Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Principles and Concepts of Wireless Sensor Network and Ant Colony Optimization: A Review

Renu Jangra
Ph.D., Research Scholar
Department of Computer Science & Applications
Kurukshetra University, Kurukshetra, India

Dr. Ramesh Kait
Assistant Professor
Department of Computer Science & Applications
Kurukshetra University, Kurukshetra, India

Abstract: Wireless Sensor Network (WSN) is a suitable technology that joins the sensing; processing; and wireless multi-hop networking. The given paper provides an extensive evaluation about WSN concepts including basic of WSN, architecture of sensor node and architecture of communication protocol in WSN. Furthermore, characteristics, challenges, designing issues, applications, security issues, routing protocol of wireless sensor network are given. Also, the concept of Ant colony optimization (ACO) with its basic principle, pseudo code and flowchart are explained. The entire features create the paper helpful for wide selection of potential readers, research workers in WSNs, students doing research work in WSNs and WSN application designers.

Keywords: Wireless Sensor Network; Ant Colony Optimization; Routing Protocol

INTRODUCTION

1. Wireless Sensor Network:

Wireless Sensor Network (WSN) is the network that is wireless consists of a base station (BS) and hundreds or thousands of sensor nodes, to sense the motion, temperature & pressure, etc., in diverse atmospheric condition. Attribute of sensor networks, is the cluster of sensor nodes, to generate high class information about the sensing surroundings. These nodes are self-organized. They are competent of wireless communication. It is forced in circumstances of memory; dimension, energy, processing power and sense environmental data. Sensor nodes perform a inadequate/limited processing & communicate over short distances [1].Thus, a wireless sensor network has sensing component as well as the capabilities of, on--board processing, storage and communication. By these improvements, a sensor is prone for data collection correlation, in network examination and combination of other sensor nodes data and its own sensor data also. While several sensors nodes supervise the large physical environment, they structure a wireless sensor network. The sensor nodes communicate with each another and with the base station (BS) also with the use of wireless radios. These wireless radios allowing them to broadcast their sensor data help in distant processing, visualization; analysis; and storage systems [2].

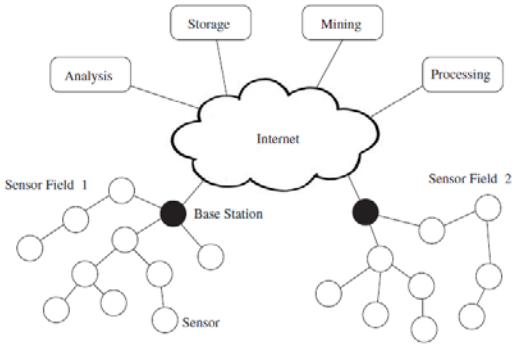

Fig 1. Wireless Sensor Network

For example: In Fig 1, two *sensor fields* monitoring two dissimilar geographic regions and using their base stations, they are connected to the internet. Senor nodes have varying capabilities i.e. a single physical event is observed by simple sensor nodes, while additional complex devices may merge many dissimilar sensing methods [magnetic; acoustic; and optical]. Their communication capabilities also vary. For example, with changeable data rates and latencies of UF (ultrasound frequency), infrared or radio frequency (RF) technologies. . The straightforward sensors can only gather and communicate the information regarding the experimental environment but devices having capabilities like large storage, processing, energy capability may perform wide-ranging processing and the aggregation functions. These types of devices have extra farm duties often in a WSN. For example: these devices may form a communication spine that may be used by further resource-constrained sensor devices to arrive at the BS. In conclusion, a few devices have the right to use the extra supporting technology like Global Positioning System (GPS) receivers allowing sensors to find out their position accurately. Still such systems regularly use a large amount of energy to be reasonable in favor of low-cost and low-power sensor nodes.

1.1 Architecture of Sensor Node:

The technique sensing is used to collect the information of a physical entity as well as the occurrence of the events, i.e., modification in a state like fall in pressure and temperature. An object doing such a sensing job is called a *sensor*. A sensor is a tool that converts parameters in the material world into signals that can be calculated and analyzed. Sensor node has onboard storage and embedded processing capabilities. The node contains so many sensors working in the acoustic; seismic; radio (radar); infrared; optical; magnetic; and chemical or natural fields. Every scattered sensor nodes have the skill [39] to assemble data; evaluate and direct them to a chosen sink position.

Sensors are classified into three parts: (i) Passive (ii) Omni-directional sensors (iii) Narrow-beam sensors (iv) Active sensors. Passive sensors give the good judgment about the data without really influencing the surroundings via active probing. These are self powered means that energy is only

© 2015-19, IJARCS All Rights Reserved

required to increase their analog signals. But, the active sensors actively explore the atmosphere, for example; a sonar or radar sensor and they want nonstop energy from a power resource. The narrow-beam sensors include a definite concept of way of measurement, same as the concept of a camera. The Omni-directional sensors have not the concept of way of measurement and direction.

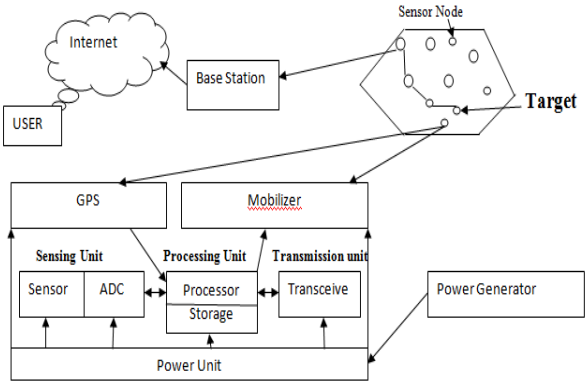

Fig 2: Sensor Node Architecture

The main point of sensor networks is given as:

- Sensor nodes are strongly deployed.
- Sensor nodes have chances of failure.
- The physical arrangement of a sensor network alters repeatedly.
- Sensor nodes have power; computational capacities; and memory that are very limited.
- Sensor nodes have huge overhead and have many nodes so they may not have any global identification number.

Sensors

Dimension	Small. Example : nanoscale electromechanical systems (MEMS)	Medium. Example : micro scale electromechanical systems (MEMS)	Large. Example : radars, satellites in cubic centimeters to cubic decimeters
Movement	Stationary. Example : seismic sensor	Mobile .Example : on robot vehicles	
Category	Passive. Example : acoustic; seismic; video, infrared, magnetic	Active. Example : radar, ladar	

In Fig 2, Architecture of sensor node contains six parts: Sensing unit; Processing unit; Transmission unit; Power unit; Global Positioning System and mobilizer.

Sensing Unit: Information gathering as input like pressure, temperature etc., from the environment is performed by the sensing unit [40] and generates the output in the form of electrical and optical signals. The analog signals are transformed into digital signal by ADC (Analog to Digital Converter).

