the main bunching steering convention planned by Cui et al. [17]. To expand the organization existence, every hub chooses the bunch beginning from side to side the political decision component, along with every "round" inside the organization determination lead the group leader political decision as well as organization redesign, and towards forestalling the bunch cranium on or after get-up-and-go disappointment because of extreme energy utilization. Based on the LEACH convention, ensuing specialists led numerous improvement studies and proposed DEEC [18], CRBED [19], and different techniques. In [20], focusing on the lack of the old-style grouping LEACH convention, the A GA-LEACH steering convention is proposed, which is a mix of a miniature hereditary calculation utilizing LEACH convention, to improve the group head determination as well as furthermore lessen the energy utilization of the organization. In [21], in every surrounding of bunch remaking, the drain calculates to be projected choose group heads in the group to lessen the energy misfortune. In [22], the no uniform grouping EEUC calculation was proposed. Groups of various sizes are set by the distance to the door hub, which safeguards the hot hubs and balances energy utilization. In [23], a calculation in light of circulated learning automata was planned. By choosing a subset of hubs in the organization, every hub was safeguarded by somewhere around one dynamic hub to accomplish the worldwide objective of the organization, and every hub acknowledged self-assurance, in this way drawing out the existing pattern of the hub. Article [24] introduced a Modified threshold-based Cluster Head Replacement (MT-CHR) convention. A novel likelihood of living being a group cluster, intended for any hub in any the round was proposed which concurred decently employing the presumptions presented in the LEACH convention. Another statement of edge energy is proposed, which considers deferring the passing of the main hub and staying away from any information.

Architecture Design:

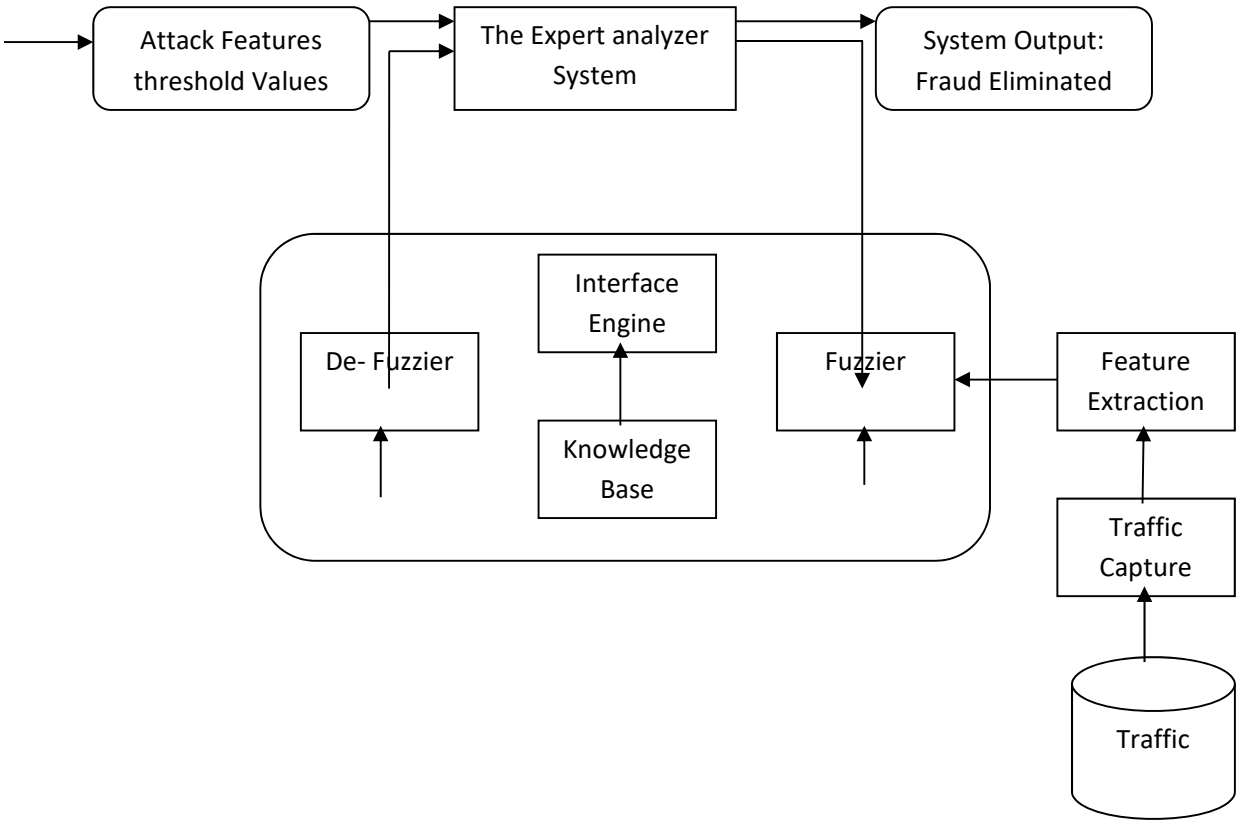

Fig 1: Architecture Diagram

In writing [25], H-LEACH innovation is wished-for to tackle the get-up-and-go thought issue inside the appointment of cluster heads. The edge situation is utilized to choose outlet head, in addition to the remaining liveliness and greatest liveliness of hubs in each round were thought of. Article [26] proposed a ravenous fractional inclusion (GPC) calculation, which utilized neighbor hubs to keep up with the availability of chosen hubs, and utilized the cross-over connecting hubs in the direction of accomplishing the necessary inclusion velocity, which further developed the inclusion rate and availability among hubs and diminished the power utilization of the organization.

In [27], the novel LEACH convention given proclivity engendering was proposed; it empowers a completely circulated manage and resolves commonsense limits of ordinary LEACH-based conventions through working on a set of connections functionalities as well as diminishing feeler equipment costs. In [28], and productive bunch head choice calculation, PSO-ECHS, given molecule swarm enhancement was proposed, and a successful molecule coding and wellness work plot were taken on to further develop the energy proficiency of molecule swarm improvement. In [29], it focused on late progressive directing conventions, which were relying upon the LEACH convention to improve its exhibition and increment the lifetime of the remote sensor organizations. Hub rank calculation relies upon both way cost and the number of connections between hubs to choose the bunch top of each group. Article [30] proposed the pDCDs calculation which was a knowledge machine base calculation for PCP. It tracked down hubs to screen percent inclusion into conveyed networks, which proficient occupied organization inclusion and essentially further developed the existing pattern of the organization. In [30], a better energy-saving (IEE-LEACH) convention was proposed, which thought about the energy of the leftover hubs and the normal energy of the organization. To acquire the ideal quantity of cluster heads, the hubs near the base station are denied from joining the bunch, which enormously decreased the power utilization of the remote sensor organization. The ancestors have done a great deal of examination on the LEACH convention to take care of the issues existing in the LEACH convention itself. However, they frequently upgrade the LEACH convention commencing a particular point of view, rather than according to various viewpoints.

