IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

VPN ABSTRACTION SERVICE IN COMMUNICATION NETWORKS

REJINA P V
ASSISTANT PROFESSOR
COOPERATIVE ARTS AND SCIENCE COLLEGE,MADAI,PAYANGADI,KANNUR

SYMBOLS & NOTATIONS

RL	:	Risk Level
BRM	:	Breuer of Risk Management
RPA	:	Risk Protection Agency
ORC	:	Optimum Risk Commission
IARM	:	International Agency for Research on Risk Management
ROQ	:	Risk Operation Quality

ABSTRACT

In this research work, we present a routing algorithm for virtual private networks based in clusters, which performs periodic data collection environment. The environment monitor is divided into a uniform grid to locate clusters headers. The algorithm works in two distinct rounds of selection and training of headers of clusters, and other supply information to the base station using some function aggregation. The measurement of environmental variables is essential for monitoring and control environments and activities of diverse nature. In industrial applications is done, medical, agricultural, environmental preservation or creation of intelligent environments, among others. In many of the above applications, the sensing of the variables of interest must be made in remote or hostile environments that make it difficult wiring and routine care of the measuring devices. For these reasons, they have begun to use wireless smart virtual private networks (RISI) to obtain the necessary data.

The RISI are a particular type of virtual private networks consist of nodes in addition to collecting data from the environment, are able to process and work with your neighbors to transmit to the / base stations. These networks are self-organizing to adapt to changing topologies, and work under tight restrictions of energy, trying to maximize their lifetime.

A RISI performs two key activities to bring relevant information to the base node for the application. The first deals with the sensing and information processing, and the second of the spread of the same network. Both tasks consume energy, which has already mentioned is a resource that must be carefully preserved. It has been established that transmission consumes most of the available energy, so try to minimize the task of disseminating information by all possible local processing.

In this sense, techniques have been developed that allow data aggregation that information processing is performed in a distributed way network nodes.

CHAPTER 1 INTRODUCTION

This chapter presents a brief introduction of VPN. Recent advances in wireless communication, micro system and low-power technologies have enabled the VPN. Generally, VPN consist of many, low-cost, low-power and small Sensor Nodes (SNs) and the Base Station (BS). Once the SNs are deployed at a target area, they collect some information from the area and report it to the BS. The BS takes the role of gateway to the traditional networks, so we can use the collected information for specific applications. Rest of the part is sorted out as takes after.

Section 1.1 presents architecture of VPN, components of a SN and characteristics of VPN. Section 1.2 introduces some important applications of VPN and challenges in VPN are described in Section 1.3. Section 1.4 presents introduction to Outlier detection. Section 1.5 describes some of the characteristics of outlier detection techniques for VPN. Motivation of dissertation and the objective of developed scheme is discussed in Section 1.6.

1.1 VPN

VPN consist of a large number of limited capabilities (power and processing) Micro Electro Mechanical Systems (MEMS) capable of measuring and reporting physical variables related to their environment. A VPN consists of spatially distributed autonomous sensors to hand and glove monitor physical or environmental conditions, like temperature, sound, vibration, pressure, motion or pollutants.

Sensor networks square measure being deployed for a large sort of applications, as well as by military applications like field of honor police work and is currently utilized in several industrial and civilian application areas, surroundings and surroundings observation, attention applications, home automation, and control.

In police work applications, sensors square measure deployed in an exceedingly sure field to notice and report events like presence, movement, or intrusion within the monitored space. Knowledge collected by sensors square measure transmitted to a special node equipped with higher energy and process capabilities referred to as ―Processing Node‖ (PN) or ―sink‖. The PN collects, filters, and compiles knowledge sent by sensors so as to extract helpful data.

1.1.1 Sensor Network Architecture

We take into account the sensing element spec pictured in Figure one.1. within the design SNs square measure sorted into clusters controlled by one command node. Sensors square measure solely capable of radio-based short-haul communication and square measure accountable for searching the surroundings to find a target/event. each cluster encompasses a entranceway node that manages sensors within the cluster. Clusters will be shaped supported several criteria like communication vary, range and sort of sensors and geographical location. Sensors receive commands from and send readings to its entranceway node, that processes these readings.

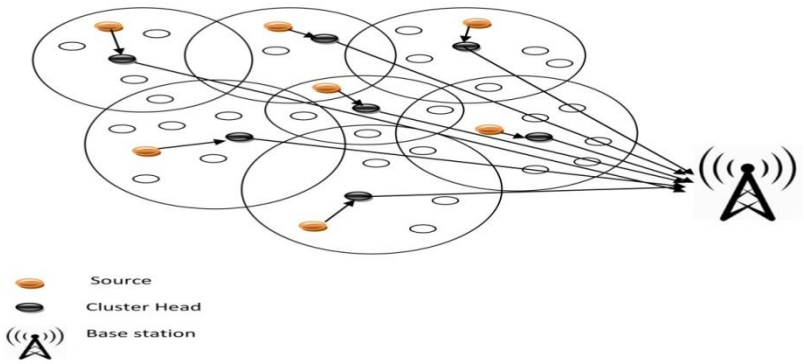


Figure 1.1: Sensor Network Architecture

Gateways will track events or targets exploitation readings from sensors in any clusters as deemed by the command node. However, sensors that belong to a specific cluster area unit solely accessible via the entryway of that cluster. Therefore, an entryway ought to be able to route device knowledge to alternative gateways. Entry way nodes interface the command node with the device network via long-term communication links.

The entryway node sends to the command node reports generated through fusion of device readings, e.g. tracks of detected targets. The command node presents these reports to the user and performs system-level fusion of the collected reports for overall scenario awareness.

1.1.2 Components of Sensor Node

A detector Node conjointly known as stuff may be a node in VPN that's capable of activity some process, gathering sensory info and communication with different connected nodes. Because of recent technological advances, the producing of little and low price sensors became technically and economically possible. The sensing physical science live close condition associated with the setting encompassing the detector and transforms them into an electrical signal. Process such an indication reveals some properties regarding objects set and/or events happening within the neighborhood of the detector. An oversized range of those disposable sensors will be networked in several applications that need unattended operations.

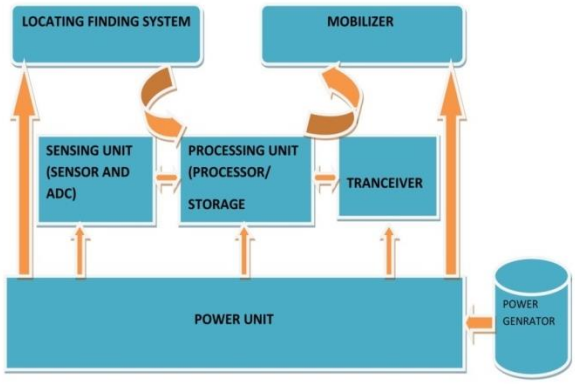


Figure 1.2: Components of SN

A VPN contains lots of or thousands of those SNs. the command node reports generated through fusion of device readings, e.g. tracks of detected targets .These sensors have the flexibility to speak either among one {another} or on to an external Base-Station (BS). A bigger range of sensors permits for sensing over larger nation-states with bigger accuracy. Figure 1.2 shows the schematic diagram of metallic element parts. Every individual node is comprised of 1 or additional sensing devices, a processor, a communication unit, and an influence offer. It shows

the communication design of a VPN. SNs square measure typically scattered in an exceedingly device field, that is a neighborhood section. Wherever the SNs are deployed. SNs coordinate among themselves to supply high-quality data concerning the physical surroundings. Every metallic element bases its selections on its mission, the knowledge it presently has, and its data of its computing, communication, and energy resources. Every of those scattered SNs have the potential to gather and route knowledge either to alternative sensors or back to an external baccalaureate. A baccalaureate could also be a fixed set node or a mobile node capable of connecting the device network to an existing communications infrastructure or to the net wherever a user will have access to the according knowledge.

1.1.3 Characteristics of VPN

Due to a lack of infrastructure, SNs need to cooperate with each other so as to maintain life and secure information. Each SN not only acts as a host, but also as a router for data forwarding. Each SN has limited power, memory storage, data processing capacity and radio transmission range. Generally, a VPN has the following characteristics:

Ad hoc Deployment

SNs are spread randomly and hence they do not fit into any regular topology. Once distributed, they usually do not require any human intervention. Hence, the setup and maintenance of the network ought to be entirely freelance and also the network ought to be self-reconfigurable.

Dynamic configuration

SNs could run out attributable to restricted power or new nodes could also be additional to the network. Hence, the network property changes with time, leading to dynamically ever-changing configuration.

Energy unnatural Operation

An important bottleneck within the operation of SNs is that the obtainable energy. Sensors usually rely on their battery for power, which in many cases cannot be recharged or replaced. Hence, the available energy at the nodes should be considered as a major constraint while designing protocols as well as computational complexity and storage. For instance, it is desirable to give the user an option to trade off network lifetime for fault tolerance or accuracy of results.

Unattended Operation

VPN are usually spread in a hostile environment, and operating in unattended mode. SNs ar unfolds haphazardly and therefore they are doing not match into any regular topology. Once distributed, they sometimes don't need any human intervention. Hence, the setup and maintenance of the network ought to be entirely freelance and also the network ought to be self-reconfigurable.

Infrastructure-less

VPN are primarily infrastructure-less. There's no central authority to watch SNs. Therefore, all routing and maintenance algorithms need to be distributed. Sometimes this property becomes main drawback in operation of SN. Due to these property SNs needs to be self-organizing and self-maintaining.

Shared Bandwidth

The radio channel in a VPN is broadcast in nature and is shared by all the nodes within its direct transmission range. So, a malicious node could easily obtain access to the data being transmitted in the network.

Large Scale of Deployment

A VPN is a large-scale network, in which thousands of sensors are arbitrarily spread to track surrounding environment or monitor a particular object.

1.2 Applications of VPN

VPN applications are often classified into 2 categories: observation and pursuit. Observation applications embody indoor/outdoor environmental observation, health and eudemonia observation, power observation, inventory location observation, manufacturing plant and method automation, and unstable and structural observation. Pursuit applications embody pursuit objects, animals, humans, and vehicles. Whereas there are a unit many various applications, below we tend to describe a couple of example applications that are deployed and tested within the real setting. Altogether of applications, it's necessary to take care of the integrity and therefore the

correct operation of the deployed network. Therefore, the safety in VPN becomes a vital and a difficult style task.

VPN area unit meant for observation AN setting. The most aim of a wireless device node is to gather information from a definite domain, method them and forward it to the sink, wherever the applying lies. However, by guaranteeing the direct communication between a device and therefore the sink could drain the nodes' power terribly quickly, as a result of higher energy demand in transferring messages. Therefore, it's typically needed that the nodes area unit collaborated to make sure communication of distant nodes with the sink. During this method, messages area unit propagated through intermediate nodes by establishing a route to the sink. Routing protocols for VPN area unit to blame of discovering and maintaining the routes within the network.

According to the participation variety of device nodes, routing protocols in VPN are often classified into 3 classes.

Direct Communication:

In the case of direct communication, any node will send info on to the bottom Station (BS). Applying this routing technique in a terribly very giant network could drain the energy of device nodes quickly. Its quantifiability is incredibly little. Example: SPIN.

Flat:

In this sort of protocols, if any node wishes to transmit information, it initial searches for a route to the SB then transmits the info. During this method, nodes round the SB could drain their energy quickly. Its quantifiability is average. Example: Rumor routing.

Clustering:

According to the agglomeration routing protocols, the entire space is split into numbers of clusters. Every cluster features a cluster head (CH) and this cluster head directly communicates with the SB. Nodes in a very cluster send their information to their corresponding CHs. Example: adolescent.