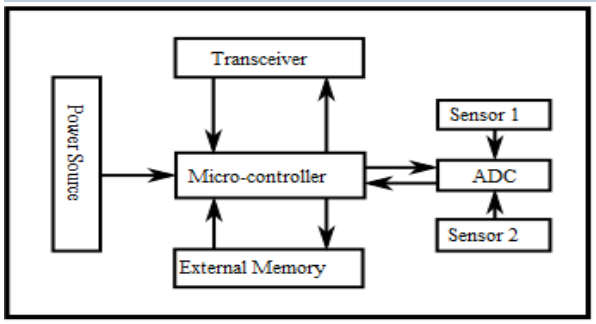

Fig 3: Architecture of Sensor Node

Transceiver: It contains the properties of both transmitter and receiver . The prepared states of transceiver devices are transmission, receive, unused, and sleep. The transceivers working in sate of idleness have same amount of power consumed in sending and receiving. So, it's good to stop the transceiver device when it is not used.

Memory: The requirement of memory is depend on the person who is using it. There are two types of memory depend on the reason of storage. These are user memory used for saving the application based data or personal data; and the program memory that is used in programming the device.

Power: Power is provided to every sensor node through battery. As sensor nodes are put in place where it is difficult to reach so, it is difficult to provide main power supply and also difficult to change the battery regularly. Node required power for sensing, communicating and data processing. Power is stock up either in battery or in capacitors. The batteries can both rechargeable and non-rechargeable and are the key resource of power provider for sensor nodes. Now, solar sources are used by the sensors to renew their energy; temperature differences; or vibration.

GPS: The sensor node can also find out the location and position through the global positioning system (GPS).

Controller/ The microcomputer: The controller performs the task of handing out the data and has power to handle the other components' functionality in the sensor node.

1.2 Architecture of communication protocol in WSN

The OSI model is a conceptual model that demonstrates the communication functions of layers used in telecommunication with no consideration of the internal configuration and technology. The OSI has aim is the interoperability of different communication systems with standard protocols.WSN based on OSI have mainly five layers named application layer; transport layer; network layer; data link layer; and physical layer. Also, the three cross layers planes are added above those five layers of OSI model named as power management plane; connection management plane; and task management plane. The features of these layers are to handle the connection of network and permit the nodes to job together to boost the efficiency of the network as a whole.

© 2015-19, IJARCS All Rights Reserved

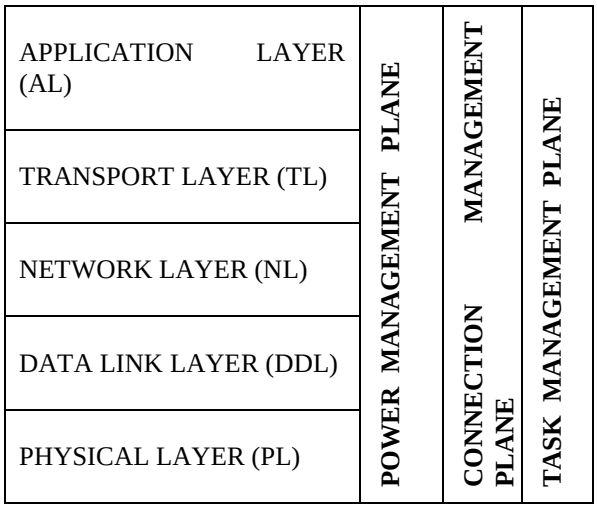

Fig 4: Layers of WSN

Physical Layer: In this layer, bits are transmitted instead of complete packet over the transmitted medium. It interacts with MAC layer to detect and correct error and performing transmission and modulation. Maximizing of network lifetime and minimizing of energy consumption is starts from the physical layer in WSN. Energy is consumed in service radio signals and in transmission of bit. Radio signal consumed the fixed energy but energy spent during bit transmission varies and depend on distance, channel loss and interference. The devices used at physical layer are repeater, hub, controller, network adapter etc [41].

Data link layer: This is the layer that has the charge of transmit the data between the two nodes of similar link by break up the input data into data frames. It provides the services that comprise medium access control; detection of error; reliable delivery; and correction of error [42]. For data transfer in wireless, there is a requirement of medium access control and its management.

DDL (Data Link Layer) has two sub layers:

- LLC (Logical link Control) – present at the top of DDL provide flow control and provide flow control error notification, address and control of data link.
- MAC (Medium access control) - present at the bottom of DDL and provide user access, frame structure delivery and frame synchronization.

Network Layer: It handles the routing of data throughout the network from source to the target and successfully routing packets along the path. The requirement of different routing protocol varies and depends on the communication path set up. Some routing protocol favor the path that assist WSN to convey the QoS and other the best lifetime and so on [43].Routing protocols in WSNs are at the variance from conventional routing protocols in numerous ways like IP addresses are not contains in sensor nodes that is why routing protocols that are based on IP are not used in a WSN.

Transport layer: This layer ensures the consistency and superiority of data at the source and destination. It provides host to host and end to end communication services like flow control, multiplexing and reliability. It uses TCP (Transmission Control Protocol) connection oriented and UDP (User Datagram Protocol) connectionless protocol.

Application layer: The AL layer resides close to the user of the system [44]. Various applications are implemented here including Telnet, HTTP, FTP, SMTP etc. In case of WSN, the application layer programming mainly deals with processing, encryption, formatting and storage of sensed information. It also examines the essential layers to sense if satisfactory network assets and services are existing to meet the user's necessity.

Cross layer plane: To increase the network efficiency, management of network and node coordination, the cross plane layers are used.

- **Power management plane**: It manages the power that a node used for sensing, processing and communication. For example, when the node has low power intensity, it informs the cross plane and node does not participate in any activities like sensing.
- **Connection management plane:** Management of network configuration is done by this layer for better connectivity of nodes.
- **Task management plane:** Distribution of task among the nodes for better utilization of resources, so the network lifetime is better.

1.3 Characteristics of Wireless Sensor Network:

Following are the major characteristics of wireless sensor network [3].

- **Size** : Size of nodes may be small(nanoscale electromechanical system) , medium (micro scale electromechanical system) and large(radar ,satellite) cubic centimeter .
- **Physical security:** Sensor nodes are prone to failure for the reason that each sensor node should have plenty of safety mechanism in order to test unauthorized access, attacks, and accidental harm of the information within the sensor node. Moreover, additional isolation method must also be built-in.
- **Power**: As the size of nodes is small, low battery usage required.
- **Memory space:** Limited processing and power capabilities.
- **Unreliable communications**: It can be communicated in RF, Infrared; optical and acoustic medium. No raw data is transmitted to increase the lifetime of network. Unreliable Transfer: Usually the routing based on packet routing in sensor network is connectionless and hence inherently unreliable • Conflicts: The communication may be unreliable even if the channel is reliable. This is due to the broadcast nature of the WSN.
- **Low cost**: In WSN, to measure the physical environment thousands of sensor nodes are used for fulfill the purpose. With the aim of reducing the cost of the network as a whole must keep the sensor nodes cost at the very low rate [51].
- **Energy efficient**: To perform the different tasks like communication, computation and storage, energy is required. And this energy should always be available, when need to perform above tasks, that is, there should be an option to recharge the sensor nodes. So, during design phase, the protocols and good algorithms must be considered and developed.

1.4 Challenges and Designing Issues in WSNs:

Following are the parameters that are considered while designing of WSNs [27].