Writing studies [7] and [13] improved LEACH convention through different calculations and zeroed in on energy research while disregarding different issues of LEACH convention, for example, information volume. Writing studies [8], [10], and [14] accomplished the motivation behind enhancement by concentrating on the area choice of group head hubs while overlooking different parts of LEACH convention, like organization inclusion. Writing [12] enhanced LEACH convention by lessening the equipment upward of remote sensor organizations. Commencing what have be examined over, the above research was completely cantered around the leftover energy of hubs or distance, utilizing different calculations enhancing LEACH arrangement and drawing out the organization life cycle. In any case, it overlooked the effect of group size on the organization and had no life cycle extensive enhancement energies, altitude, position, and some other contributing elements. Consequently the examination point is generally on its own. This paper advances and further develops the bunching technique in the protocol convention, changes physical dimensions were groups, along with dodges the arrangement of very huge bunches furthermore minuscule groups. bearing in mind the effect of several factor, for example, the leftover force of bunch start and focus of significance hub, remoteness, and indicate, beside choosing the focal point of gravity hub another group arrangement and information transmission component are proposed. Re-enactment marks demonstrate that the new bunching system can steadiness the power utilization of hubs and expand the existing pattern of remote antenna organizations.

Flow Chart:

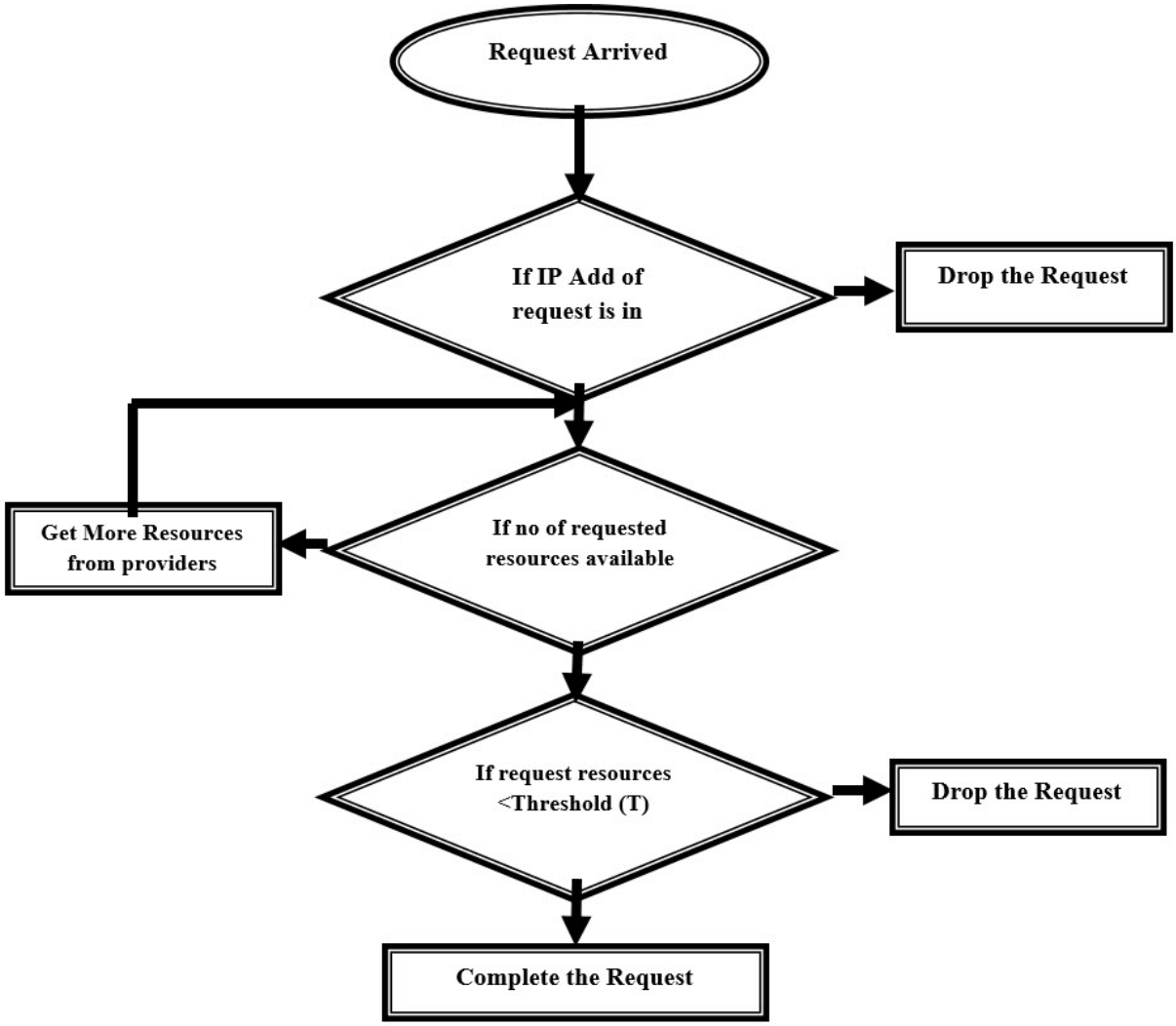

Fig 2: Flow Chart of DOS System

Sensor hubs are bunched utilizing the Distributed Clustering with Hybrid Energy Efficiency protocol. The CHS is picked dependent on two grouping boundaries: every hub's remaining energy and intra-bunch correspondence cost, which is a component of hub degree or group thickness. Regard outlives LEACH as far as organization life expectancy. On the off chance that a hub neglects to perform shared validation, it is named noxious. At the point when a CH recognizes a pernicious or traded-off hub, it requests that the KDS stop the undermined or vindictive hub's activities. The KDS erases the hub's mysterious key from the KDS records, bringing about a keyless hub. CHS sends an encoded message to any remaining bunch heads illuminating them regarding the recognized vindictive hub, keeping it from speaking with the remainder of the group. The exercises of the excess bunches do not interfere. It not just shields the remote sensor network from disavowal of-administration assaults, yet in addition guarantees sensor hub validity, realness, and classification. A bunch might be noxious if the assailant comprehends our interaction. This strategy is both compelling and exact.

