International Journal of Smart Home
Vol. 11, No. 1 (2017), pp. 17-40
http://dx.doi.org/10.14257/ijsh/2017.11.1.02

A Comprehensive Study on Ant Colony Optimization Technique with Special Reference to Wireless Sensor Network for Smart Home

Ruby Bhatt[1] and Piyush Kumar Shukla[2*]

[1]*Assistant Professor, Choithram College of Professional Studies, Indore*
[2]*Assistant Professor, Department of CSE, UIT, Bhopal 462023, India*
E-Mail: ruby_15@rediffmail.com
E-Mail: pphdwss@gmail.com[*]

Abstract

Wireless Sensor Networks consists of smaller nodes. These have limited power and when deployed gathers useful information. In WSNs, it is critical to collect the information in an efficient manner. Routing in Wireless Sensor Network is also a tough job. In order to avoid the problem Bio-Inspired mechanism for routing, Ant Colony Optimization (ACO) can be utilized. ACO is a dynamic and reliable protocol. It provides energy-aware, data gathering routing structure in wireless sensor network. It can avoid network congestion and fast consumption of energy of individual node. Then it can prolong the life cycle of the whole network. ACO algorithm reduces the energy consumption. It optimizes the routing paths, providing an effective multi-path data transmission to obtain reliable communications in the case of node faults. The main goal of this comprehensive study is to provide newer researchers with utmost information and to let them know how to maintain the maximum lifetime of network, during data transmission in a efficient manner.

Keywords: *Ant Colony Optimization, Bio-Inspired Routing, Energy efficiency, Wireless sensor networks, Adaptive Harmonic Optimization*

1. Introduction

Today it is quite obvious that technology [42] has changed humanity. Contemporary period is the time of Wireless Technology [42] and Wireless Network [41]. Now a days, it is very popular because of its benefits and futuristic applications [43] in many fields, such as health monitoring [43], environmental control, military, industries. Wireless sensor networks (WSN) [41] consist of many low-power, low-cost, and small-size sensor nodes. These nodes consist of three main components-sensing, data processing and communication [41]. The sensing technology blended with processing power and wireless communication makes it lucrative for being exploited in abundance in future.

Basic feature of this technology [42] includes: A few or large number of nodes having asymmetric flow of information, from sensor nodes to a command node. Communication is triggered by events. At each node there is a limited amount of energy [40]. It uses broadcast communications [40] instead of point-to-point. Nodes do not have a global ID such as an IP number. The network architecture depends on the application deploying WSN. For example, some nodes are connected directly to the sink without passing through other nodes. Other layers might go through other nodes to forward the data [41] to the sink.

[*] Corresponding Author

ISSN: 1975-4094 IJSH

Designing phase of Wireless Sensor Network faces many challenges, some of them regarding power consumption which must be kept as minimum as possible to extend the life of the network[41] and others, taking into consideration the hardware and software constraints[40] such as sensors, location finding system, antenna, power amplifier, modulation *etc*.

There are many advantages of wireless sensor networking [41], like, they can store a limited source of energy, they have no hassle of cables and have mobility, it can work efficiently under the harsh conditions, and it has deployment up to large scale *etc*. The other side of coin says, it also has some disadvantages which really take the moral of this technology down, such as, they have very insufficient speed of communication [41], it is to disturb the propagation of waves and it is too costly to use.

Sensor networks are a powerful combination of distributed sensing [40], computing and communication. Therefore, three major application areas for wireless sensor networks are military surveillance, home health care or assisted living and environmental science [44]. They also have countless applications in medicine, transportation, agriculture, industrial process control, and the military as well as creating new revolutionary systems[40] in areas such as global-scale environmental monitoring, precision agriculture, home and assisted living medical care, smart buildings and cities, and numerous future military applications[43]. The distinguishing traits of sensor networks have a direct impact on the hardware design of the nodes at at-least four levels: power source, processor, communication hardware, and sensors.

