Protected Combination Of Artificial Neural Network With Wireless Sensor Networks

Pardeep Kumar, Udayabhanu N P G Raju

Abstract: ***WSN offers a down to earth arrangement of conveyed detecting, preparing, communication and control while ANN's self-adaptively and nonlinear mapping capacity make it progressively invaluable in displaying nonlinear framework or framework with obscure dynamics. We feel that the blend of WSN and ANN can be an incredible demonstrating arrangement. First, a trainable ANN demonstrate assembled itself from test information, subsequently, adequate information sources are important to acquire a precise ANN show. The rich sensor information from WSN consequently can be utilized in preparing the ANN. Likewise, WSN information based ANN displaying has high down to earth esteems: the conduct of certain framework is exceptionally perplexing and hard to examine, particularly when numerous nonlinear and time-differing impacts are available.***

Index Terms: ***ANN, Malicious Traffic Flow, Energy Consumption, WSN.***

I. INTRODUCTION

Wireless Sensor Networks (WSN) is considered as a noteworthy innovation as far back as its introduction to the world, a wireless sensor network (WSN) comprising of self-ruling sensor nodes can give a rich stream of sensor information speaking to physical estimations. It very well may be portrayed as a network of dispersed self-fueled nodes that could detect or trade with condition. The fundamental preferred standpoint of WSN is that it could be effectively and quickly introduced and accumulate data for an extensive stretch of time, giving a tremendous amount of sensor information. WSN based applications have appeared fast development in an assortment of fields, including target following and reconnaissance, cataclysmic event help, wellbeing observing, condition investigation and land detecting, and so forth [5]. Up until this point, a large portion of the sensor networks conveyed include a generally set number of sensor nodes. They are normally associated with a focal preparing unit where all flag handling is performed [6]. Despite what might be expected, the WSN is a wireless appropriated network, in which the flag preparing is regularly finished with acquisitions. To more readily comprehend the need of sending WSN in genuine applications, some portrayal and articulation ought to be made:

- Wireless Cabled sensors networks work superbly when nodes can be wired to stable energy sources and dependable foundation of communications. In any case, in numerous pragmatic applications, the checked target-territory does not prepared any of these, for instance, when the observing target is a gathering of wild creatures in the nature. Subsequently sensor nodes ought to depend on nearby, limited, and moderately little energy sources just as wireless communication channels, this would open another entryway for more extensive applications with portability and Autonomy.

- Distributed detecting, when an exact area of the intrigue zone is obscure in an observation zone, WSN permits an appropriation of progressively independent sensors in the spot nearer to the needed checking region. Rather than utilizing just one or couple of sensors, this gives progressively flag to clamor proportion (SNR) and better open doors for the viewable pathway. SNR can be tended to at times by the arrangement of a high affectability sensor, nonetheless, the observable pathway of and all themore for the most part aggravation of clamor can't be prepared by the organization of a sensor with high affectability. Consequently, disseminated detecting gives more strength under various natural conditions.

- Distributed preparing: It might be viewed as sensible that in the cabled sensor networks, information can be conveyed back to a focal handling unit. In any case, for the sensor nodes of WSN, there are two principle hindrances: first, the limited energy spending plan is the first essential imperative. RF (Radio Frequency) Communication makes the fundamental energy buyer. Also, most wireless sensor network characterized restricted information transmission rate. Consequently, we have to process information however much as could reasonably be expected inside the network to decrease the energy utilization just as the quantity of bits transmitted, especially over longer separations.

Artificial Neural Network (ANN)

PC has become an essential device in building. Architects have utilized different PC applications to improve their productivity and execution. As far back as mid 70s, Artificial Intelligence (AI) have been executed by architects to perform specific undertakings plan.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)

Dr.Pardeep Kumar*, Department of CSE , Vignan Institute of Technology and Science, Hyderabad, India.
Dr. Udayabhanu N P G Raju, Department of CSE , Vignan Institute of Technology and Science, Hyderabad, India.