© 2015-19, IJARCS All Rights Reserved

- **Deployment of nodes**: Location of nodes in network.
- **Power consumption**: As energy consumption, determine the life span of the wireless sensor network. Most of the sensor nodes make use of battery power as their source of energy .So, there is necessity to develop the network which efficiently uses the battery power and also the software and hardware blueprint needs to be carefully designed so, used the energy efficiently.
- **Heterogeneity of network**: Heterogeneous wireless sensor network have sensor nodes which have diverse calculating power and sensing range.
- **Topology of the network**: Though, WSNs have advanced in lots of phases, still this is the network that is constrained in provisions of energy resource; computing power; memory; and connections capabilities. Out of these constraints, energy utilization is more vital, that is proved by the huge number of algorithms; techniques; and protocols to accumulate energy .Hence, expand the natural life of the network. Topology safeguarding is one of the most significant issue find out, to decrease the energy consumption in WSN.
- **Reliability& scalability**: There are many nodes in WSN. Depending on the need, the quantity of nodes can be amplified or diminished. The wireless sensor network should be such that it should be capable of accepting new node and synchronize them with already present nodes.
- **Medium of transmission**: The communicating nodes are connected by a wireless intermediate in a multi-hop sensor network. The communiqué between the nodes are done using radio transmission as well as optical or infrared communication .The conventional problems (fading & high error rate) associated with a wireless channel possibly will also influence the action of the sensor network.
- **Fault tolerance**: It is very common for the sensor nodes to turn into a defective and a unreliable due to the operation of sensor nodes in an unrestrained environment. The nodes can be failed due to the hardware problems or physical break or by draining their power supply. Due to this, some nodes cannot communicate with other nodes. We look ahead that the node breakdown to be much more than the one presented in wired or wireless infrastructure networks. Thus, the structure can be flexible to the arrival of defective nodes.
- **Cost**: If the cost of conventional sensors is fewer than the cost of network then wireless sensor network is not defensible.

1.5 Applications of WSN:

Following are the application [4] of WSN:

1.5.1 **Health**: Variety of health parameters, chronic disease are monitored by WSN and it is also used in various hospital sensors.

- **Monitoring**: WSN used for measuring heart rate function, glucose level and discovery of cancer..
- **Chronic Disease: Chronic** diseases like Cochlear implants and artificial retina are treated with the help of WSN application.
- **Hospital Sensor: Sensor** nodes are used for intellect the data for observing the vital signs; and the record anomalies.

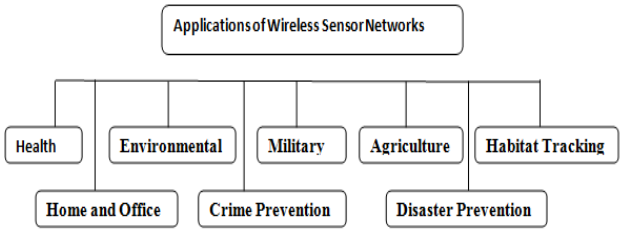

Fig 5. Classification of WSN applications

1.5.2 **Environmental:** The WSNs employ for environmental concerns such as mapping of bio complexity for environmental, detection of fire in forest, water and air pollution detection. It is also used for flood detection and precision agriculture.

1.5.3 **Military:** WSNs use for monitoring enemy strength movement and utilize in bullets and equipment.

1.5.4 **Home and Office:** The WSNs knowledge also used for residence and office application to manufacture the smart environment and in automation of homes/offices.

1.5.5 **Habitat Tracking:** The WSNs offer a way to follow and supervise the habitat movement and actions in the place where it is not possible to place the network.

1.5.6 **Disaster Prevention:** The WSNs is capable to guess the seismic activities of earthquakes and avoid the tragedy result of earthquakes as much as feasible with the aid of sensor nodes.

1.5.7 **Crime Prevention**: Crime prone region is simply tracked and examine with the help of WSNs and can effortlessly avoid crime rate.

1.5.8 **Agriculture Application:** By wireless input output sensor devices, water systems are supervised by pressure transmitters sensors to confirm the level of water in tanks and pumps.

1.6 Security problems in WSN:

Security required both for operation of the network and for maintaining the accessibility of the complete network. So, it is essential to be familiar with and understand the following security requirements prior to implementing the safety plan for WSN.

a. Data Integrity

It is desirable to make sure the consistency of the data. It conforms that the data packets which are received by the sink is same as the data packets which is transmitted by the sender. Any person in the middle cannot alter that packet. Message digest and MAC are the techniques of integrity of the data. The data integrity attacks can be resolved by providing these data integrity methods. Data integrity is accomplished by way of validation the data content.

b. Data Confidentiality

Confidentiality of data is to defend it and only be understood by the intended recipient during communication in a network. Cryptography techniques are used to provide confidentiality. The confidentiality of data on the network means that the data is transfer between source and sink will be entirely safe and not the third entity has right to use it. The confidentiality of the data can be attained by means of cryptography methods like symmetric or asymmetric key.

© 2015-19, IJARCS All Rights Reserved

c. Data Availability

Availability ensures that the services are available all the time in the network even when any type of attack is occur such as Denial of Service attack. It decides whether a node has the ability to use the resources & whether the network is accessible for the messages to communicate. The researchers planned different mechanisms to achieve this goal. It guarantees that sensor nodes are active in the network to fulfill the functionality of the network.

d. Data Authentication

The data authentication confirms the receiver that the data has not been changed during the broadcast of a sensor node. It is attained by symmetric or asymmetric mechanism where the secret key is shared between both sending and receiving nodes. In asymmetric cryptographic, the authentication of any message or user is authenticate by digital signatures whereas in symmetric key; (MAC) Message Authentication Code are used for authentication purpose

e. Data Freshness

Freshness of data makes sure that the data received by the recipient is the current and fresh data and no rival can repeat the previous data. Data freshness is very essential because an attacker can send an expire packet to misuse the network resources and lessen the network lifetime. The freshness in data is attained by using mechanisms like timestamp by adding it to each data packet.

Types of Attack: Attacks can be divided into two main categories: Active Attacks and Passive Attack

a) Active Attack: it can be stated that the attack implies the disturbance of the normal functionality of the network means that the information is interrupted; modified, or fabricated. Active attacks examples include jamming; impersonating; modification; denial of service (DoS); and message replay.

- **DoS**: is an effort to build a computer resource that is unavailable to its intended users. Even though the means to carry out the motives and targets of a DoS attack may vary and generally consists of the intensive efforts of a person or persons to stop an Internet site or service from the working of its function efficiently or at all, momentarily or indefinitely. Perpetrators of DoS attacks mainly target the sites or services hosted on a high-profile web servers such as banks; credit card payment gateways, and even root name servers [37].
- **Replay attack**: A replay attack is a violation of security. In this attack the information is stored without authorization and then retransmitted to trap the receiver into illegal operations such as fake identification or authentication or a duplicate transaction. For example; post from a certified user who is logging into a network may be captured by an invader and resent (replayed) the next day. Even though the messages are encrypted and the invader may not recognize what the real keys and passwords are, even then, the retransmission of valid logon posts is adequate to achieve the access to the network. Also known as a "man-in-the-middle attack". A replay attack can be prohibited by using strong digital signatures that contain time stamps and inclusion of unique information from the earlier transaction such as the value of a constantly incremented the sequence number.
- **Jamming**: Jamming attack prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on. It is a kind of Denial of Service attack. Jammers attempt to purposely insert fake data throughout the communication between two nodes which affects the data transmission and also the performance of WSN reduces as it causes the overutilization of the scarce resources like battery power, memory etc[38].

b) Passive Attack: The attack acquires the exchange of data in the network without disrupt the communication. Passive attacks examples are eavesdropping; traffic analysis; and traffic monitoring.