1.1. Background

Sensor devices, or wireless nodes (WNs) [41], are also called motes. Sensors are internetworked via a series of multihop short-distance low-power wireless links particularly within a defined sensor field; they utilize either Internet or some other network for long-haul delivery of information to a point (or points) of final data aggregation and analysis. In general, within the sensor field, WSNs employ contention-oriented random-access channel sharing and transmission techniques. Other channel management techniques are also available. Sensors are typically deployed in a high-density manner and in large quantities. WSNs have unique characteristics, power constraints and limited battery life for the WNs, redundant data acquisition, low duty cycle, and, many-to-one flows. Therefore, new design methodologies are needed including, information, transport, network and operational management, confidentiality, integrity, availability, and, in-network/local processing. In some cases it is challenging to collect or extract data from WNs because connectivity to and from the WNs may be inter-mitten due to a low-battery status *e.g.*, if these are dependent on sunlight to recharge or other WN malfunction. Furthermore, a lightweight protocol stack is desired.

Sensors can be simple point elements or can be multipoint detection arrays. Typically, nodes are equipped with one or more application-specific sensors and with on-node signal processing capabilities for extraction and manipulation or preprocessing of physical environment information. Embedded network sensing refers to the synergistic incorporation of micro sensors in structures or environments; embedded sensing enables spatially and temporally dense monitoring of the system under consideration *e.g.*, an environment, a building, a battlefield. Sensors may be passive and be self-powered; farther down the power-consumption chain, some sensors may require relatively low power from a battery or line feed. At the high end of the power-consumption chain, some sensors may require very high power feeds *e.g.*, for radars.

Sensor networks deal with space and time: location, coverage, and data synchronization. Data is of greatest significance in sensor network. There is large amount of time-stamped time-dependent data. Therefore, sensor networks often support in-network computation. Architectures used by sensor networks are (1) Source-node

processing; or (2) Hierarchical processing. Instead of sending the raw data to the nodes responsible for the data fusion, nodes often use their processing abilities locally to carry out basic computations, and then transmit only a subset of the data and/or partially processed data. In a hierarchical processing architecture, processing occurs at consecutive tiers until the information about vents of interest reaches the appropriate decision-making and/or administrative point.

1.1.1. Technologies used by WSN

WSNs can use a number of wireless COTS technologies, such as Bluetooth, Infrared, Lasers for LAN Environment and ZigBee, Radio Signals, Microwave, WiMax and 3G for Wide Area Environment.

1.1.2 Security Concern in WSN

Wireless Sensor networks are prone to security attacks. Broadcast nature of the transmission medium makes it vulnerable to attacks. Security concerns [46] deal with [1]:

1. Attacks on secrecy and authentication. 2. Silent attacks on service integrity.

3. Attacks on network availability. The following security concerns to be taken care are:

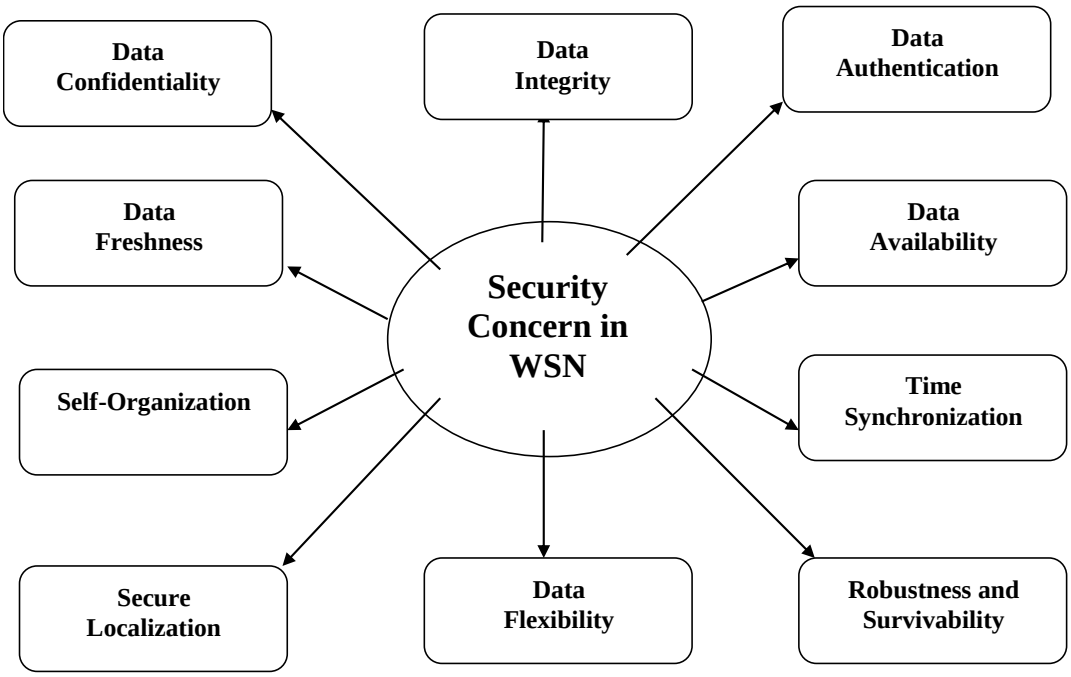

Figure 1. Security Concerns in WSN

1.1.3. Various Attacks in Wireless Sensor Networks

Wireless communication is broadcast by nature. A common radio signal is easy to jam or intercept. An attacker could overhear or disrupt the service of a wireless network physically. Attacks [45] can be classified on following basis:

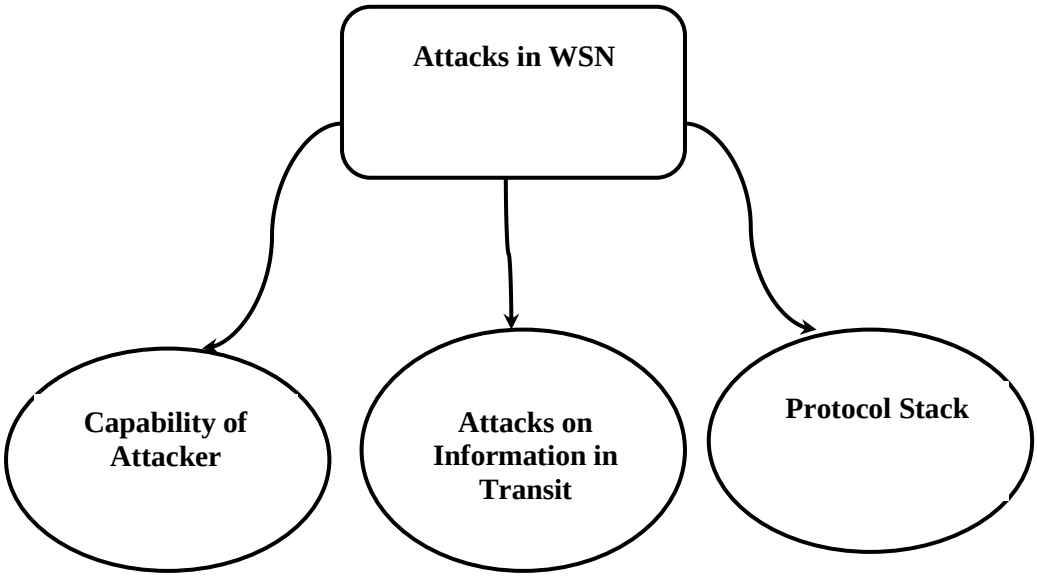

Figure 2. Attacks in WSN

Table 1. Based on Capability of Attacks, it is further classified as

S. No.	Name of Attack
1.	Active and Passive Attack
2.	Outside and Inside Attack
3.	Mote-Class and Laptop-Class Attack

Table 2. Based on Attacks on Information in Transit, it is further classified as

S. No.	Name of Attack
1.	Interception
2.	Interruption
3.	Modification
4.	Fabrication

Table 3. Based on Protocol Stack, it is further classified as

S. No.	Name of Layer	Name of Attack
1.	Physical Layer Attacks	Eavesdropping
		Device Tempering
		Jamming
2.	Data Link Layer	Traffic Manipulation
		Identity Spoofing (Sybil Attack)
3.	Network Layer	**Node Capture Attack**
		Fake Routing
		Black Hole
		Sink Hole
4.	Transport Layer	Flooding
		De-Synchronization
5.	Application Layer	Denial of Service (DoS)

		Selective Message Forwarding
		Data aggregation Distortion

Elaborate description of major attacks in wireless sensor networks:

(1) Node Capture Attack: In Node Capture Attack [28], an attacker physically captures sensor nodes and compromises them so that sensor readings sensed by compromised nodes are inaccurate or manipulated. The attacker may also attempt to extract essential cryptographic keys like a group key from wireless nodes that are used to protect communications in most wireless networks. Node capture not only enables to get a hold of cryptographic keys and protocol states, but also to clone and redeploy malicious nodes in the network.