There is a unit some problems within the style of routing protocols for VPN as a result of many constraints within the network. VPN suffer from the restrictions of many network resources like,

energy, bandwidth, computation power and storage. The planning challenges in device networks involve the subsequent key aspects:

Limited energy capacity:

Since the device nodes area unit battery hopped-up is having restricted energy capability, energy could be a huge challenge for the network designers in hostile environments. For instance, in a very piece of ground, it's virtually not possible to access the sensors and recharge their batteries. Also, once the energy of a device reaches a definite threshold, it's going to become faulty and will not be able to perform properly, which may have a serious impact on the network performance. Thus, routing protocols designed for VPN ought to be as energy economical as attainable to increase the period of the sensors and thus prolong the network period whereas guaranteeing good overall performance.

Sensor locations:

Another challenge that's two-faced throughout the planning of routing protocols is to manage the locations of the sensors. Most of the protocols assume that the sensors either area unit equipped with GPS receivers or use some localization technique to find out concerning their positions.

Limited hardware resources:

The process and storage capacities of sensors also are restricted because the energy capability. Thus, they will solely perform restricted procedure practicality. These constraints create to several challenges in network protocol style for VPN, that should contemplate not solely the energy potency of device nodes, however additionally the process power and storage capacities.

Massive and random node deployment:

Sensor node readying in VPN is application dependent and affects the performance of the routing protocol. Device nodes are often scattered every which way in a very specific space or born massively over a distant or hostile region in most of the applications.

When the resultant distribution of nodes is un-uniform, best agglomeration helps in property and facultative energy economical network operation.

Network characteristics and dynamic environment:

A device network usually operates in a very dynamic and unreliable setting. The constellation, outlined by the sensors and communication links between them, changes oftentimes as a result of device addition, deletion, damages, node failures or energy depletion. Moreover, the device nodes area unit joined by a wireless medium, that is clattering, liable to errors and time varied. Therefore, routing protocols ought to contemplate constellation dynamics to take care of specific application needs in terms of coverage and property.

Data Aggregation:

Sensor nodes could generate important redundant information. So, similar packets from multiple sensors are often aggregate to scale back range of transmissions. Information aggregation techniques area unit accustomed accomplish energy potency and to optimize information transfer within the routing protocols.

Diverse application requirements:

VPN have a good vary of applications every having completely different needs. No network protocol will meet all the necessities of each application. Hence, routing protocols ought to guarantee information delivery and its accuracy to produce the sink with the specified information concerning the physical and condition on time.

Scalability:

Routing protocols ought to be capable of scaling with the network size. Also, sensors needn't essentially have equivalent capabilities in terms of energy, process and communication. So, communication links between sensors might not be centro symmetric (i.e. .a try of sensors might not be able to have communication in each direction). This could be taken care of within the style of routing protocols.

Clustering in VPN

The major advantage of VPN is the ability to deploy it in an ad-hoc manner [8], as organizing these nodes into groups pre-deployment is not feasible. For this reason, a lot of research has been conducted into ways of creating these organizational structures (or clusters). A clustering scheme divides the sensor nodes in a VPN into different virtual groups, according to some set of rules. In a cluster structure, sensor nodes may be assigned a different status or function, such as cluster head or cluster member[46].We can see in the Figure 1.2, the architecture of a generic VPN, and examine how clustering is an essential part of the organizational structure. Sensor Nodes: Sensor nodes are the building blocks of a VPN. They can play multiple roles in a VPN, such as simple sensing, data processing, data storage and routing. Clusters: Clusters are the organizational unit of VPN.

The dense nature of VPN requires them to be broken down into clusters to simplify tasks such as routing. Cluster heads: Cluster head is the organizational leader of a cluster. It organizes the activities in a cluster.

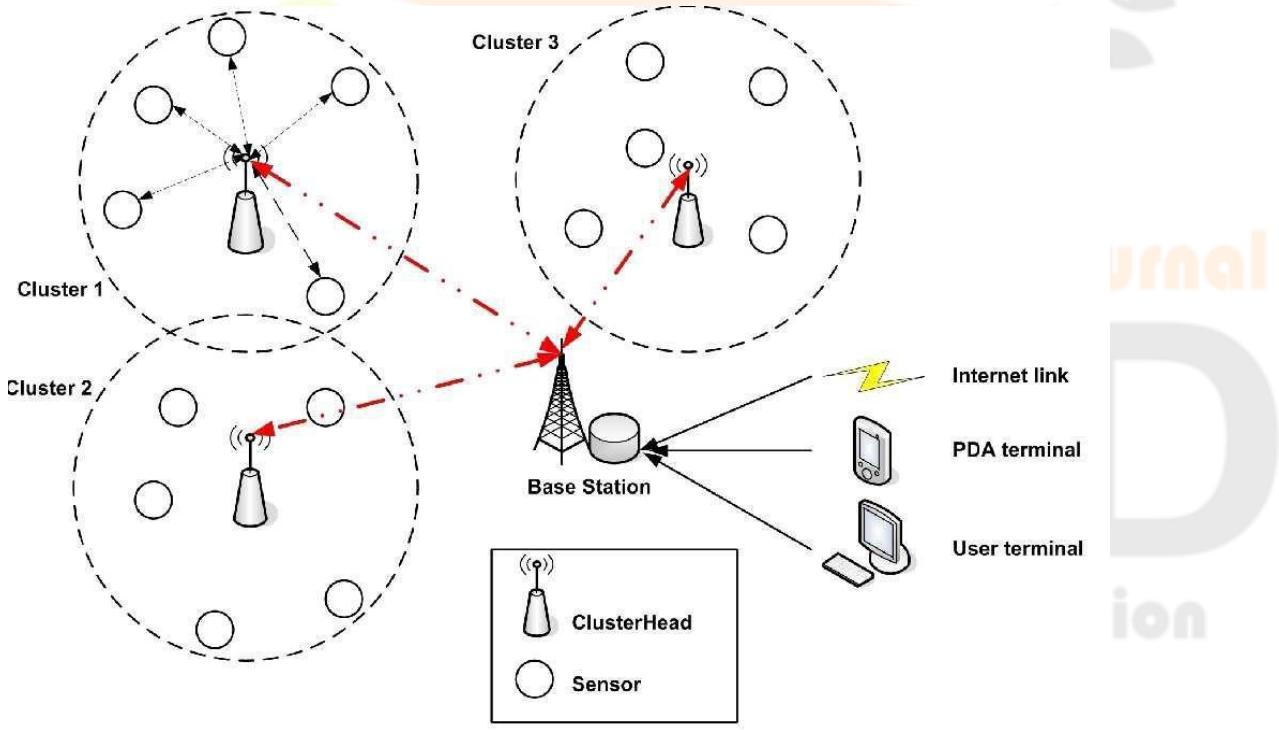


Figure 1.3: Clusters in VPN

The activities include data-aggregation, diffusion, organizing the communication schedule of the cluster, etc. Base Station: The base station is often located far from the network. It provides the communication link between the VPN and the end-user.

The data obtained from sensor network can be used for a wide-range of applications. A particular application can make use of the network data over the internet, using a PDA, or even a personal computer. In a queried sensor network, queries are generated by the end user.

1.6.1 Clustering Algorithms:

Many algorithms have been proposed for routing in VPN. Clustering algorithms have gained popularity in this field. Clustering algorithms can be classified as:

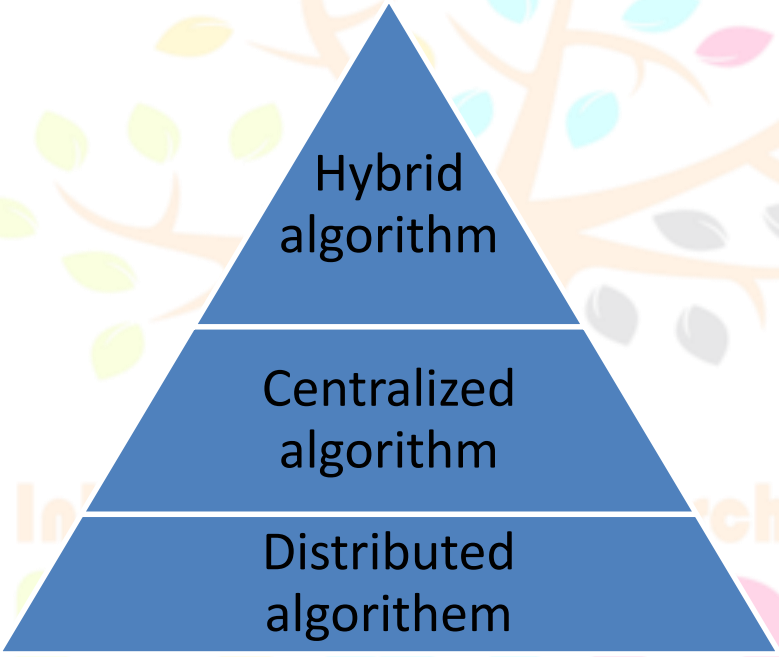


Fig: 1.4 classification of clustering algorithm

In distributed clustering techniques, any node can choose itself as a CH or join an already formed cluster on its own initiative, independent of other nodes. Distributed clustering techniques are further classified into four sub types based on the cluster formation criteria and parameters used for CH election as identity based, neighborhood information based, probabilistic and iterative.

In centralized strategies [47], the baccalaureate needs international info of the network to regulate the network. CHs area unit electoral by the bottom station. Hybrid schemes area unit composed of centralized and distributed approaches.

Programming wireless virtual private networks (VPN) is an error-prone process. Each virtual private network has a variety of components that have to be programmed with different methods and / or programming languages. Web 2.0 applications are facing similar problems. Google Web Toolkit (GWT) is a tool for Web 2.0 applications, which allows to develop the entire application in just a programming language, without knowledge of the different techniques. This research work intends to use the GWT concepts to try a possible adaptation / modification, so that the programming of VPN in a new way can be realized; Web 2.0 way.

VPN are the result of multiple technological advances in electronics, nanotechnology, wireless communications, computing power, network development and robotics. Compose distributed systems devices usually composed of integrated, including at least CPU, radio, and sensors / actuators number. The wireless virtual private networks (VPN) heterogeneous networks are formed by sensors, gateways and backend resources very limited physical. The sensors can measure parameters such as temperature, movement, lighting, humidity, etc..; the gateways establish the link with networks traditional and familiar. The back ends are responsible for the processing and display unit the captured data. Development VPN applications is a complex task, I must take the form of distributed applications and integrated, there are extra complications as the heterogeneity and scale environmental influences.

Although several studies showed VPN middleware, has not been achieved with this industry acceptance due mainly to the different methodologies programming. The teams consist of VPN lowest consumption, costs and form factors. the reality is quite different environments applications are supported with equipment more powerful and fed by redundant power networks. The work aims to define a way that developers can use technologies existing compatible standard to describe processes and services offered by VPN, without extra coding. The advantages of the method are Two: immediate adaptation of a VPN company, and integration of services VPN applications for higher-level simple modifications. The reality is that the main problems encountered in programming VPN relate the different based programming, as well with heterogeneity in both hardware and operating systems [1]. While businesses and offices in the applications are supported with high-quality equipment and computing power are powered by redundant power networks; VPN are optimized for scenarios minimum energy consumption,

lower costs and reduced form factors. in environments corporate or government is important adapt business processes to underlying software infrastructure in order to able to react quickly to potential changes and demands markets.