- **Traffic analysis**: Traffic analysis works on patterns. It is the process of interrupting and examining messages in order to infer information from patterns in communication.
- **Eavesdropping**: The term *eavesdrop* derives from the practice of actually standing below the eaves of a house, listening to the conversations inside. Eavesdropping is illegal access to the real-time interception of a personal communication like a phone call; instant message; and videoconference or fax transmission.

1.7 Routing Protocol:

It can be classified as

- Based on the style of functioning, routing classified as Proactive; Reactive; and Hybrid.
- Based on the participation fashion of nodes, routing classified as direct communication; Flat; and Clustering.
- Based on the network structure, routing classified as Hierarchical; Data Centric; and Location based.

Based on style of of functioning, routing classified as proactive; Reactive; and Hybrid:

- **Proactive:** Proactive routing protocol maintains a table of routes of nodes by the broadcasting routing information. Information regarding route of each node is available before it needs [49]. If traffic occurs at one route then route can be changed with the help of routing table that contains the updated information of routes of all the nodes. Following are the proactive routing protocol SPIN, Directed Diffusion (DD), LEACH, SPEED and GBR.
- **Reactive:** In this, routing table is not maintained in advance but the route setup between source and sink is worked on its dynamic search according to demand. To find out the path from source to target, a route discovery query is apply and for replies, the reverse path is used. Once the route is recognized, it is maintained by the route preservation process [50]. Following are the reactive routing protocol TEEN, GEAR, PEGASIS, ACQUIRE, MCFA, CADR.
- **Hybrid:** Hybrid routing uses both proactive; and reactive routing. Hybrid routing is used for large network. The network is divided into clusters. When routing needed within the cluster, proactive routing is used and if outside then reactive.

Based on network structure, routing categorized as Hierarchical; Data Centric; and Location Based:

- **Hierarchical Routing Protocol**: It is performed the energy-efficient routing in WSNs. Low energy node is used to sense the network while the high energy node do processing and sending of information. Some nodes

© 2015-19, IJARCS All Rights Reserved

are grouped together to form cluster and among them one node is made as a cluster head which is less energy constrained [45].This cluster head send information to destination on behalf of other nodes. Following protocols are used in hierarchical routing:
LEACH (Low Energy Adaptive Clustering Hierarchy)
PEGASIS (Power-Efficient Gathering in Sensor Information Systems)
TEEN (Threshold-sensitive Energy Efficient sensor Network)
APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network)
HPAR (Hierarchical Power-aware Routing)
VGA (Virtual Grid Architecture routing)
SOP (Self Organizing Protocol)

- **Data centric protocol:** These are based on the query concept and used to manage the redundancy of data. Redundancy exists due to lack of global identification number of node that defines them uniquely. The destination send query to particular region and based on query particular node reply back [46][47].
  Three types of messages are used to send information.
  ADV message: Promote new data.
  REQ message: Request desired data.
  DATA message: Actual data itself.
  Following are the protocol used:
  SPIN (Sensor Protocols for Information via Negotiation)
  COUGAR ()
  ACQUIRE (Active Query Forwarding in Sensor Networks)
  CADR (Constrained anisotropic diffusion routing)
  MCFA (Minimum Cost Forwarding Algorithm)
  IDSQ (Information-driven sensor querying)
  DD (Direct Diffusion)
  RR (Rumor Routing)

- **Location based Routing**: The nodes are identified on basis of their location in location based routing. The position of nodes is obtained through the radio signal, GPS signal etc [48]. The distance between the adjacent nodes is predicted on the base of arriving signal strength that helps to calculate the energy consumption among the nodes.
  Following are the protocol used:
  GAF (Geographic Adaptive Fidelity)
  GEAR (Geographic and Energy Aware Routing)
  MFR (Most Forward within Radius)
  GEDIR (The Geographic Distance Routing)
  GOAFR (The Greedy Other Adaptive Face Routing)

Based on participation fashion of the nodes, routing classified as Direct communication; Flat; and Clustering

- **Direct communication**: Any sensor node can send information directly to the base station in direct communication protocols. When this concept is applied to a very huge network, the sensor nodes' energy may be exhausted rapidly. Its scalability is very small. For example SPIN protocol.
- **Flat protocol**: In the case of flat protocols, if any sensor node wants to send data, it first has to search the valid route to the base station and then transmits the data. The nodes in the region of the base station may drain their energy speedily. Its scalability is average. For example Rumor Routing,
- **Clustering protocol**: In clustering protocol, the complete area is separated into numbers of clusters. Every cluster has a cluster head (CH) and these cluster heads directly communicates with the BS. All nodes in a cluster send their data to their corresponding CH.For Example: TEEN.

2. LITERATURE SURVEY:

Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh [10] describes the importance of security in WSN. Routing; QoS provisioning; energy efficiency; security; and multicasting are disputes in WSN. When working on any software/hardware, security required from the application should also be marked and sometimes some additional actions also are taken into account.

Zhen-wei Shen; Yi-hua Zhu, Xian-zhong Tian, Yi-ping Tang [11] proposed Energy Prediction and Ant Colony Optimization Routing (EPACOR). In that paper, ant colony systems are used to set up the path with optimal or sub-optimal power consumption when a node needs to deliver data to the sink. Meanwhile, learning mechanism is embedded to guess the energy consumption of neighboring nodes when the node chooses a neighboring node added to the route. They also compare EPACOR is with both MST (Minimal Spanning Tree)-based routing algorithm following the Prim algorithm and the Least Energy Tree (LET)-based routing algorithm following the Dijkstra algorithm. The result shows that the EPACOR has the best network lifetime among the three while keeping energy consumption in low level.

Feng Wang, Jiangchuan Liu [12] presented a investigation on the current advances in network sensor data collection. First, they highlight the special points of the sensor data collection by comparing it with both wired sensor data collection and other applications using WSNs. They divided the wireless sensor data collection into three main stages: the deployment stage; the control message dissemination stage; and the data delivery stage.

K.Syed Ali Fathima, Mr.K.Sindhanaiselvan [13] projected a innovative technique called Bio-Inspired mechanism for routing. The chief purpose is to keep the highest life span of network during data transmission. This paper presents the implementation of WSN and then compares its performance in terms of packet delivery ratio, energy level and throughput with AODV routing protocol based on ant colony algorithm.

B.Chandra Mohan, R. Baskaran [14] reviews various recent researches and implementation of ACO. After study, they proposed a modified ACO model for solving the network routing problem and then compared it with existing traditional routing algorithms.