Node capture attacks [34] result from the combination of passive, active, and physical attacks by an intelligent adversary. In order to initialize or set up an attack, the adversary will collect information about the WSN by eavesdropping on message exchanges, either local to a single adversarial device or throughout the network with the aid of a number of adversarial devices deployed throughout the network. Even if message payloads are encrypted, the adversary can extract information about the network operation and state, effectively learning about the network structure and function. In addition to passive learning, the adversary can actively participate in network protocols, probing the network for information and maliciously injecting information into the network. Once a sufficient amount of passive and active learning has taken place, the adversary can physically capture nodes. The gathered information can be used to help the adversary make an informed decision of which sensor nodes to capture in order to optimize the performance of the attack with respect to a specific attack goal. To serve as a basis for attack optimization and in order to measure the performance of an on-going attack, the adversary must develop an attack performance metric for the specified attack goal. In addition to the evaluation metric, the adversary must also be able to associate a value with each potential node capture in order to optimize the impact of the attack. Because of the purpose of the node value metric, it will be intimately related to the attack performance metric. A notable difference between the performance metric and the node value metric, however, is that the adversary may incorporate the heterogeneity of the WSN nodes by normalizing the node value with respect to the associated attack cost.

(2) Denial of Service: Denial of Service, (DoS) [19] is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

(3) Attacks on Information in transit: In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping,

any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks. As sensor nodes typically have short range of transmission and scarce resource, an attacker with high processing power and larger communication range could attack several sensors at the same time to modify the actual information during transmission.

(4) Sybil Attack: In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack [45]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols. Detection of sybil nodes in a network is not so easy.

(5) Blackhole /Sinkhole Attack: In this attack [45], a malicious node acts as a blackhole to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations.

(6) Hello Flood Attack: Hello Flood Attack [45] uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

(7) Wormhole Attack: Wormhole attack [45] is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information.

2. Brief Review of Work Already Done in the Field (Literature Review)

Various security schemes are proposed and implemented so far for wireless sensor networks, which are summarized as follows:

JAM [1] presented a mapping protocol which detects a jammed region in the sensor network and helps to avoid the faulty region to continue routing within the network, thus handles DoS attacks caused by jamming.

In [2] the authors showed that wormholes could effectively be used as a reactive defense mechanism for preventing jamming DoS attacks that were considered harmful for WSN.

Ye *et. al.*, [3] presented a statistical en-route filtering (SEF) mechanism to detect injected false data in sensor network and focused mainly on how to filter false data

using collective secret and thus preventing any single compromised node from breaking the entire system.

Newsome *et. al.,* [4] proposed some defense mechanisms against sybil attack in sensor networks.

[5] Presented a probabilistic secret sharing protocol to defend Hello flood attacks. The scheme used a bidirectional verification technique and also introduced multi-path, multi-base station routing when bidirectional verification was not sufficient to defend the attack.

[6] Proposed separate security schemes for data with various sensitivity levels and a location-based scheme for wireless sensor networks that protected the rest of the network, even when parts of the network were compromised.

[7] Implemented symmetric key cryptographic algorithms with delayed key disclosure on motes to establish secure communication channels between a base station and sensors within its range.

[8], [9] and [10] proposed key pre-distribution schemes, which targeted to improve the resilience of the network.

[11] Proposed key pre-distribution schemes for key-management scheme in distributed sensor networks that enhanced the efficiency of the network.

[12] proposed REWARD. This was a routing algorithm which fought against blackholes in the network.

TinySec [13] proposed a link layer security mechanism for sensor networks that used an efficient symmetric key encryption protocol.

Perrig *et. al.,* [14] proposed that SNEP & μTESLA [14] were two secure building blocks for providing data confidentiality, data freshness and broadcast authentication in their paper, SPINS: Security Protocols for Sensor Networks.