The collaboration Focused on a game In WSNs, fuzzy Q-learning (G-FQL) combines the fuzzy Q-learning method along with a game-theoretic progress. On the off chance that the assaults are completed on a typical or sporadic premise, the IDPS may change its learning boundaries to recognize potential assaults utilizing fluffy Q-learning. Sink hubs, a base station, and a gatecrasher are the three parts in this three-player procedure game. Message assaults are observed by the sink hub utilizing a game-based FQL measure. At the point when the assailant attacks the sensor hub after finishing the initial step, the sink hub sends a caution to the base station. The recognizable proof wellness test is utilized in mix with the data set to decide assault examples and power in the wake of getting a sporadic sign from the sink hub. It additionally alarms the influenced sink hub that it should safeguard itself against the malignant assault design. On the off chance that the sink hub recognizes an inconsistency, it suggests that the identification procedure be amended. The component rehashes until the assault circumstance is settled and the cautious arrangement is reestablished to its unique state. The sink hub illuminates IDS2 that the sensor hub assault has been effectively countered and that the assault has finished. The IDS2 has now finished its protection of the sensor hub. Execution beats some other individual safeguard techniques when the game hypothesis and the Fuzzy Q-preparing structure are consolidated. During reproduction, the Game-FQL keeps a bigger amount of antenna hubs. Utilizing advancement, the agreeable game-based FQL approach improves oomph efficiency11.

Agreeable fluffy counterfeit insusceptible framework (Co-FAIS) sniffs network information and examinations sensor action progressively. The six components that make up the device are the Wireshark Modules, Flexible Exploitation Detection Subsystem, Hazard Detection Subsystem, Intuitive Lee Vaccination Subsystem, Collaborative Decisions - making Subsystem, as well as Rejoinder unit. The sniffer unit catches bundles as of online organization interchange as well as sends them to the location module for examination. When there is a lot of traffic, the sniffed information is taken care of to a disconnected worker, with the result is put away within a record document. A fluffy principle-based parcel analyzer is utilized seeing that a location unit to pre-measure bundle usefulness. The Fuzzy Misuse Detector Module computes the most elevated coordinating with esteem among bundles and self-parcels and afterward reports it. Catching traffic, including extractor, fuzzification, fluffy deduction motor, information base, and master analyzer are the segments of the FMDM. The danger profile is produced utilizing the organization traffic gathered by the capacity extractor. Computer processor use (Eu), memory load (Bs), transmission capacity immersion (Tr), and connection numbers are utilized to construct the danger profile (Co). The info/yield etymological factors are depicted in fuzzification. Participation capacities are likewise portrayed. The fluffy standards utilized by the fluffy derivation motor to acquire another reality are put away in the information base.

The master analyzer decides if assessed parcels are focused because of defuzzification. The Danger Detector Module analyzes the current framework's client profile to that of a standard framework put away in the profile information base, searching for and estimating expected deviations. It's utilized to recognize new dangers. By dissecting the conduct of a genuine assault in a controlled climate and testing the framework's capacity to react and secure itself, the Fuzzy Q-learning Vaccination Module refreshes data about the framework as far as limits, profiled devices, etc. The FMDM and FQVM finder results are joined in the Cooperative Decision Making Module. An ordered result is obtained, as well as knowledge of the attack source, which depicts what the true cause for the attacking maybe, and also the identity of both the onslaught if the machine is aware of it. The Answer Module adjusts has in the organization or updates information bases. The reaction module creates an assault mark and eliminates it from the protected rundown, taking into account a speedier reaction to a similar assault later on. The arrangement module goes about as a safeguard component, making a quick online move to stop the assault. The FAIS that is centered around participation has a higher exactness positioning. It has a higher pace of identification. It additionally considers the protection of a bigger number of sensor hubs. The pace of energy utilization is lower. Be that as it may, planning time is considerable2.

The methods are differentiated as far as routing calculation, assessment boundary, assault location boundary, malevolent hub conduct, and positive hub conduct. To stay away from a DoS assault, every strategy distinguishes the malignant hub and endeavors to confine it from the organization. To upgrade network security, Co-FAIS identifies assault conduct and cautions its part hubs to the assault design. Nonetheless, it has a few blemishes, for example, an absence of learning capacities and the way that it depends on a standard model made online that doesn't change over the long haul during discovery.

Table 1. Summary comparing Network attacks mitigation approaches

Techniques Name	Malicious Behaviour	Good deeds are rewarded	Parameter	Protocol	Parameter of evaluation
Game Theory Approach	Blackhole and Fault node Message	Status	Status	Utility-based unique source Routing convention	Mean bundles drop
Authorizing Security utilizing Economical Modeling	None Helpful Nodes	Status	-	Secure Auction based directing convention	Mean bundles drop
Frequent Game Theory Approach	Consent to advance bundles is come up short	Status	Charge of Forward	Game theory protocol	No of the hops received packets
Strength-based detection and prevention	None Cooperative Nodes	Status		S-LEACH	Total packet received
An ANT based Framework	Respond of Hello Messages	Indication Potency	Indication Potency	ANT Based Procedure	Network lifetime energy used
Production using KDS	Flooding	Reliability	-	HEED Protocol	-
Message Observation Mechanism	Node replication capture nodes	Manual Authentication	No of Message and Content of message	Message Observation Mechanism protocol	The loss rate of packets

In this paper, a resistant framework for DoS assaults on WSN is proposed. There are a couple of huge issues to recall. Because of the fast development of remote sensors, securing sensor hubs is troublesome work. It ought not to corrupt the framework's exhibition while forestalling a DoS assault. It should keep its exactness. The pace of bogus alerts ought to be insignificant. The anticipation system ought to have the option to withstand rehashed assaults on a similar hub. New learning boundaries are being considered in our proposed structure to expand framework precision and recognize various assaults

Proposed System:

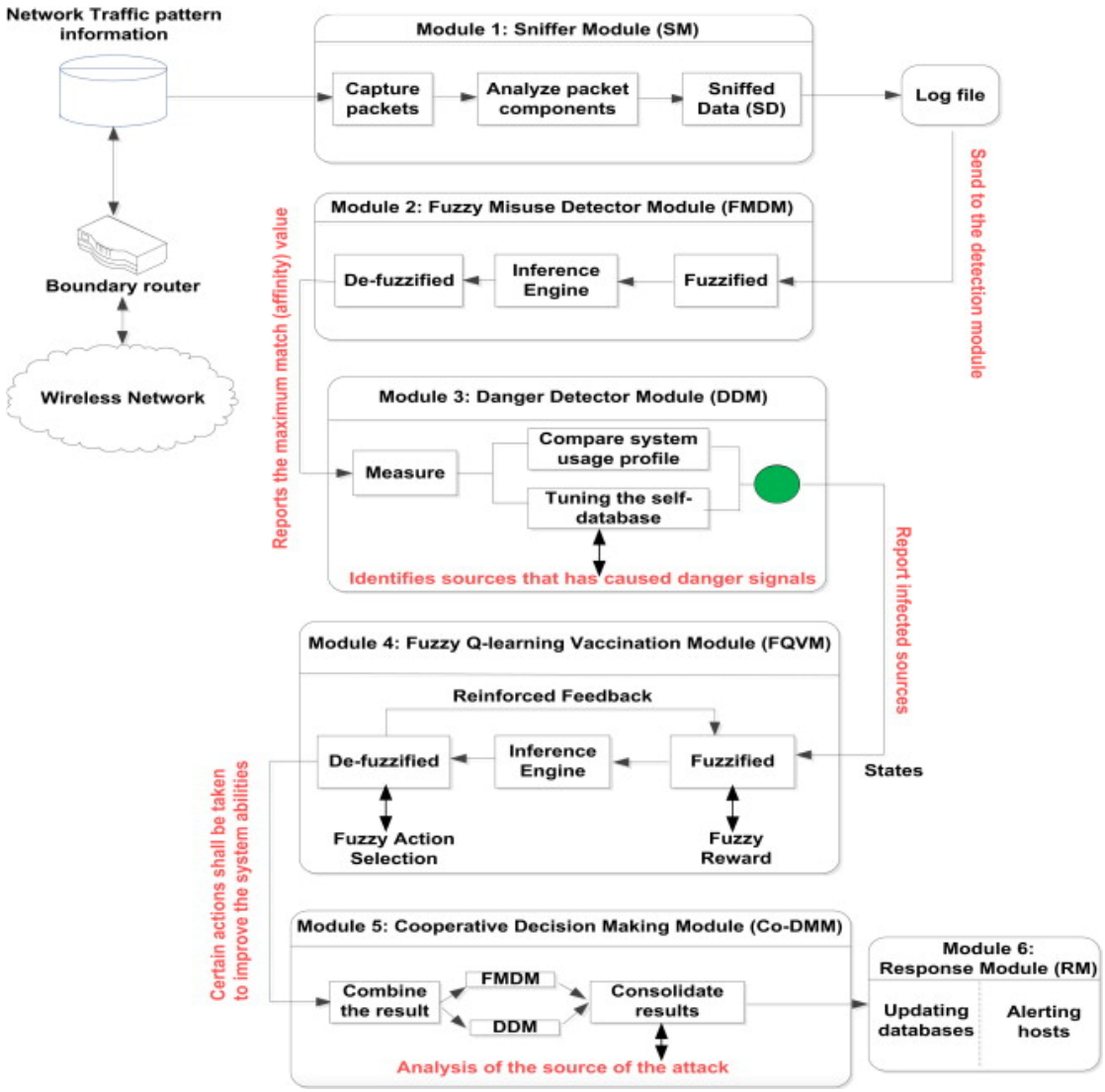

Fig 3: Proposed Co-FAIS System

The Co-FAIS infrastructure is impregnable to Cyberattacks on WSN. It is the primary ongoing interruption discovery model. It utilizes fluffy rationale to compare the current framework to the standard framework to recognize the assault. It does, nonetheless, have a few disadvantages, for example, an absence of learning abilities and the utilization of a solitary ordinary model that doesn't move over the long run during discovery. Thus, the standard model should be refreshed in contrast with the new system. Additional learning boundaries can be applied to the structure to upgrade learning abilities. By adding two learning boundaries to the fluffy framework, the proposed insusceptible framework would help the current Co-FAIS. It will expand identification precision and improve learning.

The six modules in the proposed resistance architecture are the Sniffer Module (SM), Fuzzy Misuse Detector Module (FMDM), Danger Detector Module (DDM), Fuzzy Q-learning Vaccination Module (FQVM), Cooperative Decision Making Module (Co-DMM), and Response Module (RM). Figure 1 depicts the suggested resistance structure for a DoS attack on WSN. In the secret segment, you'll track down the two fleecy modules. In the proposed procedure, we changed the number of learning limits. We acquainted two new learning limits with the current Co-FAIS: Throughput and Sleep Interval.

Module sniffer

It gathers bundles from online organizations and sends them for pre-handling towards the Fuzzy maltreatment identification module It makes parcels log accordingly.

Module for Fuzzy Misuse Detection

It's a fluffy-based module that recognizes pernicious bundles. It thinks about the current bundle to the standard parcel and reports the qualities that surpass the limit. Catching traffic, work extractor, fuzzification, fluffy surmising motor, information base, and master analyzer are all important for it. The danger profile is created utilizing the organization traffic gathered by the capacity extractor. The danger profile in the current system is centered around CPU utilization (Eu), memory load (Bs), data transmission immersion (Tr), and the number of associations (Co). The danger profile in the current structure is centered around CPU utilization (Eu), memory load (Bs), transmission capacity immersion (Tr), and the number of associations (Co). The quantity of boundaries in the proposed technique has been expanded. Two extra boundaries, throughput (Th) and rest stretch (Si) have been applied to the proposed framework throughput (Th) and rest span (Si), which will build the framework exactness. Six boundaries currently distinguish a danger profile (TP). TP = Eu, Bs, Tr, Co, Th, Si, where Eu signifies the energy utilization of the sensor hub; Within a particular time frame, Tr denotes the range of the time difference between two associations; The length of the packet between source to objective is denoted by Bs and the number of associations with the same hosting as even the previous association in the last two seconds donated by TP. Tt represents throughput, which are characterized as quantity of effectively got bundles in a given measure of time. The hub's rest period is Si. The information/yield semantic factors are portrayed in fuzzification. These factors are referenced in Table 2. Enrolment capacities are additionally depicted. The fluffy standards utilized by the fluffy deduction motor to acquire another fact are put away in the information base. The master analyzer decides if tried parcels are focused because of defuzzification.

Table 2. Displays the variable abbreviations and fuzzy linguistics for each parameter.

Boundaries	Inputs etymological factors	Range
Power utilization (Pu)	Small (S), Average (A),	1-150 (J)
Barrier size (Bs): kb	Lofty (L)	5-7805 (Kb)
Moment in time response (MTr): ms		0-110 (ms)
Calculate (Ca): ms		1-5 (%)
Throughput (Tt): bps		76-99(%)
Slumber Distance (SD): ms		6-99(ms)

Module for Detecting Danger

Assuming an assault is noticed, this module estimates the contrast among malignant and customary bundle boundaries. It's even saved in an information base with the goal that new dangers can be found.

Vaccination Module of Fuzzy Q-learning

In this module, genuine assaults are noticed. It tests the framework's capacity to identify and secure against an assault. The attack is distinguished utilizing the Fuzzy Q-learning calculation. The fluffy min-max activity determination and award work is joined with conventional Q-learning in this calculation. It is comprised of a fluffy regulator that changes constant contributions to fluffy sets. For the fluffy Q-learning input, six fluffy sets have been portrayed to address six distinct circumstances as a Q-learning state space. Power utilization (Pu), Moment in time reaction (MTr), Barrier size (Bs), Calculate (Ca), Throughput (Th), Slumber Distance (SD) are fluffy Q-learning inputs that compare to the organization's fluffy state. Specialist A's conduct is addressed by irregularity, which is the yield of the FQL (t). The fluffy sources of info are utilized to depict fluffy laws. To demonstrate the noticed assault conduct, fluffy states are utilized. Given the fluffy rationale regulator, the FQL specialist doles out a load to all conceivable next states (FLC). It is feasible to accomplish ideal expense by a partner it with the edge esteem.