Cherifa Boucetta, Hanen Idoudi, Leila Azouz Saidane [15] present a Power Aware Scheduling and Clustering algorithm based on Ant Colony Optimization (PASC-ACO). The ACO proposal can take a significant part in the enrichment of network lifetime by choosing the optimum path to arrive at the base station. The PASC-ACO algorithm runs for various

© 2015-19, IJARCS All Rights Reserved

network scenarios by simulation. The outcome shows that the proposed scheme is better than other existing techniques such as LEACH; M-GEAR and PASC. PASC-ACO accomplishes better performances in terms of lifetime by matching the energy load among all the nodes.

Dina S. Deif, Yasser Gadallah [16] discussed the design aspect of wireless senor network, planned deployment and random deployment which are the two deployment strategy of sensors. In this paper, they focused on planned deployment and proposed an algorithm using different mathematical approaches like Genetic Algorithms; Computational Geometry; Artificial Potential Fields; and Particle Swarm Optimization.

Ziqiang An [17] proposed center fusion method worked on the ant colony algorithm concept. It can significantly reduce the energy consumption of the wireless sensor network and prolong the lifecycle of WSN

F. Karray, M. W. Jmal and M. Abid, M. S. BenSaleh and A. M. Obeid [18] present a study to optimize the performances in particular real-time; low power; cost; and time to market in wireless sensor node architectures.

Kashif Saleem, Norsheila Fisal [19] proposed a fresh WSN routing protocol nameded as Secure Real-Time Load Distribution (SRTLD) that offer real time transfer; longer sensor node lifetime; and high delivery ratio. SRTLD is compared with LQER, MMSpeed, RTPC and RPAR. A narrative Biological inspired self-organized Secure Autonomous Routing Protocol (BIOSARP) develops to improve SRTLD with self-optimized and independent secure routing mechanism. The proposed BIOSARP is developed to minimize the overhead of broadcasting the packet in order to reduce the delay; packet loss; and power consumption in WSN.

Zalak Modi, Sunil jardosh, Prabhat Ranjan [20] proposed a Rumor routing that works on diverse types of traffic patterns. The simulation result shows the major reduction in energy consumption after applying the optimization over Rumor Routing algorithm named as Optimized Rumor Routing.

Zhenxing Luo, Paul S. Min [21] reviews the different methods of sensor selection. These methods are used for distributed detection; distributed estimation; and distributed tracking in wireless sensor networks.

Omar Abdulwahabe Mohamad, Rasha Talal Hameed, Nicolae Ţăpuş [22] makes a comparison between the Destination Sequenced Distance Vector and Ad hoc On Demand Distance Vector routing protocols based on performance. The result of protocols is comes out based on the criteria like delay time and data delivery ratios with routing overload parameters. Experimentally, it is observed that DSDV gives better performance as compare to AODV on other hand DSDV has smaller routing carry and delay time as compare to AODV.

Zhong Luo .et.al. [23] proposed an improved aco based security routing protocol for wireless sensor network. The result of experiments illustrate that the algorithm gives assurance that the cost is less in discovering the forwarding path with premise of ensuring security.

Wang Jiahao.et.al.[24] proposes a tracking cluster based mobile cluster distributed group rekeying protocol (MCDGR).They introduce a multi-path reinforcement scheme, q-composition scheme and one-way cryptographic hash function based random key pre distribution algorithm (RKP), which can guarantee a high accuracy and security and a low energy consumption on the same time in large-scale sensor networks.

Rajashree.V.Biradar,.et.al [25] considered the design issues of the sensor networks and then presents a comparison and classification of routing protocols. With the help of comparison one can design and evaluate new routing protocols for sensor networks by considering the evaluated features.

Ali Modirkhazeni, .et.al. [26] focus on secure- hierarchal routing protocols and characterize highlighted approaches for its security in wireless sensor networks . They developed a matrix that generalized the previous tasks and inspect the planned matrix. After that the suggested matrix of the protocols is applied on the proper application.

Jeril Kuriakose, .et.al. [27] done survey on the localization techniques that resolve the trouble of identify the current location of the node. Because GPS cannot update the location of indoor environment and doing it manually is very difficult for dense network.

Soumitra Das[28] provides a detailed review of nature inspired techniques applicable on existing energy optimization by taking only parameters that are related to energy efficiency as the central objective. She summarized the paper by presenting main disadvantages of various protocols that are used for energy efficient routing with respect to the nature inspired computing.

M. Dorigo, V. Maniezzo and A. Colorni [30] proposed a method of traditional travelling salesman problem that shows the system can quickly gives the good optimal solutions. They discuss the work flow of algorithm and also display all the essential simulation results. They also give some hints of how to apply this approach on variety of optimization problems.

Sridhar.S, Sharon priya.S[31] shows various optimization problems are proposed based on the idea of ACO technique and many others are also take advantage of it and are in processing stste.

Mohammed Abo-Zahhad, .et.al [32] done analysis on WSNs concept, definition and application ,WSNs constrains and judgment metrics, communication protocol stack for WSNs and provides analysis and comparisons of existing simulation programs .

Mohamed Watfa, .et.al. [33] aims to present a algorithm in the field of wireless sensor network security that make use of existing public-key algorithms by separating the network into clusters. The proposed algorithm provides data

© 2015-19, IJARCS All Rights Reserved

confidentiality; node authentication; and data integrity within the acceptable memory; time; and energy constraints. Chris Karlof, David Wagne [34] proposed a algorithm that applies security goals for routing in wireless sensor networks and illustrate how attacks alongside ad-hoc and peer-to-peer networks can be modified into dominant attacks against sensor networks.

AMALN. AL-KARAK, AHMEDE. KAMAL [35] present a survey of state of the art routing techniques in WSNs. Also highlight the advantages and performance issues of each routing tech-nique.

Thomas Stützle, Holger H. Hoos [36] present a *MAX–MIN* Ant System (*MM*AS) that vary from Ant System in a number of ways. MMAS is applied on Traveling Salesman Problem and the Quadratic Assignment Problem that shows that *MM*AS is currently best among various other algorithms that run on these problems.

TEODOR-GRIGORE LUPU[37] discuss the dispute in the security problem. They want to find a fine and balanced state between two of the most important necessities: the requirement of developing networks in order to maintain the rising business opportunities and work level; and the need to take care of classified; private and; strategic information.
Mehreen Shaikh, Abid. H Syed[38] present a brief survey of the types of jamming attacks, methods used to detect and defend the jammers.

3. ANT COLONY OPTIMIZATION

Swarm intelligence takes encouragement from the community behaviors of insects and from other animals. Comparatively, it is a novel approach for problem solving. In particular, ant's behavior concept is used by a number of methods and techniques. Among all, the most victorious and deliberated optimization technique is ant colony optimization (ACO). The foraging behavior of ant species inspired ACO. The ants set down a chemical stuff called pheromone on the ground. This substance marks a positive path that should be followed by other members of the ant colony. Ant colony optimization exploits a same mechanism for solving optimization problems [5].ACO algorithm is a part of the swarm intelligence scheme. This probabilistic technique finds a path near to optimal path through a problem space.Dorigo.M, Maniezzo.V and Colomi.A, Italian scholars use the foraging behavior of ant colony and apply simulation and results in a simulated evolutionary algorithm ACO Ant Colony Optimization based on population's. This technique finds the best solution through analyzing the development process of ant group that is collection of candidate solutions. There are various fields where this algorithm is applicable like combinatorial optimization; network routing; data mining; function optimization; and robot path planning etc with giving best results during last ten years. Good distributive; calculative mechanism; and strong robustness is the quality of this algorithm. ACO is easily merged with other methods and show nice performance on resolving the complex optimization problems. It is more appropriate for solving the optimization problems in composite environments. For that reason, it has an immense educational meaning and engineering value to construct theoretical analysis and valid study to ACO. ACO has been also useful in data analysis; solution of multi-robot coordination problems as well as in fields such as electric; communication; mining; chemical; water conservancy; architecture and traffic; etc [6].