Chi Lin and Guowei Wu [15] in their paper, "Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach", explained that in the node capture attack, the adversary intelligently captures nodes and extracts the cryptographic keys from their memories to destroy the security, reliability and confidentiality of the wireless sensor networks. However, it suffers from low attacking efficiency and high resource expenditure. For the same, they developed a matrix-based method to model the process of the node capture attack. Matrix indicated the compromising relationship between the nodes and the paths. Matrix-based node capture attack Algorithm (MA in short) was proposed which could maximize the destructiveness while consuming the minimum resource expenditure. Experiments were conducted to show the performance of MA. Experimental results manifest that MA could reduce the attacking round, shorten the execution time, enhance the attacking efficiency and conserve the energy cost. For designing Matrix-based node capture attack Algorithm, the approaches of modeling the node capture attack was reviewed from the following: UML methods, probability analysis, system theoretic approach, epidemic theory, and vulnerability analysis.

Qiang Liu, *et. al.,* [23] in the paper, "FADE: Forwarding Assessment Based Detection of Collaborative Grey Hole Attacks in WMNs",. In this paper, they focused on a special type of denial-of-service attack, called selective forwarding or grey hole attack. When this attack is launched at the gateways of a WMN where data tend to aggregate, it could lead to severe damages due to loss of sensitive data. According to them, most of the existing proposals that focus on detecting stand-alone attackers via channel overhearing were ineffective against collusive attackers. They proposed a forwarding assessment based detection (FADE) scheme to mitigate collaborative grey hole attacks. Specifically, FADE detects sophisticated attacks by means of forwarding assessments aided by two-hop acknowledgement monitoring. They analyzed the optimal detection threshold that minimizes the sum of false positive rate and false negative rate of FADE, considering the network dynamics due to degraded channel quality or medium access collisions.

Extensive simulation results were presented to demonstrate the adaptability of FADE to network dynamics and its effectiveness in detecting collaborative grey hole attacks.

Bin Cao [24], in his paper, "Cooperative Media Access Control with Optimal Relay Selection in Error-Prone Wireless Networks", stated that cooperative communications could be regarded as one of the promising techniques to improve throughput and coverage performance in wireless communications. The relay node (RN) plays a key role in cooperative communications, and RN selection may affect the performance gain in a network with cooperative media access control (MAC). He addressed the issue of RN selection while taking into account MAC overhead, which was incurred by not only handshake signaling but frame retransmissions due to transmission failure as well. He designed a cooperative MAC mechanism with optimal RN selection algorithm, which is called optimal relay selection MAC, and used a theoretical model to analyze the cooperation performance gains. He conducted simulation experiments based on Network Simulator to evaluate Cooperative MAC. Numerical results validate the effectiveness of analytical model.

Bhavana Butani *et al.,* [36] in the paper, "An Exhaustive Survey on Physical Node Capture Attack in WSN, surveyed and concluded a tabular depiction of different approaches for modeling of node capture attacks in WSN.

Table 4. Different Approaches for Modeling of Node Capture Attack in WSN [36]

Authors	**Tague et al. [30]**	**Tague et al.[31]**	**De P et al. [32]**	**Bonaci et al.[33]**	**Mishra et al.[34]**	**Wu G et al.[35]**	**Chi Lin et al. [15]**
Proposed Works	Modeling of Node Capture Attacks Using Different Greedy heuristics in multi-Hop Wireless networks.	Modeling of Node Capture Attacks using GNAVE algorithm.	Modeling of Node Compromise that captures the unique topological characteristics of deployed wireless sensor network using Pair-wise key schemes.	Study of Physical Node Capture using a Control Theory Framework.	Model of Information gathering process by an attacker For Node Capture Attack.	Modeling of node capture attack algorithm based on route minimum key set (GNRMK).	Modeling of Node Capture attack algorithm using a matrix approach.
Approach	Vulnerability evaluation approach	Vulnerability evaluation approach	Epidemic Theory	Probabilistic analysis (System theoretic model)	Probabilistic analysis	Vulnerability evaluation approach	Vulnerability Evaluation Approach
Centralized/ Distributed	Distributed Attack	Distributed Attack	Centralized Attack	Distributed Attack	Distributed Attack	Distributed Attack	Distributed Attack

Piyush Kumar Shukla *et. al.,* [29] in the paper, "Finding Robust Assailant Using Optimization Functions(FiRAO-PG) in Wireless Sensor Network", proposed an empirically designed multiple objective node capture attack algorithm based on optimizing functions as an effective solution against attacking efficiency of node capture attack. The objectives of this algorithm included: maximum node participation, maximum key participation and minimum resource expenditure.