Since the early 90s, has sought to achieve this goal with modeling, analysis and adaptation processes business. So architectures have appeared service-oriented, which are based on Internet (SOA (2)). In parallel, the VPN have achieved such a degree of development that is considered as an integral part of the Internet the future, achieving extend the domain of this network to the real world. The two trends, together form the basis of a new type of applications where devices interact processes in an impossible way imagine a few years ago. This was true for single virtual private nodes up to application servers' scale, with this, and if the trend is not declined, the captured by the VPN data would influence the information flow of current processes real time, and could even trigger new processes. To achieve this level of interaction, VPN should relate unfailingly existing SOA with current technologies, such as XML (3), Web Services (4), and Execution Language Business Process (BPEL (5)), to name only a few. However, due to the high demand for resources of these applications are difficult applicable in restricted environments of VPN.

Some common features of VPN applications are defined by the own taxonomy of these networks. Not a good idea to add support for each of the platforms in the tools development. This is rationalized by the addition of an integration layer between the hardware and application, known as middleware. The middleware has been the subject of research Distributed systems for many years.

Create VPN middleware for a challenge, considering the restrictions set by this technology, methods well known as CORBA or Enterprise Java Beans should be discarded by excessive requirements computing power and memory. Furthermore, by the instability of communications in the VPN environment, methods traditional client-server is not recommended [6], [7], [8].

CHAPTER 2

REVIEW OF RELATED LITERATURE

In the literature, clustering attributes in VPN, generally, can be roughly classified into cluster characteristics, cluster-head characteristics, clustering process and entire proceeding of the algorithm. In this section, we have a tendency to discuss loads of careful cluster attributes for VPN, and propose a additional comprehensive and fine-grained taxonomy compared thereto of previous work. The classes enclosed within the taxonomy area unit on an individual basis analyzed within the subsections that follow.

2.1 Classification of Clustering Attributes in VPN

The Attributes for clustering are classified according to:

Cluster Characteristics

Cluster-Head Characteristics

Clustering Process

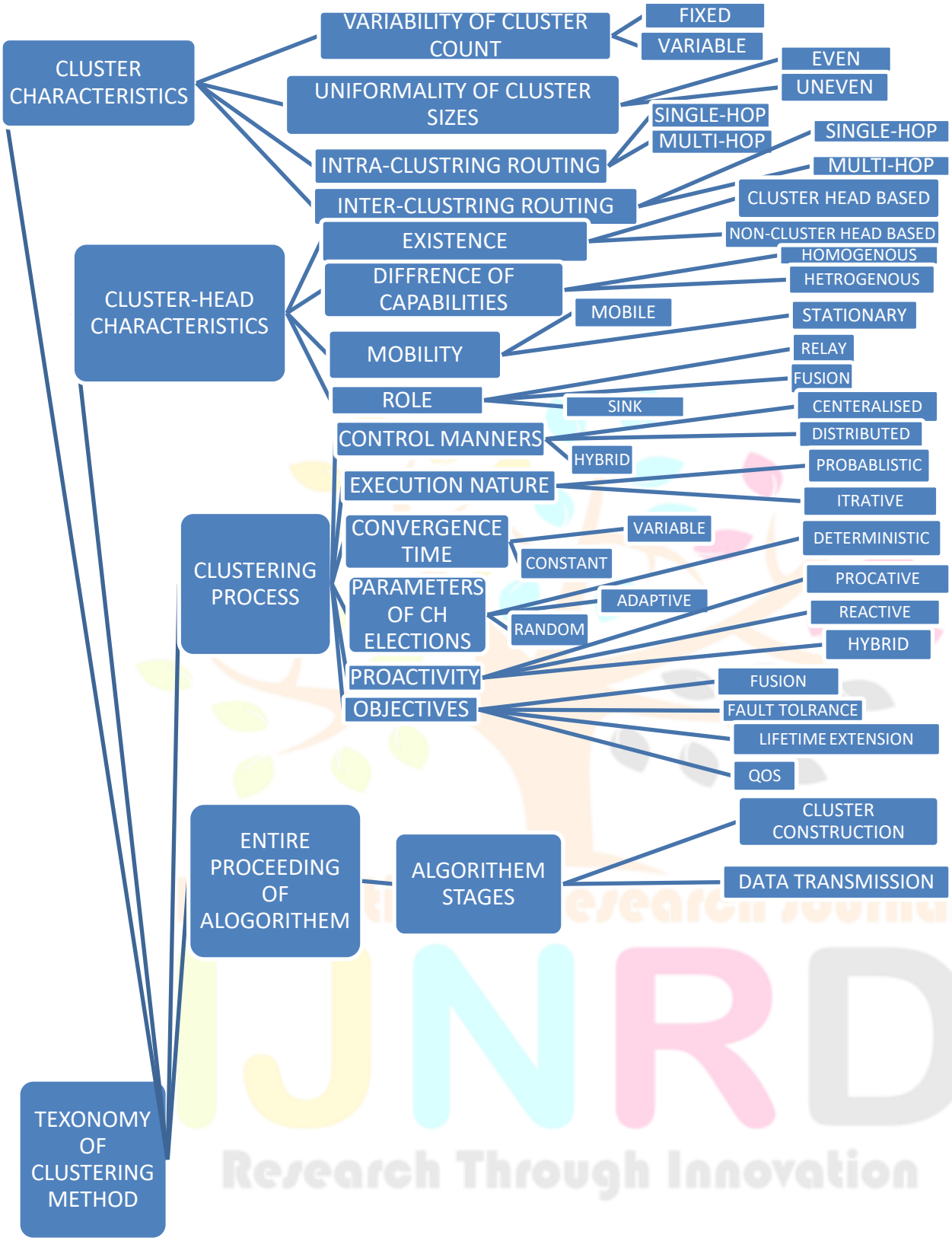
Entire Proceeding of Algorithm

Taxonomy of Clustering Methods in VPN

In this subsection, we integrate the set of attributes that can be use to categorize and differentiate clustering methods for VPN. Based on the discussion above, a relatively comprehensive and fine-grained taxonomy of clustering methods in VPN is proposed, which is summarized in Figure 2.1. In this section, we present a more comprehensive and critical survey of prominent clustering routing protocols for VPN compared with previous work. We analyze sixteen classical VPN agglomeration routing algorithms intimately supported the classification of various algorithm-stages.

LEACH (Low Energy adaptation agglomeration Hierarchy) may be a self organizing, adaptation clustering-based protocol that uses irregular rotation of cluster-heads to equally distribute the energy load among the device nodes within the network. LEACH supported 2 basic assumptions:

1. Base Station is fastened and placed distant from the sensors.
2. All nodes within the network area unit homogenized and energy strained.



The idea behind LEACH is to form clusters of the sensor nodes depending on the received signal strength and use local cluster heads as routers to route data to the base station and the corresponding clusters.

Ajay Jangra et al. [1] present a novel security S-LEACH mechanism which is the extension of LEACH routing protocol used for detecting the Sybil attack. The mechanism is configured to initiate the Sybil attack whose detection is relayed on RSSI (an indicator of signal strength) when the number of cluster heads in VPN is above the threshold. The security mechanism is canvassed by the safety of the stage and energy consumption through a series of experiments. Accordingly, the simulation results show that the system is an efficacious and robust for guarding the attack Sybil.

Baiping Li et al. [2] proposes the central management algorithmic rule to create the clusters. And simulation result shows that this algorithmic rule might manufacture higher clusters by dispersing the cluster-head nodes throughout the network. Then a sequence routing between cluster-heads is established to scale back the quantity of nodes that communicate with the bottom station. More improvement in energy value for information gathering is achieved if just one cluster-head transmits to base station and if every cluster-head transmits solely to native neighbor cluster-heads within the information fusion section. This can be the idea for LEACH-CC (LEACH-Centralized with Chain).

Bijan Kumar Debroy et al. [3] during this paper propose a brand new methodology for cluster head choice supported device nodes energy per cost. The experimental study shows that the planned methodology, by adopting few choice criteria on selecting cluster head, will increase the system life and maximize electronic communication as compared to existing dominant approaches.

David Gugelmann et al. [4] have presented a novel data dissemination protocol with a focus on reliability and energy-efficiency. Scheduling of image dissemination only during reserved time slots eliminates interference with the regular data gathering protocol and increases the observability during the network reprogramming phase.

Deng Zhejiang et al. [5] performed; due to the limitation of power and memory size for VPN, the routing protocol for VPNs must maintain small routing information and reduce the power consumption as much as possible. LEACH protocol and PEGASIS protocol are analyzed firstly

in this paper. Use for reference of the ideas used in both of the two protocols of reducing power dissipation, a three-layered routing protocol for VPN based on LEACH(TL-LEACH) is given. Then, this improved LEACH protocol is simulated and the simulation results show that TL-LEACH protocol is with greatly improved VPN lifetime than LEACH protocol.

Fan Xiangning et al. [6] studies LEACH protocol, and puts forward energy-LEACH and multihop-LEACH protocols. Energy–LEACH Protocol improves the selection methodology of the cluster head, makes some nodes that have additional residual energy as cluster heads within the next spherical. Multihop-LEACH Protocol improves communication mode kind single hop to multihop between cluster head and sink. Simulation results show that Energy-LEACH and Multihop-LEACH Protocols have higher performance than LEACH Protocols.

Fuzhe Zhao, You Xu, Ru Li, dynasty Zhang et al. [7] propose a replacement methodology of selecting cluster-heads with decreases inessential consumption of energy spent on computing every node throughout each spherical. as a result of the normal selecting formula neglecting to the modification of nodes energy can create the nodes acting as cluster-heads too persistently die early due to consume an excessive amount of energy. So as to create the energy distribute additional even within the network, the thought of the dynamic modification of device nodes energy are introduced throughout the choice of CHs.

Fuzhe Zhao et al. [8] proposes a replacement methodology of selecting cluster-heads that decreases inessential consumption of energy spent on computing of every node throughout each spherical. As a result of the normal choice formula neglecting to the modification of nodes' energy can create the nodes acting as cluster-heads (CHs) too persistently die early due to consume additional energy. For creating the energy distribute additional even within the network, the thought of the dynamic modification of device nodes' energy are introduced throughout the method of choosing of CHs. Simulation method show that our improved protocol performs higher than the initial LEACH.

Haosong Gou et al. [9] this paper proposes an improved LEACH (LEACH-C) algorithm called partition-based LEACH (pLEACH), which firstly partitions the network into optimal number of sectors, and then selects the node with the highest energy as the head for each sector, using the centralized calculations.

Heewook Shin et al. [10] within the paper "Energy-Efficient clump with just one occasion Setup for VPN" planned a replacement energy economical clump theme. He declared that in LEACH, however, further energy and time square measure consumed to reform clusters at the setup section of each spherical. This aspect impact is unhealthy because the range of clusters will increase. This paper gift a unique energy-efficient clump theme to get rid of cluster recreating method needed at each spherical once the primary spherical, that is named COTS (Clustering with just one occasion Setup). The planned COTS permit that the role of cluster head is revolved among members in a very cluster while not cluster reforming method. This fashion considerably saves the energy as a result of the cluster reforming method isn't required, leading to hyperbolic network period.

Hemant Sethi et al. [11] have planned AN Energy economical Interest based mostly reliable knowledge Aggregation (EIRDA) Protocol for VPN. Here every cluster assumes the distribution of detector nodes as standardized distribution victimization EIRDA that could be a static clump theme. Author bestowed beta-distribution perform on give dependability with the assistance of purposeful name construct. The impact of all the measures taken at every section of protocol implementation is clearly visible on the energy spent within the setup section of the protocol.

Hu Jumping et al. [12] performed a VPN consists of lots of or thousands of tiny energy-limited sensors that square measure densely deployed in a very massive realm. It's been incontestable that Low-Energy adaptation clump Hierarchy is AN energy-efficient routing algorithmic rule for VPN. During this paper we have a tendency to gift a Time-based Cluster-Head choice algorithmic rule for LEACH. We have a tendency to decision this new protocol TB-LEACH. This paper states the principle of TB-LEACH and provides the most flow diagram and pseudo codes realizing TB-LEACH. This paper provides a comparison between our protocol and LEACH protocol.