3.1 Basic Idea of Ant Colony Algorithm:

By the cautious inspection and study, bionicists came to know the fact that ants will put down a chemical substance called pheromone on their path to look for foodstuff. More the ants crossed the same path; more substance will be left or collected on that path. This is done to accomplish two objectives (a) it helps the ants to locate their way back to the nest (b) it allows other more ants to recognize the path they have taken, so that the others can also track them. So, the probability will be bigger for the ants to pursue the identical path. This is the phenomenon by which ants will make communication possible to find their foodstuff at last. The more time the ant takes, to cover the distance from the nest to the foodstuff and come back to the nest, the pheromones have to disappear as the time is over; the pheromone evaporates and thus its quantity decreases. This process is circulated around both the positive and negative feedback. The positive feedback shows depositing of more pheromone catch the attention of other ants to follow the same path that leads to increase in quantity of pheromone and negative feedback shows the scattering of the pheromone by evaporation leads to decreasing the level of pheromone therefore disappointing the other ants to follow the same path [7]. Each ant will independently seek out for the solution and as it gets solution, leave some pheromone on that solution. As solution gets better more pheromones will leave by the ants on that solution. So, there will be a high probability of chosen of that solution which have more pheromones. At the initial stage, all solutions start with same amount of information. As we move on in the algorithm, the better solution contains more and more information and the algorithm steadily becomes convergent. Ant Colony Optimization [8] is constantly the underline of the algorithms. In ACO algorithm, there are many improvements are done like algorithm is a self-adaptive; rising the varieties of different groups; enhancing the local search by combining with both the global optimization algorithm and deterministic local optimization algorithm etc.

3.2. Ant Colony Optimization Algorithms: Basic Ant Colony Algorithm and Flowchart

Following is the pseudo-code of the ACO metaheuristic procedure:

```
procedure ACO-Metaheuristic
   Schedule the Activities
      Construct –Ants-Solutions
      Update-Pheromones
      Daemon-Actions                          //optional
  end-Schedule-Activities
end-procedure
```

ACO algorithm mainly contains the three procedures: Construct-Ants-Solutions; Update-Pheromones and Daemon-Actions.
Construct-Ants-Solutions: It directs the group of ants moving to the diverse neighbor nodes of the problem's

© 2015-19, IJARCS All Rights Reserved

construction graph. During the move, ants use both pheromone trail and the heuristic information to build the solution of the optimization problems. Once an ant has built the solution that will be used by the Update-Pheromones procedure to choose how much pheromone to deposit [52].

Update-Pheromones: Pheromone trails are modified in this process. The trail value of that path will increase on which the pheromone is leave by the ant otherwise pheromone evaporation donates to decrease the trail value. The additions of new pheromone increase the probability that the same path will be used by the other ants and those results in a good solution.

Daemon-Actions: The actions cannot be carried out by a single ant because they require access to nonlocal information—interact in the solution process [53].

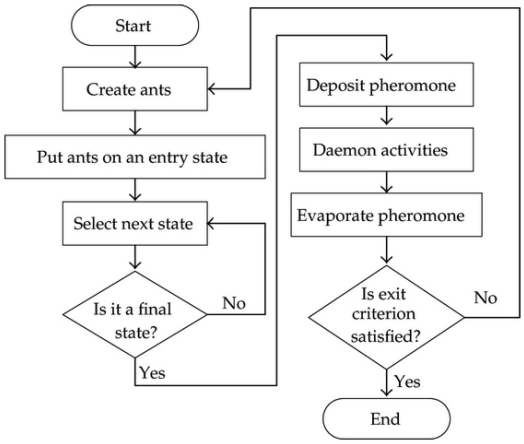

Fig 2. Flowchart of ACO

In this flowchart, initially ants are created and placed at their position(state).If ants does not reach their final state then they move further and choose the next state. If they reached the final state, then pheromone is updated and corresponding daemon actions are constructed. Next check the exit criteria, if it satisfied then exit otherwise again start from the first step, that is, ants are created. Although, ACO algorithm has a good quality in finding the global optimal solution [29] so has been widely applied in many fields. It still has some weakness mainly concluded in two points: (a) ACO algorithm takes a long time to search and most time is spend on solution construction when compared with other optimization algorithms. (b) The stagnation and local minimum problems may occur during the execution process of ACO algorithm.

Improvement of ACO Algorithm:

- Ant System: The key uniqueness is positive feedback; distributed computation; and the use of a constructive greedy heuristic. The positive feedback accounts for rapid discovery of good solutions; distributed computation evades premature convergence; and the greedy heuristic helps in finding the suitable solutions in the early stages of the search process.

- Elitist AS: Each time after finished one circle of travelling, select the some best solutions (paths), repair the pheromone of the corresponding path to make sure that the solutions remained each time will have a superior quality. That will improve the operational speed but may cause local minimum problem because the intensity of pheromone on some paths have relative high which makes ants gathering on these paths.

- Ant Colony System: ACS is the improved side of ACO algorithm. Its main variation from the ACO is that when selecting the next city, ACS makes more use of the current better solutions and only adds the pheromone at the subordinate side of global best solution. Every time when the ant moves from City i to City j, the pheromone on (i, j) will properly decreases.

- MMAS: The MAX–MIN Ant System (MMAS) algorithm allows only the greatest solution to add pheromone during the pheromone trail update. MMAS can simply be extended by adding local search algorithms. MMAS is the best performing ACO algorithms for many different combinatorial optimization problems like TSP and the Quadratic Assignment Problem (QAP) to improve the solutions generated by the ants with local search algorithms [36].
- Rank Based AS: Ant System uses different sensitive ants to the pheromone trail to keep the variety of obtained solutions. Some ants select a path in the standard way among existing paths, which means that they tend to select a path with a large amount of pheromone trail, some ants tend to select a path with a small amount of pheromone trail & others select a path at random. This method selects solutions for the ranking list, not only to the tour length but also to the difference between each solution and the iteration-best one at each iteration.

4. SIMULATORS IN WSN

WSNs contain large number of sensor nodes that are used to observe, study phenomenon and giving the information of places where it is impossible to reach. It is not easy to build a model analytically with good accuracy, so simulation is important to learn WSN. It requires a suitable model based on accurate assumptions. Simulation provides accurate environmental settings for manipulating and improving the design factors.

- **MATLAB:**
  MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and fourth-generation programming language. A proprietary programming language developed by MathWorks, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, Fortran and Python.