Table 5. Tabulation of Base & Concerned Papers on Node Capture Attack in WSN

	Authors Name and Important Points of their Research Paper			
Features	**Chi Lin et al. [15]**	**Ozgur Koray Sahingoz [37]**	**Rehman Saif et al. [38]**	**Piyush Shukla et al. [29]**
Used Technique	Modeling of Node Capture attack algorithm using a matrix approach.	Multi-level dynamic key management scheme	Post deployment encryption key generation for fully connected secure WSN.	Empirically designed multiple objectives node capture attack algorithm
Security	Medium level of security as it restricted random key pre distribution protocol.	Low level security for sensed data and High level security for sensitive data.	High level of security due to high variance in encryption keys.	Considerable Secure System
Efficiency / Reliability	Efficient and Reliable as it could enhance the attacking efficiency.	Efficient and Reliable	Efficient and Reliable due to use of public key encryption.	FiRAO-PG provided higher attacking efficiency.
Accuracy	Medium Accuracy	Medium Accuracy	Medium Accuracy	Good Accuracy
Speed	High Speed as it could reduce the attacking round and shorten the execution time.	Good Speed	Considerable Processing Speed.	High Speed
Application Area	Monitoring and surveillance applications, Military & Health Care	Transportation, Energy, Military, Manufacturing & Health Care.	For detecting illegal activities, Law Enforcement and used in extreme weather conditions.	Military surveillance and environment monitoring

3. Optimization Techniques and Functions with Respect to Wireless Sensor Network

Optimization problems [27] relating to wireless sensor network deals with planning, design, deployment and operation. It gives rise to multi-objective optimization formulations where multiple desirable objectives compete with each other and the decision maker has to select one of the tradeoff solutions. These multiple objectives may or may not conflict with each other. Keeping the nature of the application in view, the sensing scenario and input/output of the problem, the type of optimization problem change.

Optimization techniques are needed at different design levels [26] (*e.g.*, sensor node hardware and software, data link layer, routing, operating system (OS), *etc*.) in order to assist designers in meeting application requirements. WSN optimization techniques can be generally categorized as static or dynamic. Static optimizations optimize a WSN at deployment time and remain fixed for the WSN's lifetime. Whereas static optimizations are suitable for stable/predictable applications, static optimizations are inflexible and do not adapt to changing application requirements and environmental stimuli. Dynamic optimizations provide more flexibility by continuously optimizing a WSN/sensor node during runtime, providing better adaptation to changing application requirements.

There are many classifications of Optimization Techniques based on various categories with respect to WSN, viz:

Table 6. Optimization at Different Design Levels [26]

S. No.	Design Level	Optimization
1.	Architecture-level	Bridging, Sensor web, Tunneling
2.	Component-level	Parameter-Parameter-Tuning,Markov Decision Process(MDP) -based dynamic optimization
3.	Data Link- level	Load Balancing and Throughput, Power / Energy
4.	Network-level	Query Dissemination, Data Aggregation, Real-Time, Network Topology, Resource Adaptive, Dynamic Network Reprogramming
5.	Operating System-level	Event-Driven, Dynamic Power Management, Fault-Tolerance

Table 7. Optimization Techniques for Routing [47] in WSN

S. No.	Optimization
1.	Genetic Optimization
2.	Particle Swarm Optimization (PSO)
3.	Ant Colony Optimization (ACO)
4.	Artificial Bee Colony Optimization (ABCO)

Table 8. Optimization Techniques for Energy and Power [48] in WSN

S. No.	Optimization
1.	Direct Diffusion
2.	Clustering
3.	Data Aggregation
4.	Duplicate Suppression
5.	In-network Data Processing
6.	Address-Centric