Jia Xu et al. [13] propose a revised cluster routing algorithmic rule named E-LEACH to boost the ranked routing protocol LEACH. E-LEACH algorithmic rule shows that, the first approach of the choice of the cluster heads is random and therefore the spherical time for the choice is mounted. Within the E-LEACH algorithmic rule, here contemplate the remnant power of the detector nodes so as to balance network hundreds and changes the spherical time depends on the optimum cluster size. Outcome of simulation results show that our planned protocol will increase network life a minimum of by four-hundredth compared with the LEACH algorithmic rule.

Jun YUE, Weiming ZHANG, Weidong XIAO, Daquan TANG, Jiuyang TANG et al. [14] presents a unique unequal cluster-based knowledge aggregation protocol is planned. It divides the network into some grids with unequal sizes, and implements cluster head rotation in every grid severally. It's ready to balance energy dissipation by setting correct sizes of grids to regulate the amount of nodes that participate in cluster head rotation in numerous grids. Moreover, it adopts some ways to boost usage potency of energy. The results of simulations show that it are able to do higher performance in aspects of network life, energy potency and balanced extent of energy dissipation.

Li-Quing Guo et al. [15] performed a work; LEACH could be a in style ranked routing protocol that with efficiency maintains the energy storage of nodes in Wireless detector Network. The nodes victimization LEACH square measure divided into clusters. The irregular rotation of cluster head in every cluster will save the energy consumption of nodes. However, the random election of cluster heads while not considering nodes residual energy might cut back and oscillate the period of network. during this paper, we've got planned the adaptation Cluster Head Election and Two-Hop LEACH protocol (ACHTHLEACH) to prolong the period of network. It improves LEACH by victimization AN adaptation algorithmic rule of cluster head election and permitting multi-hop transmission among cluster heads and base station (BS).

M. Bani Yassein et al. [16] presents a replacement version of LEACH protocol known as VLEACH that aims to scale back energy consumption inside the wireless network. during this redo of LEACH protocol, the cluster contains; CH (responsible just for causing knowledge that's received from the cluster members to the BS), vice-CH (the node which will become a CH of the

cluster just in case of CH dies), cluster nodes (gathering knowledge from atmosphere and send it to the CH).In the original leach, CH can die before the opposite nodes within the cluster attributable to its operation of receiving, causing and overhearing. At the time once the CH die, the cluster can become insignificant as a result of the info gathered by cluster nodes can ne'er reach the bottom station. In V-LEACH protocol, besides having a CH within the cluster, a vice-CH is gift that takes the duty of the CH once the CH dies as a result of the explanations we have a tendency to mentioned on top of.

Ma and Y. Yang et al. [17] proposes the Adaptive Cluster Head Election and Two-hop LEACH protocol (ACHTHLEACH) to prolong the life time of network. It improves LEACH with the use of an adaptive algorithm of cluster head election and allowing multi-top transmission among cluster heads and Base Station (BS). They have taken in consideration the distance of nodes as near nodes or far nodes according to the distances to the BS. The near nodes relates to one cluster while the far nodes are divided into different clusters by the Greedy K-means algorithm. The cluster head is turn around and the node with the maximal residual energy in each cluster is elected. During the data transmission phase, the far cluster heads may select the cluster head in the near area as the next hop or communicate directly to the BS. In this paper authors in simulation results have shown that ACHTHLEACH outperforms several existing protocols in terms of network's lifeperiod. Specially, ACHTH-LEACH can achieve more than 2 times longer lifespan than LEACH and build a more stable routing environment.

Mingming Lu et al. [18] have proposed the data gathering problem in VPNs from the maximization of the expected network utility point of view. The scarcity of resource and the unstable nature of wireless channels are considered here. Problem of data gathering is designed as an optimization problem and the NP-hard problem is proved here. For both broadcast tree and reverse multicast tree problems several heuristics were proposed.

Mu Tong et al. [19] performed a piece, supported the analysis on the defect in LEACH together with the fluctuation of the quantity of cluster heads and therefore the cognitive content of the node’s residual energy, this paper presents a completely unique protocol known as LEACH-B (LEACH- Balanced). At every spherical, once initial choice of cluster head consistent with

LEACH protocol, a second choice is introduced to change the quantity of luster head in thought of nodes residual energy. As a result the quantity of cluster head is constant and close to optimum per spherical.

Muhamnmad Omer Farooq et al. [20] presents a multi-hop routing with low energy adaptational agglomeration hierarchy protocol.MR-LEACH follows the basic principle of multi-hop routing from cluster-heads to a Base station to conserve energy, in contrast to the leach protocol. In MR-leach they partition the network into totally different layers of clusters. Wherever Cluster heads in every layer collaborates with the adjacent layers to transmit sensor's information to the bottom station. Normal nodes be a part of cluster heads supported the received signal strength indicator (RSSI). The transmission of nodes is controlled by a base station (BS) that defines the time division multiple accesses (TDMA) Schedule for every cluster-head. BS chooses the higher layers cluster Heads to act as super cluster heads for lower layer cluster heads. By conniving performance analysis it's shown that MR-LEACH achieves vital improvement within the leach protocol and provides energy economical routing for VPN. In LEACH protocol we have a tendency to don't think about the residual energy of nodes which can cut back and oscillate the lifetime of network.

Muhammad Omer Farooq et al. [21] performed a piece. During this paper, we have a tendency to gift a Multi-hop Routing with Low Energy adaptational agglomeration Hierarchy (MR-LEACH) protocol. So as to prolong the time period of Wireless sensing element Network, MR-LEACH partitions the network into totally different layers of clusters. Cluster heads in every layer collaborates with the adjacent layers to transmit sensors information to the bottom station. normal sensing element nodes be a part of cluster heads supported the Received Signal Strength Indicator (RSSI).

Nandini. S. Patil, Prof. P. R. Patil et al. [22] conferred an information aggregation framework on VPNs is conferred. The framework works as a middleware for aggregating information measured by variety of nodes inside a network. They compare the performance of TAG(Tiny Aggregation) in terms of energy potency compared with associated while not information aggregation in VPNs and to assess the quality of the protocol in an surroundings wherever resources ar restricted.

Ren P. Liu et al. [23] have proposed an Efficient Reliable Data Collection (ERDC) algorithm. Maximum number of retransmissions is under control in order to achieve energy savings. Concept of Dynamic programming is used to find the optimal solution. ERDC implementation is provided which uses next hop link quality and number of hops for determining number of retransmissions.

Volker Turau et al. [24] have presented the design and preliminary evaluation of a reliable data gathering service of periodic data in the face of poor link quality and frequent disconnects. The data is stored by persistent storage provided by the nodes using services based on a packet-level, and hop-by-hop routing protocol. This scheme also provides an upper limit for sampling rate that is handled reliably.

Wendi B. Heinzelman Anantha Chandrakasan, and Hari Balakrishnan et al. [25] presents a coffee Energy accommodative agglomeration Hierarchy (LEACH) that may be a clustering-based protocol. LEACH uses randomised rotation of the cluster heads to equally distribute the energy load among the device nodes in an exceedingly network. The cluster heads broadcast TDMA schedules providing the order of transmission for members within the cluster once the clusters ar created. every of the device node has its own interval. It sends information to the cluster head inside its exclusive interval. The cluster head are going to be willy-nilly nonappointive within the next spherical when the last node within the schedule has transmitted its information. It spend localized coordination to enhance the measurability and balance the energy usage of the network among all the nodes.

Wendi Rabiner Heinzelman et al. [26] LEACH a agglomeration based mostly routing protocol that minimizes international energy usage by distributing the load to all or any the nodes at totally different points in time. LEACH outperforms static agglomeration algorithms by requiring nodes to volunteer to be high-energy cluster-heads and adapting the corresponding clusters supported the nodes that like better to be cluster-heads at a given time.

Wei Bo Hu Han et al. [27] performed a work; Conventional LEACH includes distributed cluster formation, local processing to reduce global communication, and randomized rotation of the cluster-heads. The new protocol uses multi-hop routing instead of 2-hop routing in LEACH, and related algorithm is proposed. Simulation results show that improved protocol is more energy-efficient that conventional LEACH.

Wei Wang et al. [28] performed to prolong the VPN lifetime, a refined protocol named LEACH-H is proposed in this paper. In the first round of Leach-H, the base station selects a cluster head set through adopting Simulated Annealing Algorithm in the followed rounds; the cluster heads will select new cluster heads in their own cluster. This will not only solve the problem that the cluster heads are unevenly distributed in LEACH, but also maintain the characteristics of distribution. The energy consumption of the network is cut down and the live time of VPN is extended in Leach-H.

Wu Xinhua et al. [29] performed performance evaluation of LEACH and LEACH-C protocols based on NS2 is depicted, which helps to reveal the regularity how performances of these two routing protocols change with the sink locations. For more accurate description of this regularity, two novel concepts are proposed.

Yuling Li Luwei Ding et al. [30] finds anew improve method which is called LEACH-N base on LEACH. According to this new protocol, the problem that how to choose nodes as the cluster head node depend on the residual energy of nodes in the cluster. This strategy guarantees the rationality during selecting head nodes. Moreover, the network robustness is enhanced and the life cycle for the network can be enhanced.

CHAPTER 3
PROBLEM FORMULATION

3.1 Problem Definition

A VPN is associate autonomous system of detector nodes. It's a Base Station and detector nodes. Detector nodes collect knowledge from their surroundings and send it to the bottom Station. Heterogeneous detector network contains high energy detector nodes moreover as low energy

nodes. A single-tier network will cause the entranceway to overload with the rise in sensors density.

Such overload would possibly cause latency in communication and inadequate chase of events. Additionally, the single-tier design isn't ascendible for a bigger set of sensors covering a wider space of interest as a result of the sensors area unit usually powerless of long-haul communication. Gradable cluster is especially helpful for applications that need quantifiability to a whole lot or thousands of nodes. Quantifiability during this context implies the requirement for load leveling and ancient resource utilization.

All nodes in a very network may be organized in gradable structures referred to as clusters. Every cluster consists of a cluster head and several other member nodes. The member nodes collect knowledge and send it to their cluster heads. The cluster head aggregates and transmits the info to the bottom Station. The energy consumption of cluster heads is beyond that for member nodes.

3.2 Need and significance of proposed research work

The main motive of research is to design a clustering protocol which can distribute energy in an efficient manner. A protocol which can utilizes heterogeneity in a sensor network to extend its:

Lifetime and

Throughput by electing better cluster heads in a proficient manner.

The aim of research is to analyze performance of clustering algorithm with fuzzy logics.

3.3 Objectives

(1) Design a fuzzy based clustering system based on energy and distance from base station.

(2) To enhance the stability period of sensor network by electing sensor nodes with higher residual energy as cluster heads.

(3) To make an energy efficient clustering technique for VPN networks.