LEACH B (BALANCED LEACH) Algorithm:

A LEACH-B calculation to balance the quantity of CHs relying upon the excess energy of hubs. the underlying decision of group heads relies upon LEACH's fundamental calculation and from the second round, LEACH-B is utilized. Filter B is a close ideal directing technique. Filter B's decentralized methodology is utilized during the time spent framing a bunch in which every hub knows its area and the area of the last objective paying little mind to where the organization rest hub is found. Drain B works in three phases: Cluster head determination. Group development. Information transmission with numerous gets to. Each hub picks its group head contingent upon the disseminated energy in the way between the hub and the last beneficiary. Drain B is more energy-proficient than the LEACH protocol [14, 15].

```
Cluster head election
//The process of CH election is similar to that of E-LEACH
Cluster Set-up Phase
1: BC (ADV); //CH broadcast adv message;
2: Join(IDi); //non CH node i join
3: Cluster(CH); // form a cluster CH;
//Proposed Scheme
4: Record(nCH); //save the neighbor CH data
 //(distance of the CH to the nCH and distance of the nCH to the BS)
 if(CH{s} =TRUE){
 while (nCHi_BS < CH_BS){
 nCH_candidate(nCHi)
 }
 if (num_nCH_candidate > 0){
 for (i=0;i<num_nCH_candidate;i++){
 search_nearest_nCHi
 }
 Join(nCHi)
 TransTo_nCHi
 }else{
 TransToBS
 }
 }
```

A module on Collaborative Decision Making

The results of the FMDM and FQVM detectors are combined in this module. It compiles the results and analyses the attack source.

Module of Reaction

This module makes modifications to databases or network hosts. It generates an attack signature and removes it from the safe list to speed up prevention.

Results:

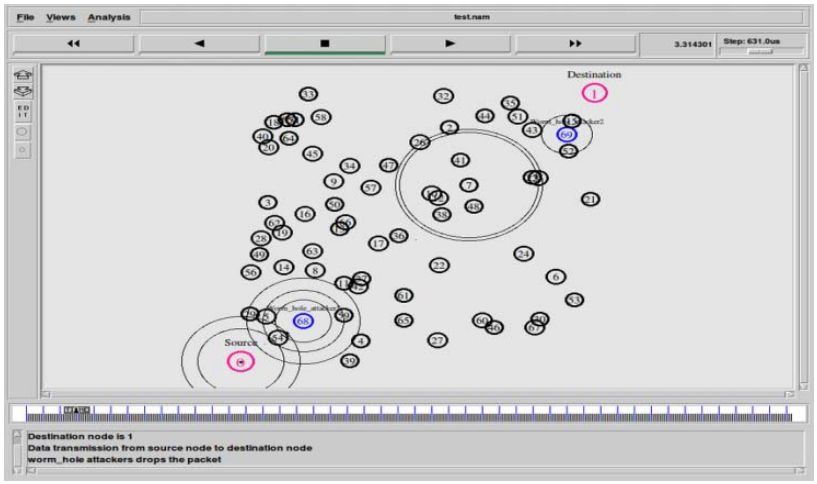

Figure 1: Data Transmission

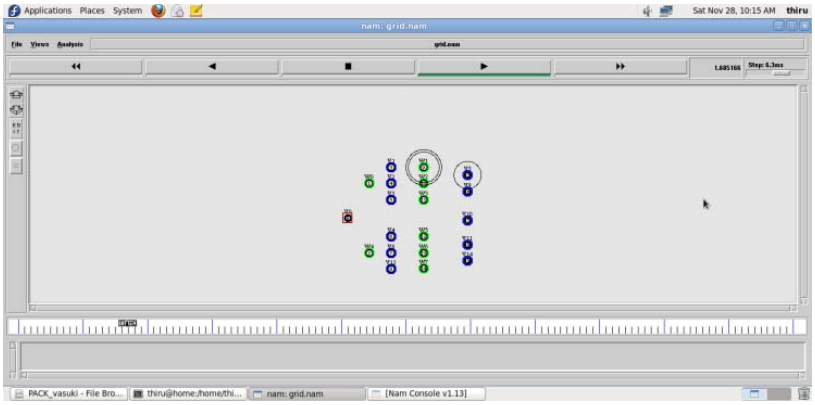

Figure 2: Assemble the Route in the topology area

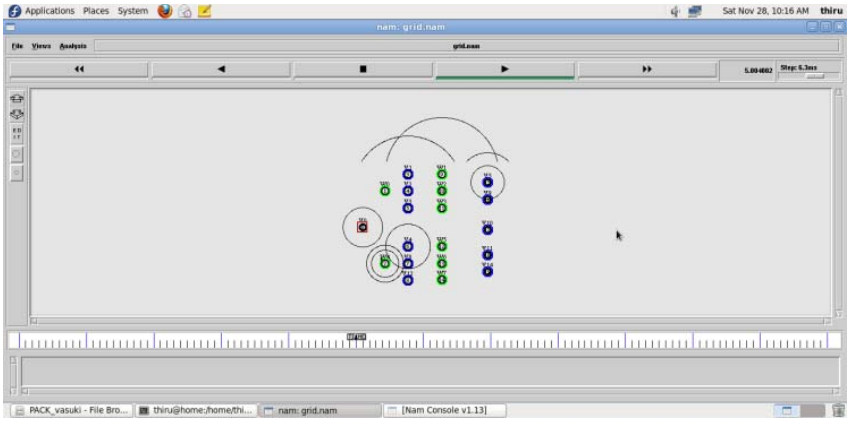

Figure 3: Sequence Data Transmission

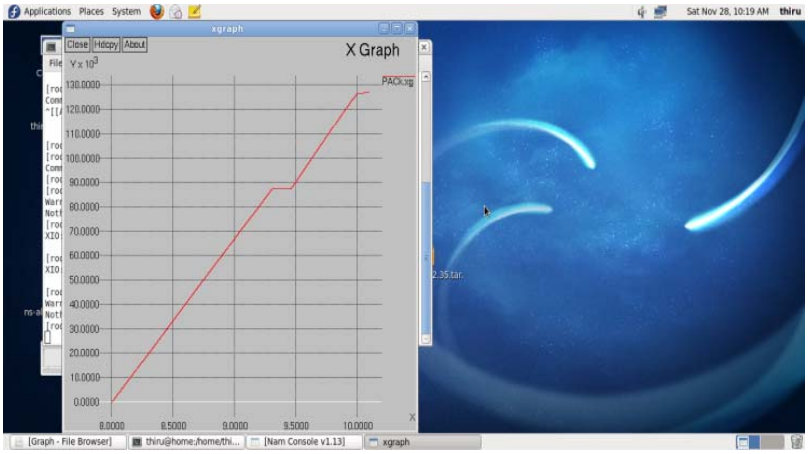

Figure 4: Energy Throughput

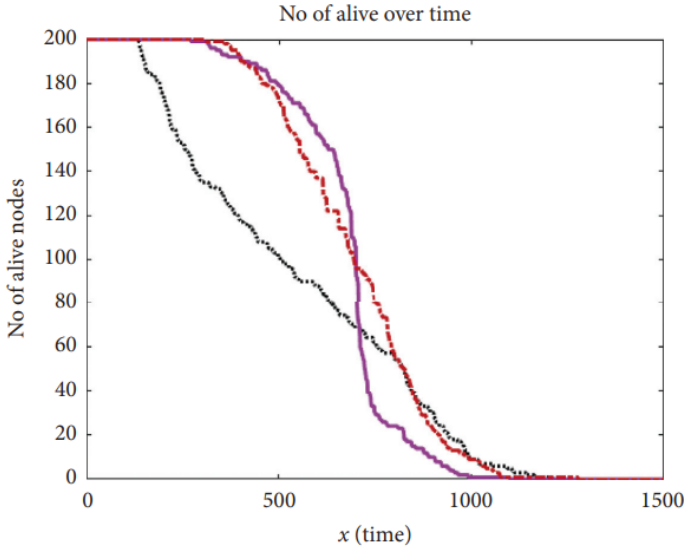

Figure 5. Comparison of alive nodes over time

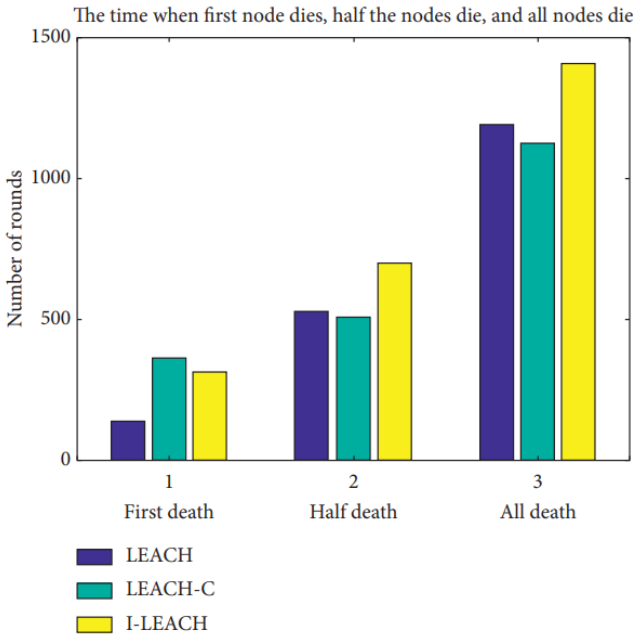

Figure 6. Comparison of network life cycle

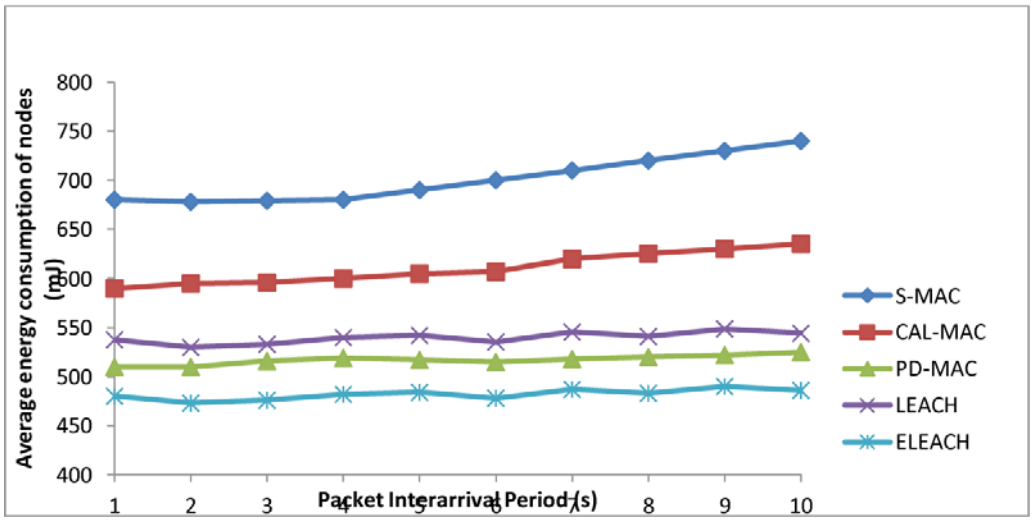

Figure 7 : Average Energy Consumption Nodes

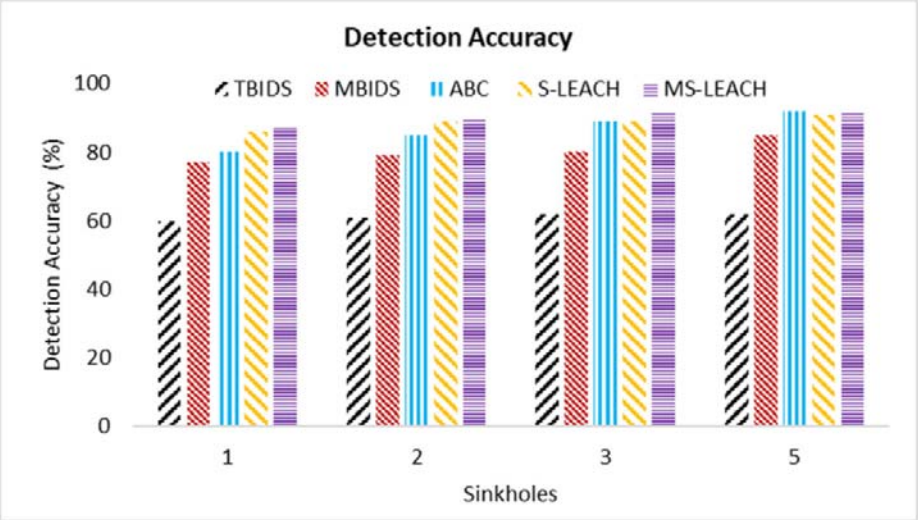

Figure 8: Detection Accuracy

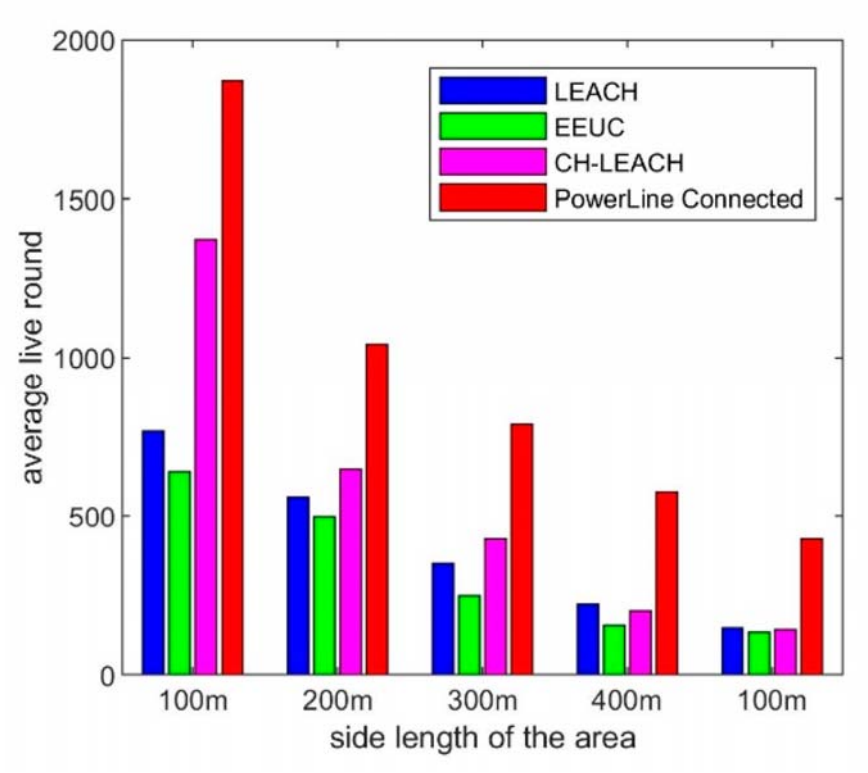

Figure 9: Side Length and Average Lie Round

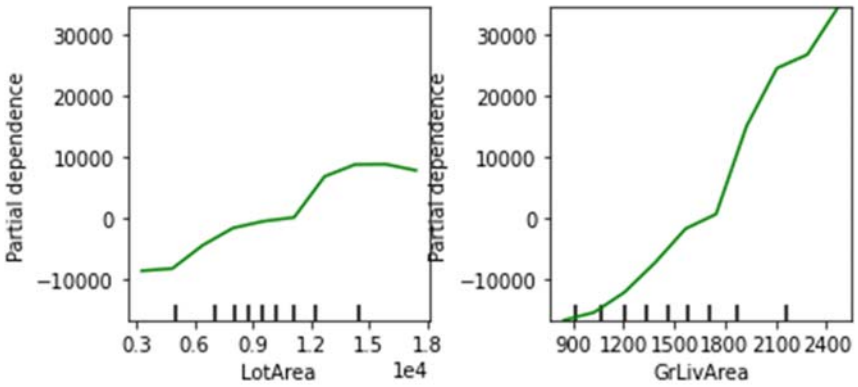