Table 9. Bio-Mimic Optimization Techniques [49] in WSN

S. No.	Optimization
1.	Particle Swarm Optimization (PSO)
2.	Ant Colony Optimization (ACO)
3.	BEES Optimization
4.	Frog Leaping Optimization
5.	Elephant Swarm Optimization
6.	Genetic Algorithm

A WSN typically has little or no infrastructure. A sensor network consists of a large number of sensor nodes, densely deployed either inside the monitoring environment or

very close to it. Unlike traditional networks, a wireless sensor network has its own design and resource constraints. Sensor nodes have very limited processing and communication capabilities. As a result, while traditional networks focus more on achieving high quality of service (QoS), sensor network protocols have to focus mainly on network lifetime issues. Various resource constraints that affect the network are low bandwidth, short communication range, limited processing and storage in each node. All the above mentioned issues are directly related to the optimization problem. Maximizing the lifetime, meeting the QoS requirements along with providing security is not an easy task. Often these three issues contradict with each other. If we want to ensure energy efficiency, then QoS and security is comprised. If QoS is assured, then the other two issues may lack proper awareness. So, from the optimization point of view of WSN, the right choice of the optimizer or algorithm for WSN problems is very important. The algorithm which is chosen for an optimization depends upon various factors like the nature of the algorithm, the type of the problem, the desired quality of solutions, the available resources, time constraints, *etc*. The nature of an optimizer determines if it is appropriate for a particular type of problem.

4. Brief Review of Work Already Done with Respect to Optimization Approaches in Wireless Sensor Network (Literature Review)

Dharini Ganesh *et. al.,* [51] in the paper, "Optimization Techniques for Wireless Sensor Networks", focused on energy conservation for wireless sensor networks mostly through various optimization techniques. These techniques concentrated on communication and operation management. In some applications there was minimum need for sensing activity for most of the time and sometimes there was need for strong sensor processing at particular instants. In such cases, there was a large variation of workloads. Energy awareness was calculated in groups as well as into the individual nodes in these applications.

Table 10. Comparison of the Various Optimization Techniques

Technique	Scalability	Concurrency	Flexibility	Energy Efficiency	Latency	Reliability	Application environment
Address-centric	Limited to smaller networks	Limited to smaller networks	Good for homogenous node applications	Good for non-redundant and completely redundant applications	Good for non-redundant and completely redundant applications	Good	Small scale commercial applications
Duplicate Suppression	Limited	Limited	Applies to homogenous nodes	Good for redundant data	Good for redundant data	Moderate	Commercial messaging networks
Directed Diffusion	Limited	Good	Can be extended to support heterogeneous nodes	Very good	Data latency in waking up intermediate nodes, setting up multipaths	Good	Suited for stationary network nodes
Clustering	Highly scalable	Moderate	Good for heterogeneous nodes when cluster head has more energy and computational capability	Very good	Lower latency	Moderate, depends on overhead of cluster head	Good for time critical application
In-network processing, data aggregation and Clustering	Highly scalable	Good	Good for all types of nodes	Very good	Least latency	Good	Target tracking and military applications

Michal Marks *et. al.*, [52] in the paper, "Optimization Schemes for Wireless Sensor Network Localization", introduced Localization Techniques. According to them, many applications of wireless sensor networks (WSN) require information about the geographical location of each sensor node. Self-organization and localization capabilities are one of the most important requirements in sensor networks. They gave an overview of centralized distance-based algorithms for estimating the positions of nodes in a sensor network. They compared three approaches: semi-definite programming, simulated annealing and two-phase stochastic optimization—a hybrid scheme that they themselves proposed. Location awareness is required for many wireless sensor network applications, but it is often too expensive to include a GPS adapter in each sensor node. An approximated geographical location is needed for acquiring and managing data, geographic routing, geographic hash tables, energy conservation algorithms, and others. Hence, various localization schemes for assigning geographical coordinates to each node in a sensor network system were proposed. Localization methods should give a solution in a short time, achieve good accuracy even in the case of unevenly distributed nodes, and scale to large networks.