Despite the fact that PCs are engaged with an assortment of designing exercises, as of now, the primary programming material territories are with all around characterized rules, for example, the complex investigation, realistic and CAD applications, and so forth. Be that as it may, where there are no characterized standards or heuristics, the utilization of PC is restricted. Artificial Neural Networks (ANN) are another AI application that has as of late been generally used to show nonlinear framework, or framework with obscure dynamics in a wide range of spaces of science and designing [7]. ANN has been observed to be incredibly helpful in circumstances where the tenets are either obscure or are hard to express. A portion of the principle qualities of ANN can be recorded as pursues:

1. ANN can take in and sum up from guides to deliver commonsense answers for issues.
2. They can impeccably adapt to circumstances where the information of the network is misty or inadequate.
3. ANN can adjust arrangements in time and to remunerate from changing conditions
4. The information for preparing an ANN can be hypothetical information, test information or exact proof based on dependable encounters.

ANN can be considered as a decent summed up approximator based on the experience of a lot of preparing information, it contains no express standards. Despite the fact that it might not have the precise convention as the customary parametric methodologies, it is as yet an incredible asset that can deliver impeccable approximations when formal customary arrangements experiences issues with lacking learning of the issue. It is picked for applications where accuracy of conventional systems can't meet the prerequisite that the issue is too perplexing to even think about modeling with tenets [4].

Combination of WSN and ANN in modeling

WSN and ANN together have scarcely been utilized in demonstrating. Nonetheless, we think there are two principle points of interest of applying WSN and ANN in displaying and framework recognizable pieces of proof. First, the nature of WSN and ANN make them a mix: WSN could be effectively and quickly actualized, giving a gigantic amount of sensor information. These information sources can be fundamental for the ANN to distinguish a fine grained model. Second, they have high reasonable qualities : customary numerical displaying, Take the warm demonstrating of structure rooms for instance, approaches like [8] are normally settled with very much characterized conditions, they are typically utilized when all is said in done recreations rather than useful applications. It is essentially in light of the fact that these models are based on components, for example, room warm capacitances/obstruction, wind stream rate, heat exchange coefficient, heat gain coefficient, and so forth. These parameters are hard to gauge unequivocally in structures. Additionally, the dynamic conduct of some marvel is mind boggling 1, It is almost difficult to acquire an exact numerical model with set number of framework parameters. The WSN framework, despite what might be expected, is exceedingly transplantable as it could be immediately prepared under any ecological surroundings to accumulate constant warm information. Also, with its self-versatile learning and mapping capacity, ANN can straightforwardly reenact the relations between the demonstrating article's sources of info and yields. Based on the two reasons, it appears that the mix of WSN and ANN can be an important and sensible answer for demonstrating.

II. LITERATURE REVIEW

The raised prevalence of WSN had been confronting a few security dangers and stages. Creating comparing countermeasure components experienced difficulties spoken to by the sensors measure, handling force and memory confinements. Information inside a water contamination observing framework ought to be shielded from any unapproved party since water is the fundamental asset of life for all nations, so security instruments are basic to see classification, accessibility and trustworthiness of the WSN segments including equipment gadgets, programming, networking types of gear and gathered information [7].

Assaults in WSN are sorted to two primary methodologies; either assaults against the utilized security instrument or assaults against the steering system. An assault that expects to hack the security instrument by misusing its shortcomings relies upon the component qualities while the keep going relies upon hacking the directing calculations inside the network [8] [12]. Refusal of administration assault (DoS) keeps the typical utilization of the communication offices inside the network by depleting its assets with additional transmitted packets; it expects to flood the network with futile information and may inevitably disturb the entire network [5]. Sybil assault is another danger in which a node guarantees various personalities so it benefit and interface as a lot of real nodes, information respectability and asset usage debases and therefore network conventions might be upset [11]. In dark entire assault a vindictive node endeavors to follow and draw in the rush hour gridlock in the network, when the adversary can get to, convey and partake in the network the whole readings could be influenced particularly in the hierarchal network topologies where information is transmitted going through a few nodes. Hi flood assault is fused by a remote foe who can flood hi solicitation to any real node in the network and break the security system, while in wormhole assault the assailant record the packets and forward to another area, at least one phony nodes are utilized with a course between them, when the malevolent node begins its work a phony course is utilized to give a way that is shorter than the first one, and subsequently the information is burrowed inside the unfortunate course [9]. Fundamentally WSN protective line relies upon the utilization of customary key methodologies for interruption identification and counteractive action, symmetric encryption procedures help to shroud the substance of transmitted packets through the network to such an extent that no pernicious node can make utilization of scrambled information regardless of whether it get the figured packets, and this is recognized by its decreased overhead contrasted and open encryption calculations. The network is as yet confronting the past sorts of assaults however despite the fact that the accessible assets inside the network are constrained extra procedures are required close to cryptography to guarantee the framework security [10].