Figure 10: Side Length and Partial Dependence

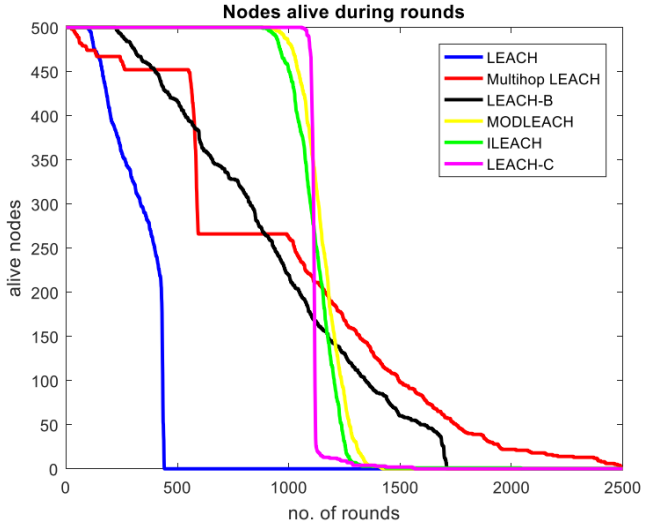

Figure 11. Number of alive nodes

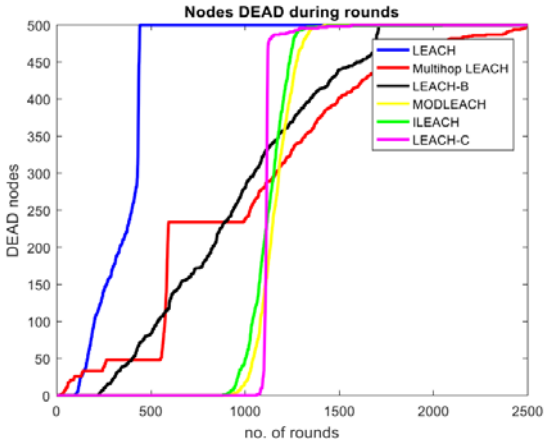

Figure 12. Number of dead nodes

Conclusions:

The system's output is harmed by a Dos attack. The most serious concerns regarding wireless sensor networks are data privacy and stability. To counteract cyber attacks in WSNs, special prevention techniques are needed. There are a few methods and strategies that can be used to protect the system from DoS attacks. Our proposed cooperative immune system is an improvement on Co-FAIS, the conventional immune system. It increases the system's accuracy. It lowers the number of false alarms. The assault is analyzed using two different parameters.

References:

[1] Abdullah, M.A.; Alsolami, B.M.; Alyahya, H.M.; Alotibi, M.H. (2018): Intrusion Detection of DoS Attacks in WSNs Using Classification Techniques. J. Fundam. Appl. Sci. **10**, pp.298–303.
[2] Afraid Agah, Kalyan Basu, and Sajal K Das (2005): Use economic modeling to enforce security in wireless sensor networks to avoid dos attacks. In, at the Mobile Adhoc and Sensor Systems Conference. IEEE **8**. pp.,
[3] Afraid Agah, Kalyan Basu, and Sajal K Das, (2005): A game-theoretic approach to preventing dos attacks in sensor networks., Communications. ICC 2005, **5**, pp. 3218–3222, IEEE International Conference, IEEE.
[4] Ahmed AlB and ElS. Ayman,(2017): A new algorithm for cluster head selection in LEACH protocol for wireless sensor networks, International Journal of Communication Systems. **31(**1).
[5] Aikaterini, Mitrokotsa and Christos Douligeris, (2004): DDoS attacks and countermeasures: description and current state of the art Computer Networks, **44(**5), pp. 643–666,.
[6] Cui Z., Cao Y., Cai X., Cai J., and Chen J.., (2019): Optimal LEACH protocol with modified bat algorithm for big data sensing systems on Internet , Journal of Parallel and Distributed Computing, **132**(), pp. 217–229.
[7] Darabkh K. A., Al-Rawashdeh W. S., Hawa M., and Ramzi S. (2018): M. T.-CHR: A modified threshold-based cluster head replacement protocol for wireless sensor networks, Computers & Electrical Engineering, **72**, pp. 926–938.
[8] Deng-Ao L., Hai-Long H., Jin-Long G., et al., (2015): Clustering and Inter-cluster routing algorithm for wireless sensor networks with energy efficiency, Automation Instrumentation, **36(**12), pp. 4–7.
[9] Dimple Juneja and Neha Arora ( ) In wireless sensor networks, an ant-based framework for preventing DDOS attacks has been developed. preprint arXiv:1007.0413,
[10] Dines Kumar. V.S and Navaneethan.C (2014): Protection against denial of service (dos) attacks in wireless sensor networks, International Journal of Advanced Research in Computer Science and Technology, **2**: pp.439–443, .
[11] Kaur A.and Grover A., (2015): LEACH and extended LEACH protocols in wireless sensor network-A survey, International Journal of Computer Applications, **116(**10), pp. 1–5.
[12] Kitjacharoenchai, P., Ventresca, M., Moshref-Javadi, M., Lee, S., Tanchoco, J.M.A., Brunese, P.A. (2019): Multiple traveling salesman problem with drones: Mathematical model and heuristic approach. Comput. Ind. Eng., **129**, pp.14–30.
[13] Le, T., Park, T. Cho, D., Kim, H. (2018): An Effective Classification for DoS Attacks in Wireless Sensor Networks. In Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic; pp. 689–692.
[14] Liu. Y., Q. Wu., Zhao. T., Tie. Y., Bai., F., and Jin. M., (2019): An improved energy-efficient routing protocol for wireless sensor networks, Sensors (Basel, Switzerland), **19(**20).
[15] Miss Laiha Mat Kiah, Ajith Abraham, Shahaboddin Shamshirband, Ahmed Patel, Nor Badrul Anuar (2014): A cooperative game-theoretic approach using fuzzy q-learning is used to detect and avoid intrusions in wireless sensor networks. Engineering Applications of Artificial Intelligence, pp. 228-241.
[16] Mostafaei H. and Obaidat M. S., (2017): A greedy overlap-based algorithm for partial coverage of heterogeneous WSNs, in Proceedings of the GLOBECOM 2017 - 2017 IEEE Global Communications Conference, pp. 1–6.
[17] Mostafaei H., M. U. Chowdhury, R. Islam and *et al.,* (2015): Connected P-percent coverage in wireless sensor networks based on degree constraint dominating set approach, in Proceedings of the Mswim 15 cm International Conference on Modeling. ACM, Cancun, MX, USA,pp. 157–160.
[18] Mostafaei H.and Obaidat M. S., (2018): A distributed efficient algorithm for self-protection of wireless sensor networks, in Proceedings of the 2018 IEEE International Conference on Communications (ICC), IEEE, Kansas City, MO, USA.
[19] Nehra V., Sharma A. K., and Tripathi R. K., (2019): I-DEEC: improved DEEC for blanket coverage in heterogeneous wireless sensor networks, Journal of Ambient Intelligence and Humanized Computing, **11(**9), pp. 3687–3698,.
[20] Pooya Moradian Zadeh, Maryam Mohi, Ali Movaghar (2009): Preventing DoS attacks in wireless sensor networks using a Bayesian game strategy. WRI International Conference . IEEE **3**, pp. 507–511.
[21] Radhika M. and Sivakumar P., (2020): Energy optimized micro genetic algorithm based LEACH protocol for WSN, Wireless Networks, **8** (1).
[22] Rao P. C. S., Jana P. K., and Banka H, (2017): A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks, Wireless Networks, **23**(7), pp. 2005–2020.
[23] Sajal K Das and Afraid Agah, (2007): A recurring game theory approach to preventing dos attacks in wireless sensor networks. International Journal of Network Security, **5**(2), pp. 145–153.
[24] Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha Mat Kiah, Vala Ali Rohani, Dalibor Petkovic, Sanjay Misra, and Abdul Nasir Khan, (2014): Co-fais is a mutual fuzzy artificial immune system for wireless sensor networks that detects intrusion, Journal of Network and Computer Applications, **42**:pp.102–117.
[25] Sivakumar P. and Radhika M., (2018): Performance analysis of LEACH-GA over LEACH and LEACH-C in WSN, Procedia Computer Science, **125**(1), pp. 248–256.
[26] Sohn I., -H. Lee J,. and S. H. Lee, (2016): Low-energy adaptive clustering hierarchy using affinity propagation for wireless sensor networks, IEEE Communications Letters, **20**(3), pp. 558–561.
[27] Sweta Jain, Aishwarya S Anand Ukey, and Virendra Pal Singh. Hello, (2013): Flood attack detection and prevention in wireless sensor networks based on signal power. International Journal of Computer Applications pp.0975–8887.
[28] Tan, X., Su, S., Huang, Z., Guo, X., Zuo, Z., Sun, X., Li, L (2019): Wireless Sensor Networks Intrusion Detection Based on SMOTE and the Random Forest Algorithm. Sensors, **19**, pp.203.

[29] Wang L., B. J. Xie, Z. Z. Liu, et al., (2017): Improved algorithm for a non-uniform clustering routing protocol, Computer Science, **44(**2), pp. 152–156,.
[30] Yuan-an Liu, Yi-Ying Zhang, Xiang-Zhen Li, and Yi-Ying Zhang (2012): Dos attack detection and protection for wireless sensor networks. Chinese Universities of Posts and Telecommunications Journal, **19**: pp.52–56.
[31] Zhang, C., Zhang, Y., Shi, X., Almpanidis, G., Fan, G.; Shen, X (2019): On Incremental Learning for Gradient Boosting Decision Trees. Neural Process. Lett., **50**, pp.957–987.

Authors Profile

B.Bharathi Kannan is a Research Scholar in the School of Computing Science and Engineering, Galgotias University (GU), Greater Noida, Uttar Pradesh, India. He has completed his B.Tech and M.Tech from reputed institutions. His research interest is mainly focused on Wireless Sensor Networks, Cloud Computing and Internet of Things (IoT).

Dr.S.Srinivasan is working as a Professor in the School of Computing Science and Engineering, Galgotias University, Greater Noida, UP, NCR- Delhi, India. He has completed his Ph.D. in Computer Science and Engineering from Anna University, Chennai and obtained his BE and ME from reputed universities. He has presented and published papers in various National and International Conferences and Journals. He has more than 22 years of experience in the field of teaching. He is expertise in Image Processing, Big Data, Cloud, IOT and Artificial Intelligence.