The hardware is important in the VPN, but technology can be fully exploited only if the platforms software are available to developers. Very few applications VPN in the real world are high level (9), (10). In most cases the development of applications is close to operating system, so you must

deal with situations involving low level, such as distributed protocols. These capabilities are rare in the current developers. A typical virtual private network consists usually by hundreds and in some cases thousands of nodes. In real situations is very difficult to establish a wired backbone, the that is used for all programming and each of the nodes, turning this into a task of high difficulty. While the focus of this work allows integration of VPN applications to IT those typical domain, the Developers must be experts in Programming VPN to implement the Services Web in restrictive environments in terms resources. The development of applications for VPN is comparable with the similar situation observed in the programming of Web 2.0 applications. Google [11] reports: "Currently, the creation web applications is a heavy process and error prone. developers can spend 90% of their time studying the peculiarities of browsers. Alternatively, the creation, reuse and Maintaining a large number of AJAX components and Java code bases Script can be complex and delicate tasks. "

To facilitate this, Google offers called "Google Web Toolkit (GWT)" helping programmers in implementation of Web applications. with GWT, developers can use the Java programming language to run both the server and browser in one application. On the server side, you can take advantage of all the functionality provided by Java, including numerous libraries, frameworks and tools. On the side of browser, there are some restrictions, the main one being that only a subset of the API Java can be used. The server and the browser does not communicate through function calls, but by sending instances of the objects together. These objects should be serialized according Java specification [12]. GWT, after compile the Java code Java Script, the executable is capable of operating in all major browsers (IE, Firefox, Opera, etc.). This is the reason for the limited set APIs available on the client side, since browsers that are offered only a limited set of possibilities. the supported classes and methods are in the GWT JRE Emulation Reference [13].

We shall study how to mitigate or further exploit interference [7] by network coding approaches. The beauty of this approach is in programmers benefit from Java tools, such as IDEs, scrubbers, writing code, etc..; achieving an executable in a single language. the resulting program is usually still more optimized than the original code. The lines of research converge studies of existing facilities, and bases to relate concepts and methods field goals of VPN. Primarily in the context where they have developed successful tools programming the web 2.0 way. This approach

is intended to analyze and assess the potential of technological adaptation: platforms, compilers, and tools API production Web services.

Wireless communications is an emerging field, which has seen enormous growth in the last several years. The objective of this work is to provide a set of development tools VPN applications, similar to the GWT provides to Web applications. It intends to implement the componenente generate the VPN (WSA) application and application running on the Internet in Java (IAP) currently on the way to server and Web browser. It aims to advance the management of following technologies and concepts: study Platform iSense sensors [14], GWT compiler, Java API and Web Service concept annotation, microfibre and Fabric [15] and LTP [16] providing Web services VPN.

It is considered a set of Java interfaces that abstract the functionality of a virtual private node. this API functionality shall provide: a) Interface radio to send, receive, record callbacks, etc.. b) routing the API c) Timers d) Serial interface e) Debugging f) Sensors. Determine if GWT compiler is sufficiently generic so that it can be modified so to use the new definition of Java interfaces sensors and generate the target language source code. One of the lessons learned during the will run the project, is that perhaps the approach adopted by GWT is best for our common goal, but GWT itself same, due to its extreme complexity. It considers analyze various modules such as Eclipse JDT (17) for converting Java source code into a syntax tree Abstract (AST) and thus to build the code required to operate with VPN. Also discussed reformulating Fabric so that they converge on several different projects independent of each other, each with a defined purpose. The working group is integrated with a researcher formed by three researchers training and administrative.

Reconfiguring, reprogramming and deployment of new computational tasks in wireless virtual private networks is a problem not satisfactorily resolved today. This research work proposes the performance evaluation enhanced with intelligent mobile agents as autonomous mechanism reprogramming wireless virtual private networks. The method used for performance evaluation is based on the measurement of energy consumption during the migration process of mobile agents between smart virtual private nodes and calculating the convergence time of the network,

defined as the time it takes for the network move from one state to another; in experiments refers to the delay in the change of the sampling time for the entire network. The most efficient, which was tested and evaluated in a wireless network consisting of 40 nodes that detect ammonia leaks in real-time solution determined that the key point is to reduce energy consumption product confirmations and unnecessary retransmissions of data and procedures, from the virtual private nodes to the base station. This fact, besides the decrease in energy consumption is a significant savings in the convergence time of the network.

A wireless virtual private network (RIS) is a system consisting of tens or hundreds of small stations called virtual private nodes. nodes are composed in turn by a specialized group of sensors and transducers have a communication infrastructure required for the chemical, pollution levels, vital body functions, gas concentrations between other. nodes Sensors have very limited computing capabilities by themselves, but when they work as a team, its processing capacity and coverage area become optimal.

The nodes of a RIS are autonomous, and be connected, form a distributed system computer working cooperatively to measuring physical variables and changes in conditions environmental. Each node is equipped with a radio, a small microcontroller, a power source which is usually a battery. The RIS are subject to more restrictions stringent than other similar electronic devices such as mobile phones or computers laptops. The entire network is frequently under management of a controller element named base station (BS), whose main function is to act as a gateway to other networks, data storage and forming network as such. It is important to note all data packets originating from nodes are sent to the BS. In other words, a RIS devices typically have full functionality (DFC), which are base stations or gateways and devices reduced functionality (DFR) data and taking send them to the DFC. The DFC have energy available all the time, more computing power and storage possibilities. Furthermore, the DFR should be battery operated and must sleep great periods, in order to optimize energy usage. The RIS can be classified into five types, depending on the working conditions, the difficulty of implementation and the specific application and must: RIS on land, underground RIS, RIS underwater RIS RIS multimedia and mobile.

There are several limitations in a RIS, related to energy consumption, the development applications faster and reprogramming new computational tasks. The following describes each one.

The first and main limitation of a RIS is the low availability of energy in the nodes. Your DFR component works usually with two AA or similar to those used by mobile phones batteries can ensure maximum 720 mA, which, in the best cases have months duration. It is impossible for this type networks consider permanent changes in batteries and unfortunately, in the near future, optimization is displayed in them, so that nodes can operate for long. to the regarding various solutions have been proposed, which ranging from the use of hardware that works with a minimum current, up protocols that optimize the process idle virtual private nodes.

The second major limitation of the RIS is in the development of applications which can then be reprogrammed; currently, once the RIS has been set and displayed, it becomes practically impossible to use it for other tasks or change their initial configuration parameters. Have proposed some solutions to this problem reprogramming and changes in new tasks for RIS, however, is not a standard method has allowing reprogramming, reconfiguration and allocation of new computational tasks. The third and last limitation is related with rapid and agile application development the RIS. It has been found in this part of the main obstacle to the RIS technology is adopted to great scale worldwide. Importantly, only there are few significant developments and even "built to order" for deployment fast application.

The task of reprogramming and reconfiguration of a RIS is defined as the ability to deploy new computer applications dynamically, without the need for human intervention in the network (that is, to reprogram manually each of the nodes and using a computer connected to it). In general, developers may be interested in making improvements to the previously developed applications, or want to build a new application or perhaps change some of the parameters of the nodes (eg., The sampling time downtime or node). Also, it might be of interest completely convert the application or troubleshoot software errors. By other hand, the network may need to perform a new task or when sampling network administrators want to deploy updates software. In

conclusion, reprogramming and reconfiguration are necessary for the RIS to adapt to changes in the environment.

In this way, the mobile agent interact with external devices, process and collect information, and then returns to its origin with the data. Mobile agents have gained acceptance due to its feature mobility, since it has proven to be much more efficient than one agent is transferred to a remote location, do a search, filter, process the information and return the results to the point origin, which, by contrast, information migrate without performing any processing, which involves communication costs, memory consumption, local processing, among others. The use of mobile agents RIS should be made with caution due to acknowledgments and retransmissions that data and procedures in the RIS can carry a high energy consumption, which represents a decline in the lifetime of the network.

CHAPTER 4 PRESENT WORK

Many research projects are made on clustering in VPNs. Clustering protocols in VPN can be of homogenous or heterogeneous type. Cluster heads are elected in a stochastic and periodic manner. Hybrid Energy Efficient Distributed clustering protocol uses a probabilistic method of electing cluster heads. It guarantees a well distributed election of cluster heads. However, election of low energy cluster heads may lead to poor stability period. Generic Clustering algorithms consider residual energy for the election of cluster heads. A neighborhood with more than a single advanced node will elect a single cluster head. It may lead to the election of plain nodes as cluster heads.

Weight based clustering provide a weight based election of cluster heads. The weight depend upon several factors viz.(i) duration for which a sensor node has been a cluster head, (ii) its proximity to neighborhood nodes, (iii) node's mobility and (iv) deviation from average degree. It forms an independent dominating set. Election of an independent dominating set may lead to a suboptimal election of cluster heads as more than one heterogeneous sensor node may lie within the same neighborhood

Design a device Network

Consider a group of sensors distributed during a field. we have a tendency to assume the subsequent properties regarding the device network:

The device nodes area unit stationary.

Links area unit radically symmetrical, i.e., 2 nodes s1 and s2 will communicate victimization identical transmission power level.

The network serves multiple mobile/stationary observers, which suggests that energy consumption isn't uniform for all nodes.

Network is homogeneous i.e. all nodes have same energy at the start.

Nodes area unit left unattended once readying. Therefore, battery re-charge isn't potential.

Each node contains a mounted range of transmission power levels.

The Cluster Formation

Assume that n nodes area unit distributed during a field and also the higher than assumptions hold. Our goal is to spot a group of cluster heads that cowl the whole field. A node will be a region of single cluster solely. Nodes and cluster heads area unit victimization geometrician distance formula to calculate internodes distance.

The following necessities should be met:

- Clustering is totally distributed. Every node severally makes its selections based mostly solely on native data.

- Clustering terminates at intervals a set range of iterations (regardless of network diameter).

- At the top of every iteration, every node is either a cluster head, or not a cluster head (which we have a tendency to check with as an everyday node) that belongs to precisely one cluster.

- Clustering ought to be economical in terms of process complexness and message exchange.

- Cluster heads area unit well-distributed over the device field, and have comparatively high average residual energy compared to regular nodes.

• An advanced node that is lying within the locality of another cluster head should be elective as a cluster head instead of electing it a member of that cluster.

The overarching goal of our approach is to prolong network period of time. For this reason, cluster head choice is based on the residual energy of every node. Measurement this residual energy isn't necessary, since the energy consumed per bit for sensing, processing, and communication is often far-famed, and thus residual energy will be calculable. To extend energy potency and more prolong network period of time, we have a tendency to additionally think about intra-cluster ―communication cost‖ as a secondary agglomeration parameter. For instance, price will be a operate of neighbor proximity or cluster density.

We use the first agglomeration parameter to probabilistically choose associate degree initial set of cluster heads, and also the secondary parameter to ―break ties‖ among them. A tie during this context means a node falls at intervals the ―range‖ of quite one cluster head. The first parameter is residual energy and secondary parameters area unit distance between cluster head and nodes.

Algorithm incorporates some options of fuzzy c suggests that algorithmic rule for electing cluster head. In fuzzy agglomeration, each purpose contains a degree of happiness to clusters, as in symbolic logic, instead of happiness fully to merely one cluster. Thus, points on the sting of a cluster could also be within the cluster to a lesser degree than points within the center of cluster. Symbolic logic provides a rigorous pure mathematics for coping with inaccurate data. The linguistic input variables of the system area unit the remaining energy, expressed in percentages and also the distance between non-CH and CH (expressed in meters). The specifications connected for the input and output functions of the system and their various Linguistic Values (LV) area units as follows:

• Residual energy: u= [0,100]: LV = low, average, high;

• Distance: u= [0,100]: LV = small, average, big;

• Probability: u= [0,1]: LV = very high, high, moderately high, fairly high, average, fairly low, moderately low, low, very low.

For the representation of the linguistic states (low, high, small and large) of the input variables, the degrees of membership to these sets must remain constant for certain values of the universe of discourse.