- **ns-2 and ns-3 :**
  ns stand for network simulator. It is a name given to the series of discrete event network simulators. These discrete-event computer network simulators are mainly used in research and teaching. A network simulator is software that calculates the behavior of a computer network. Since the traditional analytical method becomes too complex to provide an accurate understanding of system behavior network because of that simulator are

© 2015-19, IJARCS All Rights Reserved

used. The computer network in simulators is modeled with devices; links; applications etc. and the performance is analyzed. Simulators typically come with support for the most popular technologies and networks in use today. ns-3 are free software for research and development. The objective of the ns-3 project is to create an open simulation environment for computer networking research that will be preferred inside the research community. It should be aligned with the simulation needs of modern networking research. It should encourage community contribution; peer review; and validation of the software.

- **OMNeT++**
  It has the properties like extensibility, modularity, component-based C++ simulation library and framework. It primarily used for building network simulators. The Network in this case includes wired and wireless communication networks; on-chip networks; queuing networks; OMNeT++ provides component architecture for models. Components are programmed in C++ and then integrated into larger components and models using a high-level language (NED). OMNeT++ is both a simulator and a simulation framework. It is released with full source code. It is free to use; modify and distribute in academic and educational institutions.

- **QualNet**
  The QualNet communications simulation platform is a planning; testing and training tool that copies the activities of a real communications network. Simulation is a cost-effective method for developing; deploying and managing network-centric systems throughout their entire lifecycle. The users can estimate the basic behavior of a network, and test combinations of network features that are likely to work. QualNet provides a comprehensive environment for designing protocols; creating and animating network scenarios; and analyzing their performance.
  QualNet allows users to:
- Design the new protocol models.
- Optimize the new and existing models.
- Design the large wired and wireless networks using pre-configured or user-designed models.
- Analyze the performance of thenetworks and perform what-if analysis to optimize them.

5. CONCLUSION & FUTURE WORK

Today, WSNs are a famous research topic and progressively more improved technique. It monitors industrial phenomenon and ecological over the last two decades. In the same way ACO is also including in recent researches.ACO is the one of the best method for solving optimization problem. It has many advantages [31] like when the graph changes dynamically, the value of ant colony algorithm can be run constantly and adjusts to change in real time over simulated annealing and genetic algorithm approaches of similar problems**.** Algorithms found good solutions on small problems. Ant Colony Optimization algorithm has applicable on a wide range of applications & efficient for Traveling Salesman Problem and similar problem. Positive Feedback accounts for rapid discovery of good solutions. In this paper, we explain the basic of wireless sensor network, architecture of sensor node, communication protocol, characteristic, challenges, application, security issues and attacks in WSN, routing protocol, basic of ACO and its algorithms. Various algorithms are proposed to get the optimal solution of the problem.ACO algorithms are used to propose these algorithms to improve the a WSN challenges .Different algorithms used different parameter like pheromone function, performance metric, simulator etc. to get the optimal solution. The algorithms EPACOR launch the route with optimal power consumption. Modified ACO model compared with existing traditional routing algorithms which are applied for network routing problem. PASC-ACO results better performance in the terms of life span by balancing the energy load among all the nodes. BIOSARP provide better decline in energy spending after applying our optimization over Rumor Routing algorithm than SRTLD. Different algorithms are enhanced and proposed to find the better solution. The already done work performs better in this area still need a more improved solution of the problems. In our future work, we trying to proposed the algorithm that spend less energy ,better routing path and having good security measures with the help ACO algorithms and its variants, different tools etc. that can help the future researchers to accomplished their task or research.

6. REFERENCES

[1] Waltenegus-Dargie,Christian Poellabauer," Fundamentals of Wireless Sensor Networks", Wiley Series on Wireless Communications and Mobile Computing.

[2] Monika Bhalla ,Nitin Pandey, Brijesh Kumar," Security Protocols for Wireless Sensor Networks",2015 International Conference on Green Computing and Internet of Things (ICGCloT)

[3] Aashima singla , Ritika sachdeva , " Review on security issues and attacks in Wireless sensor networks", IJARCSSE, vol. 3, iss. 4, 2013.

[4] Himani Chawla," Some issues and challenges of Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering,July 2014, Volume:04,ISSN: 2277 128X

[5] Marco Dorigo, Mauro Birattari, and Thomas St¨utzle," IEEE COMPUTATIONAL INTELLIGENCE MAGAZINE | NOVEMBER 2006, ISSN:1556-603X/06

[6] Stephen A. Adubi, Sanjay Misra," A Comparative Study on the Ant Colony Optimization Algorithms", 2014 IEEE

[7] XUE Xue-dong ,CHENG Xu-de , XU bing, WANG Hong-li,JIANG Cheng-peng," The basic principle and application of Ant colony optimization algorithm", 2010 IEEE

[8] Ying Pei, Wenbo Wang, Song Zhang," Basic Ant Colony Optimization", International Conference on Computer Science and Electronics Engineering,2012

[9] Colorni A ,Dorigo M and Maniezzo V. Distributed optimization by ant colonies[A] . In : Proc . of 1st European Conf . Artificial Life [C] .Pans , France :Elsevier , 1991 ,134 – 142

[10] Hero Modares , Rosli Salleh, Amirhossein Moravejosharieh," Overview of Security Issues in Wireless Sensor Networks", Third International Conference on Computational Intelligence, Modelling & Simulation 2011

[11] Zhen-wei Shen; Yi-hua Zhu, Xian-zhong Tian, Yi-ping Tang," An Ant Colony System Based Energy Prediction Routing Algorithms for Wireless Sensor Networks",IEEE 2008

[12] Feng Wang, Jiangchuan Liu,"N etworked Wireless Sensor Data Collection:Issues, Challenges, and Approaches, IEEE

© 2015-19, IJARCS All Rights Reserved

COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011

[13] K.Syed Ali Fathima, Mr.K.Sindhanaiselvan," Ant Colony Optimization Based Routing in Wireless Sensor Networks", Int. J. Advanced Networking and Applications 2013**,** Volume: 04 Issue: 04 Pages:1686-1689

[14] B. Chandra Mohan , R. Baskaran ," A survey: Ant Colony Optimization based recent research and implementation on several engineering domain", Expert Systems with Applications 39 (2012) 4618–4627

[15] Cherifa Boucetta, Hanen Idoudi, Leila Azouz Saidane ," Ant Colony Optimization Based Hierarchical Data Dissemination in WSN",IEEE 2015

[16] Dina S. Deif, Yasser Gadallah," Classification of Wireless Sensor Networks Deployment Techniques ", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION 2013.