III. PROPOSED METHODOLOGY

The proposed security system is skilled to recognize and keep an energy depletion assault. We are utilizing a bunch based WSN and an Artificial Neural Network. We expect that every one of the nodes in WSN are static in nature. The whole network comprises of two sorts of nodes, for example sensor nodes and bunch heads. Sensor nodes are utilized to gather and assemble data from environment while bunch heads are dependable to screen and gather data from every one of the individuals from that specific group, for group development and group head decision. In this figure, two jump away neighbor nodes can join the bunch head "C". We accept that all the sensor nodes are equipped for energy gathering utilizing daylight as the wellspring of outer energy.

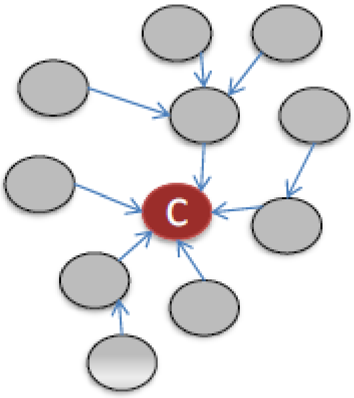

Figure 1: Dual stage clustering mechanism

A kind of network in which nodes are dealt with like artificial neurons is known as ANN. ANN is roused from normal sensory system in which if regular neuron gets solid signs initiates explicit neuron which thusly produces yield signals. An artificial neuron comprises of four segments, for example inputs, loads, enactment capacity and yield [45]. The summed up design of ANN is given in Figure 2.

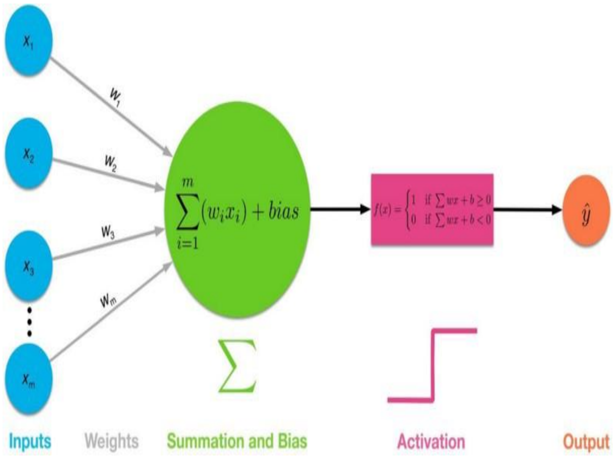
X_1
X_2
X_3
X_m
W_1
W_2
W_3
W_m
$\sum_{i=1}^{m}(w_i x_i) + bias$
$f(x) = \begin{cases} 1 & \text{if } \sum wx + b \geq 0 \\ 0 & \text{if } \sum wx + b < 0 \end{cases}$
$\hat{y}$
Σ
Inputs
Weights
Summation and Bias
Activation
Output

Figure 2. Generalized artificial neuron

In figure 2, distinct contributions of various loads are caught, and if a few loads coordinate an edge esteems, it might actuate the capacity to produce a yield. Neural network design comprises of three sorts of layers, for example, input, covered up and yield [6]. Our methodology is using unsupervised back proliferation based learning in which limit esteems are utilized as actuation work. Back spread technique is utilized. Whenever yield esteems don't matches, it very well may be balanced. The proposed model works in three stages:

- Gathering information – in this stage, each wireless sensor node monitors the packets got from neighbors, packets sent to neighbors and normal energy utilization in a particular timeframe. This stage may take a few days to get couple of ideal estimations of the framework utilization over a particular timeframe.
- Training stage – in this stage, ANN is prepared to recognize distinctive sensor nodes which are situated in its encompassing. In this stage, sensor node learns the normal number of packets each neighboring is sending over explicit time.
- Results – In this stage, the execution of ANN is tried. Presently the framework is fit to separate typical and malignant traffic stream.

$$\begin{cases} \mathit{Normal} = \{(N,A),(N,I),(N,S)\} \\ \mathit{Malicious} = \{(L,A),(L,I),(L,S),(H,A),(H,I),(H,S)\} \end{cases} \quad (1)$$

The issue which we are confronting is the distinguishing proof of typical or pernicious traffic streams. As we probably am aware, malignant traffic streams will be utilized to lead energy weariness assault against sensor node(s). This sort of calculation requires three-layer ANN. In which

- Input layer comprises of six neurons which speaks to ordinary, low force and high power assault. It additionally speaks to dynamic, inactive and rest mode.
- A concealed layer of four neurons.
- A yield layer of two neurons.

We allocated diverse loads to various conditions given in Table 1. It speaks to relegated qualities to various conditions and modes. In typical conditions, the energy utilization would be ordinary, which is spoken to as "X". In low power battery depletion assault, the energy utilization will be more when contrasted with ordinary condition utilization, which is spoken to as "Y", where Y > X. Energy utilization if there should arise an occurrence of high force assault is spoken to as "Z" where Z >Y, which implies that energy utilization in the event of high power assault is more noteworthy when contrasted with energy utilization in low force assault.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Table 1. Different values for different conditions

Condition	Active	Idle	Sleep	Normal	Low intensity attack	High intensity attack
Value	2	1	0.5	X	Y	Z

The proposed mechanism in its training phase observe many important features such as

- The measure of time a node stays in dynamic, inactive or rest mode
- Energy utilization in dynamic, inactive and rest mode
- Neighbor nodes transmission example and energy utilization for neighbor(s) information sending.
- The preparing stage has a length of a few days (depending of the precision of the framework).

The proposed component takes as info the mode (dynamic, inactive and rest) just as the energy utilization in a particular interim of time. The caught loads are multiplied and handled in the shrouded layer. The two conceivable yields are "typical" or "unusual". Where irregular implies that energy depletion assault is going on against node(s). The working component of the proposed model is appeared in Figure 3.

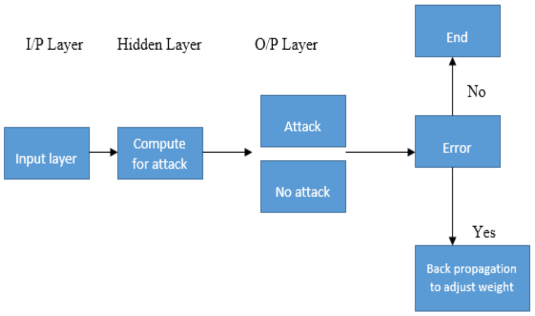

Figure 3. Working mechanism of the proposed model

We are utilizing basic databases as given in table 1 with the qualities in databases are taken after some time interim as parallel organization and are feed to include layer. For effortlessness purposes, we are utilizing character esteems, for example, the ones appeared in figure 4. So as to check our framework, we will consider two situations and see what the outcome in the two cases is. In the two situations we utilize a network of 20 nodes in a bunch of two jump neighbors. We expect that bunch development and group head determination has been performed by [34, 47].

- In the first situation, we expect a node in dynamic mode with ordinary energy utilization. In its preparation stage, ANN has taken in the typical energy utilization of dynamic mode sensor node with deference of fixed interim of time. Information layer advances loads of "2" (for dynamic mode) and "X" (for typical energy utilization got the hang of amid preparing stage) to concealed layer. Concealed layer processes the loads (2xX) and characterizes it as ordinary (no assault).
- In the second situation, we expect a node in dynamic mode and it is under an extreme energy fatigue assault with high energy utilization. Information layer advances loads of "2" (for dynamic mode) and "Z" (for high energy utilization picked up amid preparing stage) to concealed layer. Concealed layer registers the loads (2xZ) and grouped it as assault. This data is sent to different neurons too so that to advise the malignant exercises of specific node.