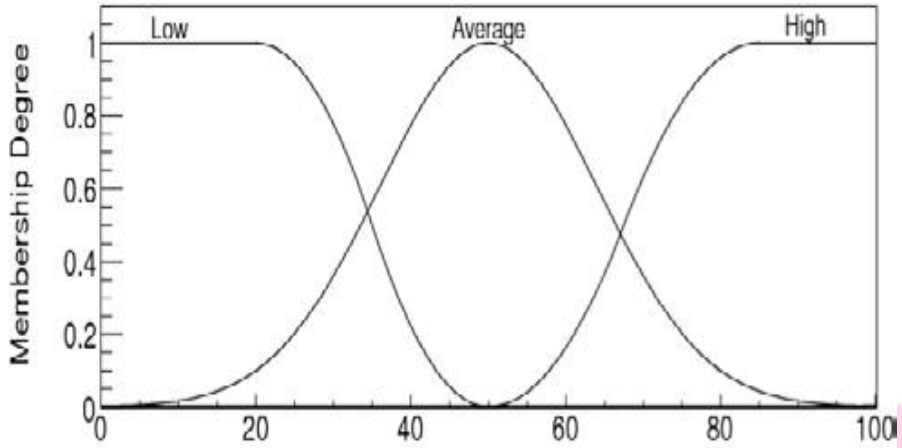


Figure 4.1: Membership Functions

The membership functions designed for the system are shown in figure 4.1. The rules are expressed as logical implications in the form of IF-THEN statements in a mapping from fuzzy input sets to output functions.

The rules are determined on the basis of an analysis of the whole network behavior through extensive simulations over time. They result in a class of higher probability, ensure an excellent chance these nodes will be elected, and differentiate depending on their distance from each CH.

Energy	**Distance**	**Probability**	
High	Small	very high	**y=1**
High	Average	high	**y=0.9**
High	Big	moderately high	**y=0.8**

Average	Small	fairly high	**y=0.6**
Average	Average	average	**y=0.5**
Average	Big	fairly low	**y=0.2**
Low	High	moderately low	**y=0.1**
Low	Average	low	**y=0.07**
Low	Low	very low	**y=0.02**

Table 4.1 shows the fuzzy inference rules used in the system.

The use of fuzzy logic is appropriate, whenever it is not possible to employ a mathematical model for the system. Additionally, fuzzy can reduce the complexity of the model; computational effort and memory. TS receive context information from nodes as input and converts into fuzzy linguistic variable input.

First order radio energy is used for performing radio analysis. It takes the following form

Energy	Amount
Einit	0.5 J
Eelec	50*0.000000001 J
EMP	0.0013*0.000000000001 J
Eda	5*0.000000001 J

Table 4.2: First order radio energy is used for performing radio analysis.

Where Einit is initial energy, Eelec is electrical energy, EMP is amplification energy, Eda is data aggregation energy. We have implemented the solution in three parts:

1. **Main**

2. **Existing**

3. **Proposed**

Existing is the function which implements weight based clustering. Proposed function implements FUZZY LOGIC BASED clustering which in enhanced form of weight based clustering in VPNs. Main calls Existing as well as Proposed function and perform analysis on performance of FUZZY LOGIC BASED clustering as compared to weight based clustering. Figure 4.2 gives the implementation modules of proposed system.

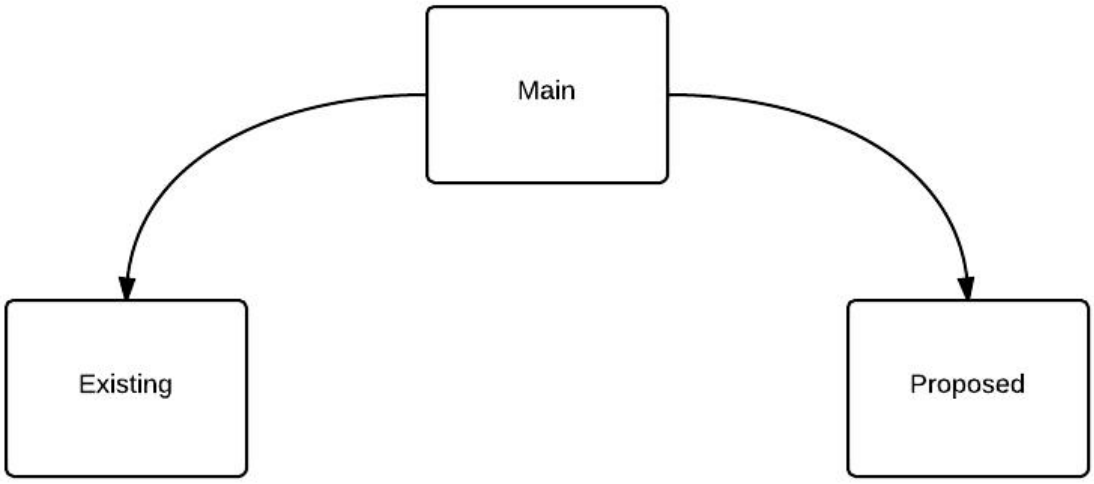


Figure 4.2: Implementation modules of proposed system

4.3 The Pseudo code

The Pseudo code of Proposed Model is as Follows:

Step1: Start

Step 2: Create a Network

Step 3: Create Clusters from network using:

a. A CH is selected from the SNs by considering a multiple metrics i.e. residual energy and a distance from non-CH to CH using the concept of Fuzzy logic and Cluster is created.

b. Based on last step, Non-CHs select the best CH based on distance metrices to become its member.

Step 4: Stop

The Flow Chart of the proposed model is given in figure 4.3:

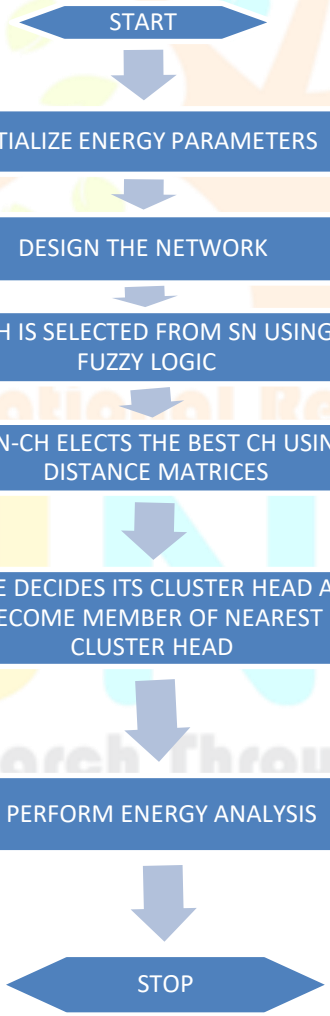


Figure 4.3: Flowchart for proposed model.

4.4 Research Methodology

We square measure victimization MATLAB for implementing our clump rule. MATLAB (matrix laboratory) may be a fourth-generation high-level artificial language and interactive surroundings for numerical computation, visual image and programming. MATLAB is developed by mathematics Works. It permits matrix manipulations; plotting of functions and data; implementation of algorithms; creation of user interfaces; interfacing with programs written in alternative languages, as well as C, C++, Java, and Fortran; analyze data; develop algorithms; and make models and applications. It's various intrinsically commands and mathematics functions that assist you in mathematical calculations, generating plots and playing numerical strategies.

4.4.1 Features of MATLAB

Following square measure the fundamental options of MATLAB:

- It may be an application-oriented language for numerical computation, visual image and application development.

- It conjointly provides associate interactive surroundings for repetitious exploration, style and drawback finding.

- It provides large library of mathematical functions for algebra, statistics, analysis, filtering, optimization, numerical integration and finding normal differential equations.

- It provides intrinsically graphics for visualizing information and tools for making custom plots.

- MATLAB's programming interface provides development tools for up code quality and maintainability and increasing performance.

- It provides tools for building applications with custom graphical interfaces.

It provides functions for desegregation MATLAB primarily based algorithms with external applications and languages like C, Java, .NET and Microsoft stand out.

CHAPTER 5 RESULTS

5.1 Simulation Scenario

Initially there is a network in which nodes are distributed randomly as shown in figure 5.1

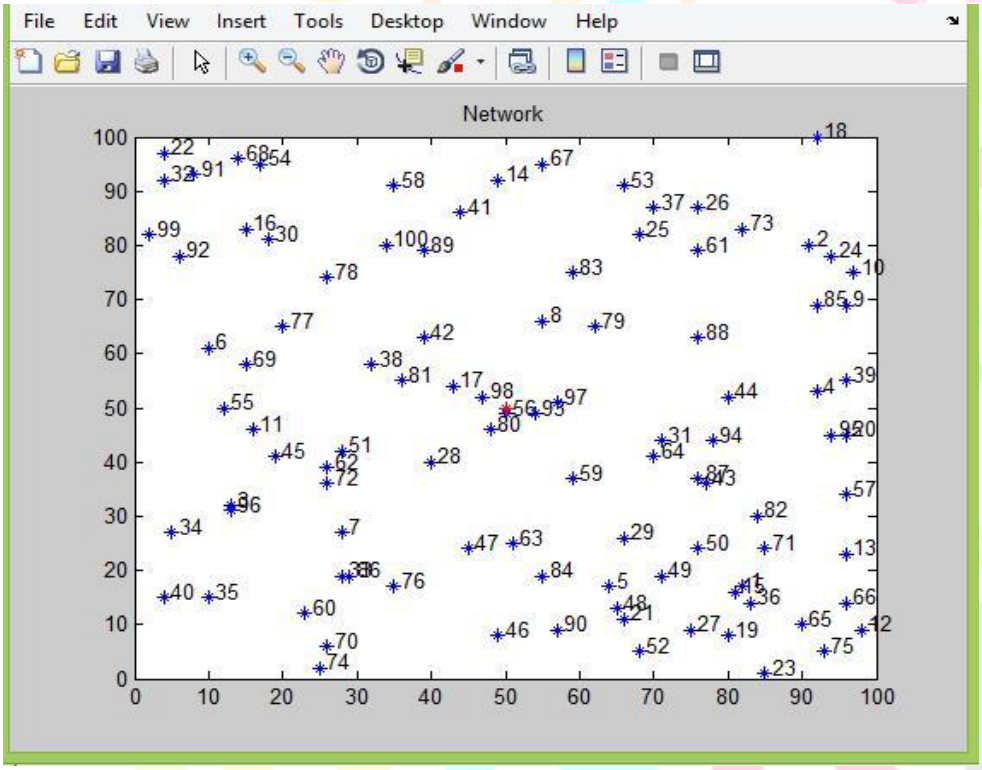


Figure 5.1: Network creation using 100 Nodes.

In figure 5.2 new schemes is implemented in which cluster head are elected based on the given logic of presented model. These cluster head are shown by star shape in blue color (*). Red stars are dead nodes.

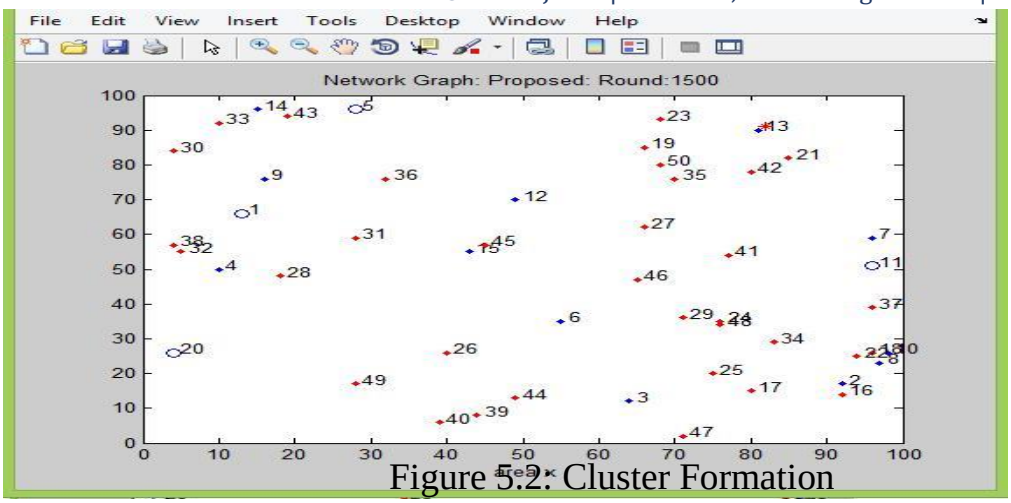


Figure 5.2: Cluster Formation

Each Normal node will elect its cluster head based on Probability which can be calculated Fuzzy Logic System using the two input variables ―distance between the node & cluster head‖ and ―Residual Energy‖.