[17] Ziqiang An,"Center Fusion Algorithm in wireless sensor Networks Based on Ant Colony Algorithm", International Conference on Computer Science and Service System 2012

[18] F. Karray, M. W. Jmal and M. Abid , M. S. BenSaleh and A. M. Obeid[18]," Review on Wireless Sensor Node Architectures ",IEEE 2014

[19] Kashif Saleem, Norsheila Fisal," Enhanced Ant Colony Algorithm for Self-Optimized Data Assured Routing in Wireless Sensor Networks",IEEE 2012

[20] Zalak Modi, Sunil jardosh, Prabhat Ranjan," Optimized Rumor Routing Algorithm for Wireless Sensor Networks"

[21] Zhenxing Luo, Paul S. Min," Survey of Sensor Selection Methods in Wireless Sensor Networks ", IEEE 2013

[22] Omar Abdulwahabe Mohamad, Rasha Talal Hameed, Nicolae Ţăpuş," Smart Home Security Based on Optimal Wireless Sensor Network Routing Protocols", International Conference,25-27|June 2015, 7th Edition

[23] Zhong Luo,Runze Wan, Xiaoping Si," An Improved ACO-based Security Routing Protocol for Wireless Sensor Networks" International Conference on Computer Sciences and Applications 2013.

[24] Wang Jiahao, Qin Zhiguang, Geng Ji1 & Wang Shengkun," RKP based secure tracking in wireless sensor networks", Journal of Systems Engineering and Electronics, Vol. 19, No. 1, 2008, pp.175–183

[25] Rajashree.V.Biradar ,V.C .Patil , Dr. S. R. Sawant , Dr. R. R. Mudholkar," CLASSIFICATION AND COMPARISON OF ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS", Special Issue on Ubiquitous Computing Security Systems Journal – Volume 4

[26] Ali Modirkhazeni, Norafida Ithnin, Mohammadjavad Abbasi," Secure Hierarchal Routing Protocols in Wireless Sensor Networks; Security Survey Analysis", IJCCN International Journal of Computer Communications and Networks, Volume 2, Issue 1, February 2012

[27] Jeril Kuriakose, Sandeep Joshi, R. Vikram Raju, and Aravind Kilaru," A Review on Localization in Wireless Sensor Networks", Advances in Signal Processing and Intelligent Recognition Systems, Advances in Intelligent Systems and Computing ,Springer International Publishing Switzerland 2014

[28] Soumitra Das," A SURVEY OF NATURE INSPIRED COMPUTING FOR ENERGY OPTIMIZATION IN WIRELESS SENSOR NETWORK", Int.J.Computer Technology & Applications,Vol 6 (6),931-942, ISSN:2229-6093

[29] Marco Dorigo and Thomas St¨utzle," Ant Colony Optimization: Overview and Recent Advances", May 2009

[30] M. Dorigo, V. Maniezzo, and A. Colorni. The Ant System: An autocatalytic optimizing process.Technical Report 91-016 Revised, Dipartimento di Elettronica, Politecnico di ilano,Italy, 1991.

[31] Sridhar.S, Sharon priya.S," Comparative Study of Ant Colony Optimization And Gang Scheduling", INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY, 2| FEBRUARY 2015 ,VOLUME: 3, ISSUE :2,ISSN: 2349 – 9303

[32] Mohammed Abo-Zahhad, Osama Amin, Mohammed Farrag and Abdelhay Ali," A Survey on Protocols, Platforms and Simulation Tools for Wireless Sensor Networks",International Journal of Energy, Information and Communications Vol.5, Issue 6(2014), pp.17-34.

[33] Mohamed Watfa, Marwa El-Ghali, and Hiba Halabi," A Scalable Security Protocol for Wireless Sensor Networks ", University of Wollongong Research Online,2008

[34] Chris Karlof, David Wagne,"Secure Routing inWireless Sensor Networks: Attacks and Countermeasures".

[35] AMALN. AL-KARAK, AHMEDE. KAMAL," ROUTING TECHNIQUES IN WIRELESS SENSOR NETWORKS: A SURVEY",IEEE,December 2004

[36] Thomas Stützle, Holger H. Hoos," MAX–MIN Ant System",ELSEVIER, Future Generation Computer Systems 16 (2000) 889–914

[37] TEODOR-GRIGORE LUPU," Main Types of Attacks in Wireless Sensor Networks ", Recent Advances in Signals and Systems, ISSN: 1790-5109, ISBN: 978-960-474-114-4

[38] Mehreen Shaikh, Abid. H Syed," A SURVEY ON JAMMING ATTACKS, DETECTION AND DEFENDING STRATEGIES IN WIRELESS SENSOR NETWORKS", IJRET: International Journal of Research in Engineering and Technology,eISSN: 2319-1163 | pISSN: 2321-7308

[39] Kazem Sohraby, Daniel Minoli and Taieb Znati , "Wireless Sensor Networks Technology Protocols and Application", Wiley-InterScience 2007, ISBN 978-0-471-74300-2.

[40] SANJEEV KUMAR GUPTA, POONAM SINHA," Overview of Wireless Sensor Network: A Survey", International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 3, Issue 1, January 2014

[41] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal," Wireless sensor network survey",ELSEVIER, Computer Networks 52 (2008) 2292–2330

[42] Keshav Kaushik," SURVEY ON RESPONSIBILITIES OF DIFFERENT OSI LAYERS IN WIRELESS SENSOR NETWORKS", International Journal of Advanced Technology in Engineering and Science Vol. No. 3,Issue 11,NOVEMBER 2015.

[43] Kamalde ep Kaur , Parneet Kaur," Wireless Sensor Network: Architecture, Design Issues and Applications ", International Journal of Scientific Engineering and Research (IJSER), ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014

[44] Shuang-Hua Yang," Wireless Sensor Networks: Principles, Design and Applications",Springer.

[45] Shamsad Parvin, Muhammad Sajjadur Rahim," Routing Protocols for Wireless Sensor Networks: A Comparative Study",International Conference on Electronics, Computer and Communication (ICECC 2008)

[46] Geetika Dhand,Dr.S.S.Tyagi," Survey on Data Centric protocols of WSN", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol ume 2, Issue 2, February 2013 , ISSN 2319 -4847

[47] P.Krishnaveni, Dr.J.Sutha," Analysis of routing protocols for wireless sensor networks", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 11,November 2012, (ISSN 2250-2459)

[48] Kemal Akkaya , Mohamed Younis," A Survey on Routing Protocols for Wireless Sensor Networks".

[49] Manal Abdullah,Aisha Ehsan," Routing Protocols for Wireless Sensor Networks: Classifications and Challenges", Journal of Electronics and Communication Engineering

© 2015-19, IJARCS All Rights Reserved

Research,Volume 2~ Issue 2(2014) p: 05-15 , ISSN(Online) : 2321-5941.

[50] Surendra H. Raut, Hemant P. Ambulgekar," Proactive and Reactive Routing Protocols in Multihop Mobile Adhoc Network" ,International Journal of Advanced Research in Computer Science and Software Engineering , IJARCSSE ,Volume 3, Issue 4, April 2013, ISSN: 2277 128X

[51] Muhammad R Ahmed ,Xu Huang, Dharmandra Sharma and Hongyan Cui,"Wireless Sensor Network: Characteristic and Architectures"

[52] Denis Darquennes," Implementation and Applications of Ant Colony Algorithms", Facultes Universitaires Notre-Dame de la Paix, Namur ,Institut d'Informatique Annee academique 2004-2005

[53] Marco Dorigo and Thomas Stutzle ,"Ant Colony Optimization", Massachusetts Institute of Technology 2004.

© 2015-19, IJARCS All Rights Reserved