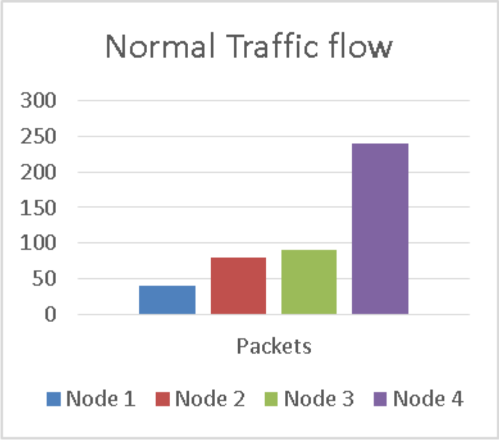

Figure 4. Normal traffic flow

In figure 4, the transmission example of node 1, node 2 and node 3 is roughly the equivalent. Anyway node 4 is sending and accepting (handing-off) more traffic. The reason is that node 4 is situated in the inside so it gets and transmits more information when contrasted with different nodes.

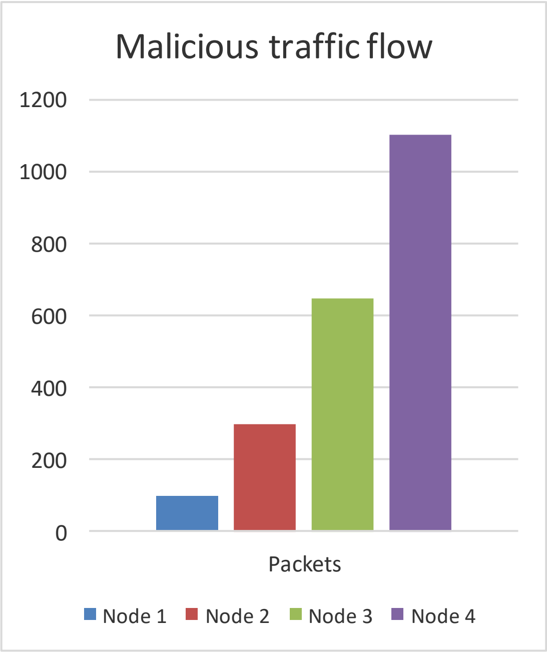

Figure 5. Malicious traffic flow

In figure 5, node 1 is vindictive and is flooding the network with colossal number of packets so that to debilitate energy assets of different nodes. In this situation, node 3 and node 4 are likewise incredibly influenced by the flooding of node 1, as node 3 and node 4 are under direct assault. Node 3 and node 4 are accepting packets from node 1 and sending to the objective node, as the two nodes are halfway nodes between sender (pernicious node 1) and goal (node 5). Be that as it may, node 2 is least influenced by this flooding, as node 2 is neither middle of the road nor under direct flooding assault. Network layer flooding assaults significantly increment energy utilization of sensor nodes as appeared in Figure 6.