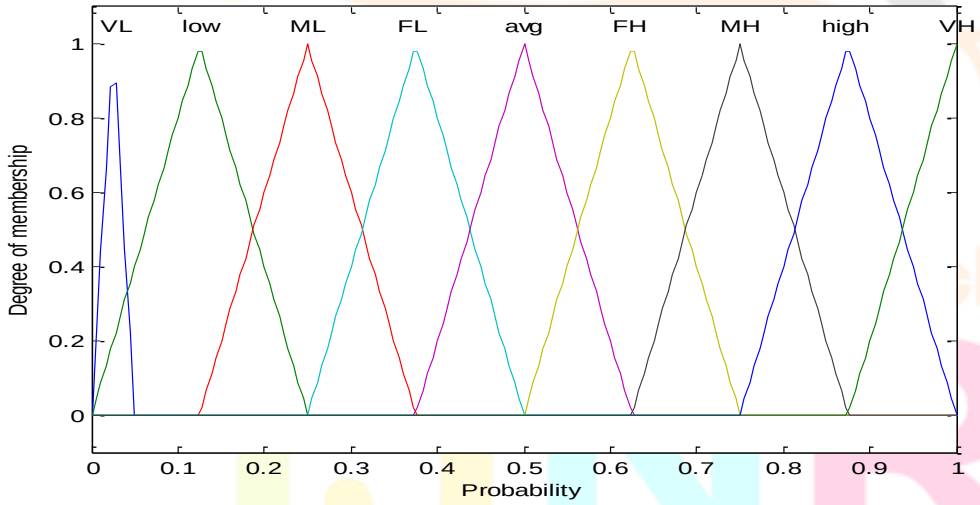


Figure 5.3: Correlation between Residual energy and Distance for Fuzzy system

Finally figure 5.4 shows the surface graph for probability calculation for cluster formation.

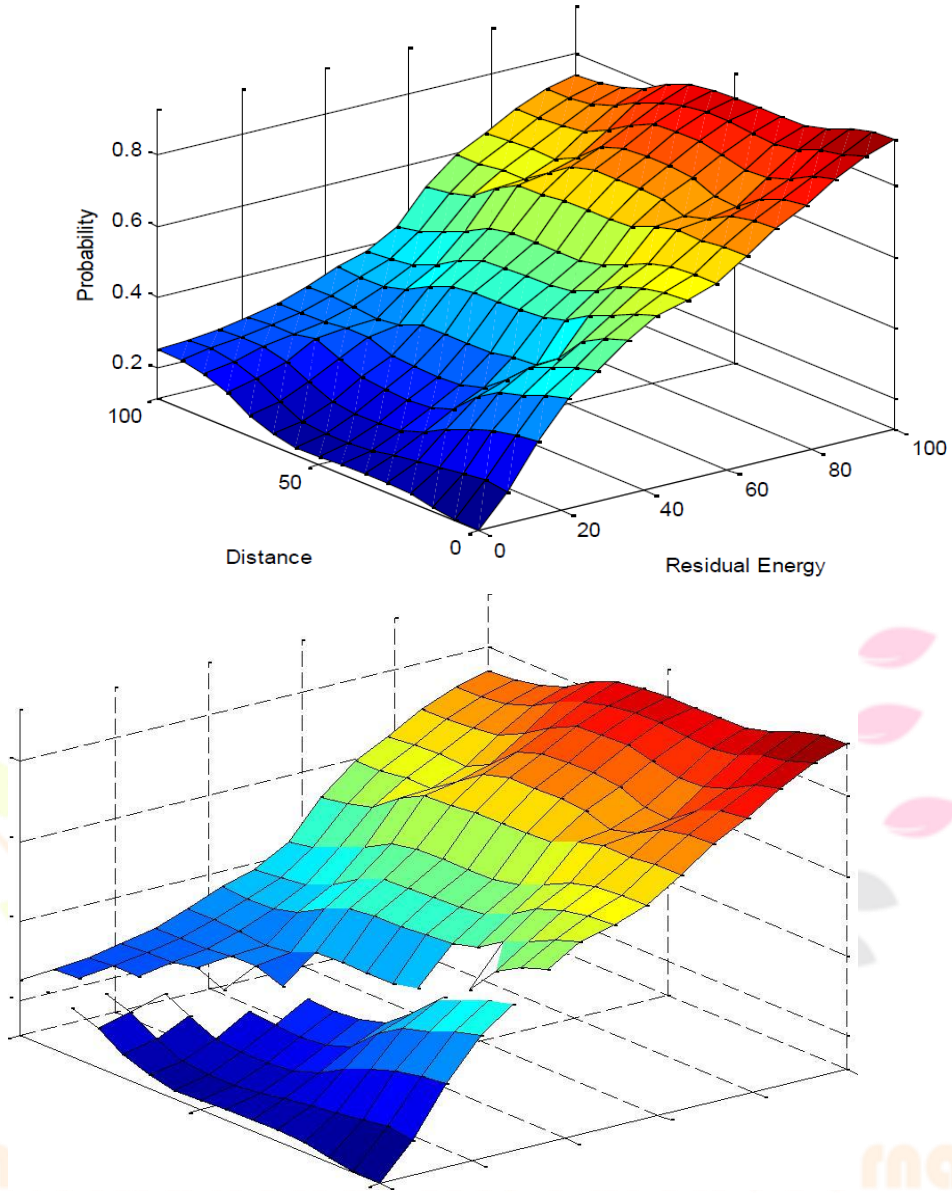


Figure 5.4: Surface Graph for Probability Calculation for cluster formation.

Using this Probability Calculation fuzzy logic, each normal node calculates the probability for each cluster head. The node which has the highest probability with respect to any cluster head will be the member of that cluster for cluster head in that round. In this way Cluster formation is done in the presented work.

5.2 Performance Evaluation

The 5.5 graph shows that first dead in our proposed algorithm happens after 700 rounds in spite of existing weight based algorithm which is having its first dead very close to 500 round. Hence our algorithm is Energy efficient then existing algorithm.

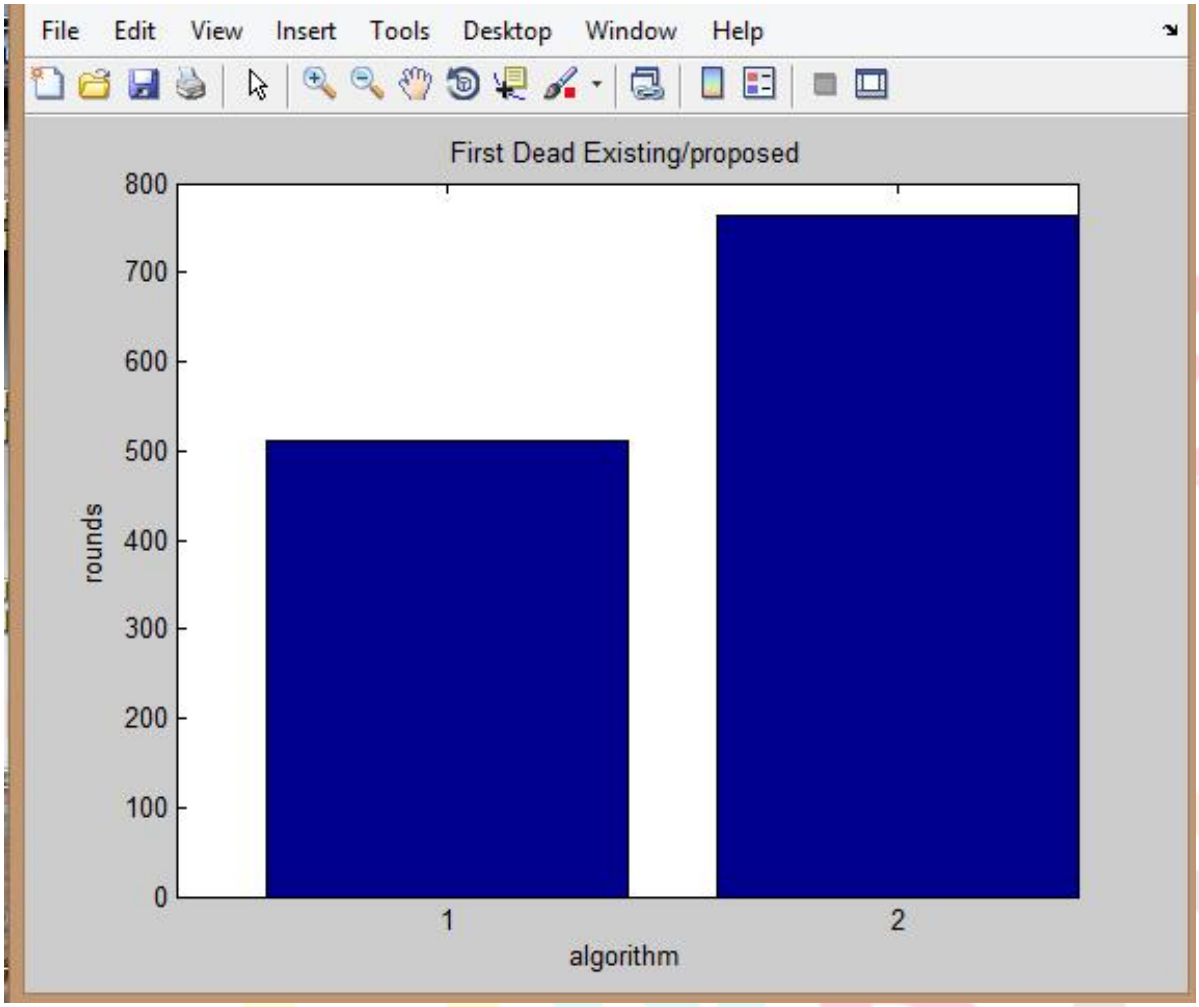


Figure 5.5: Comparison of existing and proposed system in terms of first dead.

Green line represents the proposed system and blue line represents the existing system. Graph shows that proposed system shows improved performance over existing system in 1000 rounds.

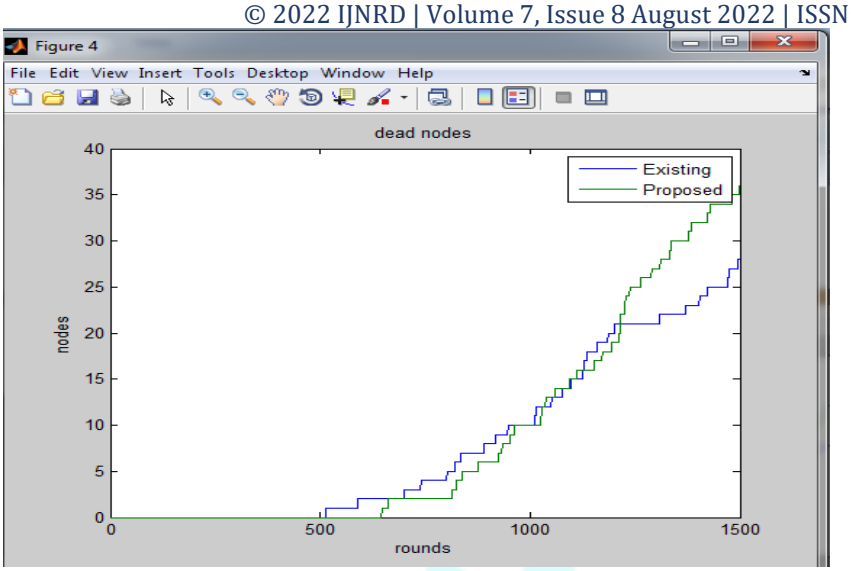


Figure 5.6: Comparison of the performance of existing and proposed system in terms of number of dead nodes with total number of clustering rounds

The graph 5.6 gives a comparison of the performance of existing and proposed system in terms of number of dead residual energy with total number of clustering rounds. Green line represents the proposed system and blue line represents the existing system. Graph shows that proposed system have almost same residual energy up to initial 500 rounds as existing system is having.