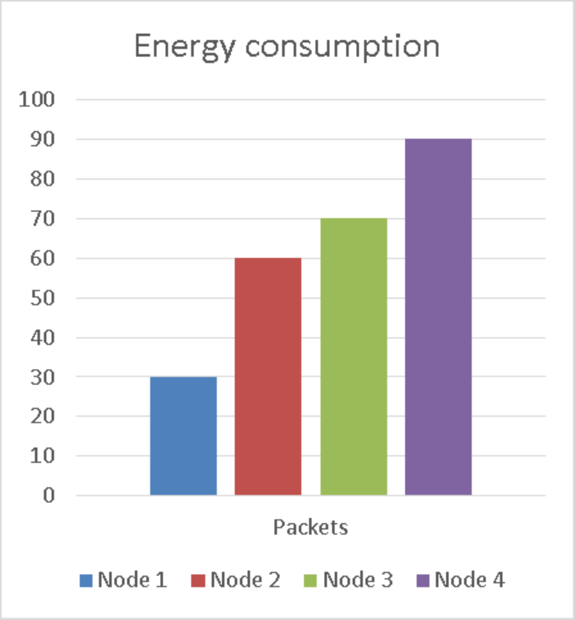

Figure 6. Energy consumption in malicious traffic flow

IV . CONCLUSION

Energy gathering is a system which is utilized to build the lifetime of sensor nodes. Be that as it may, there are assortments of energy fatigue assaults which are utilized to lessen the lifetime of sensor nodes. Within the sight of such assaults, energy gathering instruments can't make incredible distinction. In this paper, we introduced in detail a protected system to recognize energy depletion assaults. Our system is fitting in group based WSN and it is based on an artificial neural network. The proposed scheme is particularly prepared to recognize flooding assaults which are progressively extreme in nature and is proficient to deplete the energy of sensor nodes rapidly. Numerous tests are led to check the execution effectiveness of the proposed system. A location rate of 98% is observed if there should arise an occurrence of flooding assaults. The recognition rate of 95% is observed in the event of steering circle assaults. Notwithstanding, low location rate (just 55%) is observed if there should be an occurrence of information interface layer assault.

REFERENCES

1. I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks, December 2011.
2. N. Rodriguez, S. Rossetto, “Distributed systems with wireless sensor networks,” 2012.
3. Q. Mamun, “A qualitative comparison of different topologies for wireless sensor networks,” 2012.
4. A. Devasena, B. Sowmya, “Wireless sensor network in disaster management,” Indian journal of science and technology, July 2015.
5. A. K. Pathan, H. W. Lee, C. S. Hong, “Security in wireless sensor networks: Issues and challenges,” ICACT, 2006.
6. M. Momani, S. Challa, “Survey of trust models in different network domains,” 2010.
7. W. Stallings, “Cryptography and Network Security,” sixth edition, 2013.
8. V. U. Rani, K. S. Sundaram, “Review of Trust Models in Wireless Sensor Networks,” International scholarly and scientific research & innovation, 2014.
9. H. Rathore, H. Badarla, S. Jha, A. Gupta, “Novel approach for security in wireless sensor network using bio-inspirations,” IEEE, 2014.
10. G. Kulkarni1, R. Shelk , K. Gaikwad, V. Solanke , S. Gujar , P. Khatawkar, “Wireless sensor network security threats,” IET, July 2015.
11. E. P. k Gilbert, B. Kaliaperumal, and E. B. Rajsingh, “Research issues in wireless sensor network applications: A survey,” International journal of information and electronics engineering, September 2012.
12. H. A. N Jitender, S. Deogun and E. D. Manly, “Secure and energy aware routing against wormholes and sinkholes in wireless sensor network”, IEEE, 2006.
13. K.Vengatesan ,S.Selvarajan “Improved T-Cluster Based Scheme for Combination Gene Expression Data” International Conference on Radar, Communication and Computing(ICRCC) Conducted by SKP Engineering College, Tiruvannamalai on 21-22 December-2012.
14. K.Vengatesan,M.Kalaivanan Assistant Professor, Department of CSE Published a paper on, “Recommendation System Based on Statistical Analysis of Ranking From User” Information Communication and Embedded Systems (ICICES) 29 April 2013, pp. 479-484 .
15. R. W. Anwar, M. Bakhtiari, A. Zainal and K. Naseer Qureshi, “A survey of wireless sensor networks and routing techniques,” Research Journal of Applied Sciences, Engineering and Technology, 2015.
16. V. Reshmi, M. Sajitha, “A Survey on trust management in wireless sensor networks,” International journal of computer science & engineering technology, February 2014.
17. A. Doboli, “Discovery of malicious nodes in wireless sensor networks using neural predictors,” WSEAS transactions on computer research, February 2007.

AUTHORS PROFILE

Dr. Pardeep Kumar has done B.E(CSE), M.Tech(IT), Phd(CSE). His area of research is Network Security, Wireless sensor Networks.

Dr. Udayabhanu N P G Raju has done B.Tech(CSIT), M.Tech(Software Engg.), Phd(CSE). His area of research is Data Security, Quantum Computing.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)
© Copyright: All rights reserved.