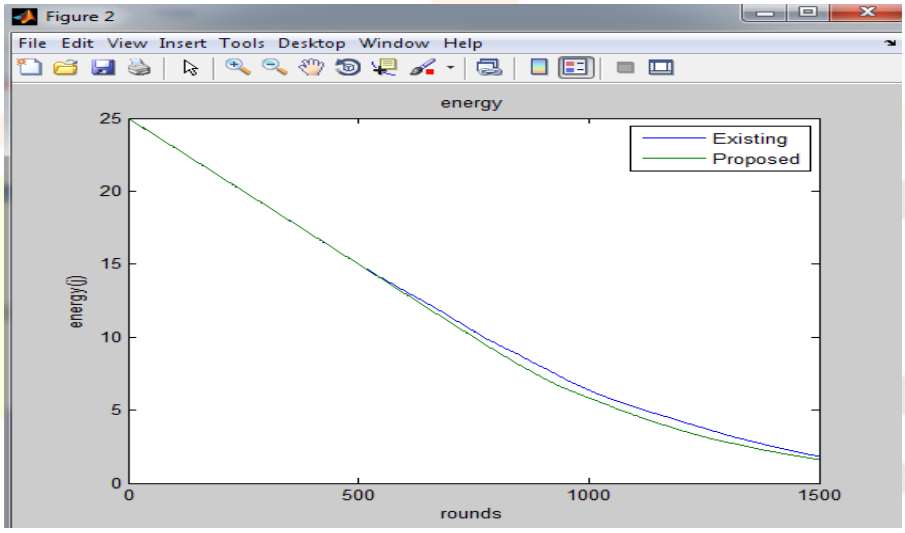


Fig: 5.7 Comparison of the performance of existing and proposed system in terms of number of dead residual energy with total number of clustering rounds

In this way, the mobile agent interact with external devices, process and collect information, and then returns to its origin with the data. Mobile agents have gained acceptance due to its feature mobility, since it has proven to be much more efficient than one agent is transferred to a remote

location, do a search, filter, process Reprogramming virtual private nodes in a RIS comprises two phases: the first is the dissemination of the code in the networks; this step involves shipping code efficiently and receipt by the destination node.

The second is to code execution. In the first phase, perhaps the more critical development is necessary efficient dissemination protocols consumption energy. Have been proposed different methods in the literature to address both stages. There are frame-based software development methods specific (middleware) in operating systems, scripts, databases and virtual machines. Rescheduling tests are usually performed in networks enabled for one or multiple hops. in this form, is calculated at each proposal adopted on time spent in reprogramming and its efficiency energy consumption.

The virtual private module is composed of part, by specific devices that capture data variables such as temperature, humidity, levels radiation, ammonia, methane, etc. and the other, for analog and digital converters. Consumption Power for the module is the execution of operations such as sampling of the signal, the analog / digital conversion or signal modulation. The virtual private module can operate in random mode or on a periodic basis, according to the configuration predetermined by the system administrator. Note that, in general, the operation of this module on a periodic basis is preferred. assuming that energy consumption in operations open (open), close (close) are constant, the energy consumed by the virtual private can be expressed.

It is important to note that both nodes the processor and the radio components sensors must work cooperatively to to perform a computational task; this fact implies the existence of a mutual relationship between all components and, hence, this relation energy consumption affects the entire node. Accordingly, in the calculations of evaluation performance should not be considered linearly independent, but should be account each component to calculate Full of energy consumed by the node.

The first thing that was done was a replacement classical base station for the RIS system embedded special, which is perhaps smaller and cheaper computer market. In this embedded system version runs as Java and Equinox. Additionally it is installed, as intelligent agent platform,

the AFME. In the embedded system intelligent agents deployed as modules called bundles. Moreover, in the nodes has a small virtual machine that allows a boards or tuples scheme, similar to the proposal.

Mobile agents are simple, they will, change the value and destroyed after perform its task. This with the intention of having increased spending on energy efficiency when transmit data from the base station to the virtual private node. Thus, it is intended to decrease unnecessary consumption of energy in the process wireless transmission to the base station virtual private. Arguably is a computational solution efficient where the best is to avoid confirmations and avoid unnecessary retransmissions from the nodes.

CHAPTER 6
CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

In this dissertation, we have presented an efficient technique for clustering of sensor node in the homogenous VPN. In the existing LEACH protocol the clusters are formed using the distance calculation from the node to cluster head. But for a network to be good designed there should be a better cluster formation.

For a better cluster formation the concept of fuzzy logic is used in which non-CHs select the best CH by considering a multiple metrics, i.e. residual energy and a distance from non-CH to CH. Then, non-CHs compute a probability value to each CH candidate. The non-CH chooses the CH with a higher probability value and sends a join message to CH.

The use of fuzzy logic is suitable, whenever it is not possible to use a mathematical model for the system. Additionally, fuzzy can reduce the complexity of the model, computational effort and memory. Energy consumption is affected by message communication between nodes, so our technique is efficient than traditional LEACH protocol.

Also weight based clustering protocol has the disadvantage that it elects unnecessarily extra cluster head. Sometimes Nodes with high residual energy were not given a chance to become cluster head. This disadvantage is overcome by FUZZY LOGIC BASED clustering algorithm.

All nodes with similar energy are given same chances to become cluster head. Also a node with high residual energy even if it is lying in captivity of another cluster head will be elected as a cluster head.

6.2 Future Scope

This algorithm is implemented for homogenous VPNs. Algorithm can be further implemented for heterogeneous networks.

REFERENCES

[1] Ajay Jangra, Swati, Priyanka, "Securing LEACH Protocol from Sybil Attack using Jakes Channel Scheme (JCS).

[2] Baiping Li1 and Xiaoqin Zhang, "Research and Improvement of LEACH Protocol for Wireless Sensor Network," 2012 International Conference on Information Engineering, Vol.25

[3] Bijan Kumar Debroy, "An Efficient Approach to Select Cluster Head in VPN", Journal of Communications, Vol. 6, No. 7, October 2011.

[4] David Gugelmann, Philipp Sommer, and Roger Wattenhofer "Poster Abstract: Reliable and EnergyEfficient Bulk-Data Dissemination in VPN," in proceedings of SenSys'10, November 3–5, 2010.

[5] Deng Zhixiang, "Three-layered Routing Protocol for VPN based on LEACH Algorithm," IEEE, 2008.

[6] Fan Xiangning, "Improvement on LEACH Protocol on Wireless Sensor Network," mt. Conference on Sensor Technologies and Applications, 7 July, 2007.

[7] Fuzhe Zhao, You Xu, Ru Li, Wei Zhang, "Improved Leach Communication Protocol for VPN," Int. Conference on Control Engineering and Communication Technology,2012.

[8] Fuzhe Zhao, You Xu, Ru Li, Wei Zhang, "Improved Leach Communication Protocol for VPN", 2012 International Conference on Control Engineering and Communication Technology IEEE.

[9] Haosong Gou, "An Energy Balancing LEACH Algorithm for VPN," 7th Conference on Information Technology, 3 October, 2010.

[10] Heewook Shin, SangmanMoh, and Ilyong Chung, "Energy-Efficient Clustering with One Time Setup for VPN" IEEE 2012.

[11] Hemant Sethi, Devendra Prasad, and R. B. Patel "EIRDA: An Energy Efficient Interest based Reliable Data Aggregation Protocol for VPN," in proceedings of International Journal of Computer Applications, Volume 22– No.7, May 2011.

[12] Hu Jumping, "A Time-based Cluster-Head Selection Algorithm for LEACH", IEEE, 1 August, 2008.

[13] Jia Xu,et al, "Improvement of LEACH protocol for VPN," 2012 IEEE

[14] Jun YUE, Weiming ZHANG, Weidong XIAO, Daquan TANG, Jiuyang TANG, "A Novel Unequal Cluster-based Data Aggregation Protocol for Wireless Sensor Network," Przegląd Elektrotechniczny, ISSN 0033-2097, R. 89 NR 1b/2013.

[15] Li-Quing Guo, "Improving the LEACH protocol for VPNs", Wireless Sensor Network, 2010. IET-VPN. IET International Conference

[16] M. Bani Yassein, A.Alzoubi, Y.Khamayseh, W.Mardini "Improvement on LEACH protocol of Wireless Sensor Network(VLEACH)",International Journal of Digital Content Technology and its Applications, Volume 3, Number 2,June 2009

[17] M. Ma and Y. Yang, *"Data gathering in VPNs with mobile collectors,"* in Proceedings of the 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS '08), April 2008.

[18] Mingming Lu and Jie Wu "Utility-Based DataGathering in VPN with Unstable Links," proceedings of the 9th international conference on Distributed Computing and Networking ICDCN' 08, pp. 3-24, 2008

[19] Mu Tong and Minghao Tang. 2010. "LEACH-B: An Improved LEACH Protocol for Wireless Sensor Network", Proceedings of 6th International Conference on Wireless Communications Networking and Mobile Computing, pp. 1-4

[20] Muhamnmad Omer Farooq, Abdul BasitDogar, Ghalib Asadullah Shah, *"MR-LEACH: Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy"*2010 Fourth International Conference on Sensor Technologies and Applications IEEE.

[21] Muhammad Omer Farooq, "MR-LEACH: Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy," Fourth Int. Conference on Sensor Technologies and applications, 2 October, 2010.

[22] Nandini. S. Patil, Prof. P. R. Patil, "Data Aggregation in Wireless Sensor Network," IEEE International Conference on Computational Intelligence and Computing Research,2010.

[23] Ren P. Liu, John Zic, Iain B. Collings, Alex Y. Dong, and Sanjay Jha "Efficient Reliable Data Collection in VPN," in proceedings of IEEE 68th Vehicular Technology Conference, VTC2008 , 2008.

[24] Volker Turau and Christoph Weyer "Long-term Reliable Data Gathering Using VPN," proceedings of 4th International conference on networked Sensing Systems INSS '07, pp. 252-259, June 6-8 2007.

[25] W.B.Heinzelman, A.P.Chandrakasan and H.Balakrishnan, "AnApplication-Specific Protocol Architecture for Wireless Microsensor Networks," Transactions on Wireless Communications, Vol. 1, No. 4, pp. 660-670, October, 2002.

[26] W.R. Heizelman, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", Proc. 33rd Hawaii Int. Conference on System Science, Vol. 2, 4-7 Jan,2000.

[27]. Wei Bo Hu Han-ying Fu Wen "An Improved LEACH Protocol for Data Gathering and Aggregation in VPN", International Conference on Computer and Electrical Engineering, 2008.

[28] Wei Wang, Qianping Wang ; Wei Luo," LEACH-H: An Improved Routing Protocol for Collaborating Network", IEEE International Conference on Wireless communication, pp.1-5, 2009.

[29] Wu Xinhua, "Performance Comparison of LEACH and LEACH-C Protocols by NS2," 9th Int. Symposium on Distributed Computing and Applications to Business, Engineering and Science, 5 October,2010.

[30] Yuling Li, Luwei Ding, FengLiu, "The Improvement of LEACH Protocol in VPN", 2011International Conference on Computer Science and Network Technology IEEE.