Arslan Munir *et. al.*, [26] in the paper, "Optimization Approaches in Wireless Sensor Networks", explained that one critical WSN design challenge involves meeting application requirements such as lifetime, reliability, throughput, delay (responsiveness), etc. for application domains. A high priority security/defense system may have both high responsiveness and long lifetime requirements. The mechanisms needed for high responsiveness typically drain battery life quickly, thus making it difficult to achieve long lifetime when limited energy reserves are provided. Commercial off-the-shelf (COTS) sensor nodes have difficulties to meet application requirements due to the generic design traits necessary for wide application applicability. They are mass-produced to optimize cost and are not specialized for any particular application. Fortunately, COTS sensor nodes contain tunable parameters (*e.g.*, processor voltage and frequency, sensing frequency, *etc*.) whose values can be specialized to meet application requirements. However, optimizing these tunable parameters is left to the application designer. They gave the following Optimization Techniques: (1) Architecture-level Optimizations (2) Sensor Node Component-level Optimizations (3) Data Link-level Medium Access Control Optimizations: 1. Load Balancing and Throughput Optimizations 2. Power/Energy Optimizations (4) Network-level Data Dissemination and Routing Protocol Optimizations: 1. Query Dissemination Optimizations 2. Real-Time Constrained Optimizations 3. Network Topology Optimizations 4. Resource Adaptive Optimizations (5) Operating System-level Optimizations: 1. Event-Driven Optimizations 2. Dynamic Power Management 3. Fault-Tolerance (6) Dynamic Optimizations: 1. Dynamic Voltage and Frequency Scaling 2. Software-based Dynamic Optimizations 3. Dynamic Network Reprogramming and (7) MDP-based Dynamic Optimizations: 1. Dynamic Optimization Methodology

Uma Sharma *et al.*, [53] in the paper, "Power Optimization Techniques in Wireless Sensor Network by using Packet Profile based Scheme", proposed packet profile based (PPB) scheme to increase the battery power of sensor node. Profile based scheme was based on probability of past information of packet transfer, and used this information as a small data base for each node. They emphasized that due to higher bit rate in the downstream direction, the congestion appears at the node. According to them, in a WSN application, all sensor nodes can transmit and receive the packet. These nodes periodically transmit data to single sink node which is based on many to one communication model. Congestion can appear at the node due to higher bit rate, this Congestion can lead to the large number of dropping of packets and increase in transmission latency. It also affects energy efficiency. So it must be handled efficiently. There can be two types of congestion in WSN: 1) Node level congestion 2) Link level congestion. Node level congestion is very common in traditional networks and it is due to the buffer overflow in the node which

leads to the packet loss and increases queuing latency. Packet loss leads to retransmission and requires more energy. In link level congestion, as the wireless channel is shared by several nodes, if CSMA protocol is chosen, collisions could occur when multiple active sensor nodes try to seize the channel at the same time. This increases packet service time and decreases both link utilization and overall throughput. This causes the wastage of energy at sensor nodes. Both node level and link level congestion have great impact on energy efficiency and QOS. In order to efficiently use the WSN, the following issues were related: (1) Overload and speed mismatches (2) Freedom from deadlock (3) Freedom from livelock (4) Latency (5) Route recompilation.

Vivek Mhatre *et. al.,* [54] in the paper, "Energy and Cost Optimizations in Wireless Sensor Networks: A Survey", focused on two main problem areas: routing and design. They stressed that in sensor networks in which the nodes use multi-hop communication, routing is a major issue. The routing problem in the context of sensor network retains some of the features of the routing problem in ad-hoc networks, but also has some specific characteristics to it, in particular to data-aggregation, addressing, and the many-to-one paradigm (each sensor node wanting to send the collected data to a single basestation). They discussed the work done on energy efficient routing, and the corresponding optimization problems for maximizing the lifetime of the network. They also discussed some of the optimization problems in the design and dimensioning of sensor networks. Most potential applications envisioned for sensor networks require high node density; therefore, node heterogeneity and hierarchical clustering could be used for better scalability of the protocols.

Mukul Pratap Singh *et. al.,* [55] in the paper, "Techniques of Power Optimization for Wireless Sensor Network", emphasized that power optimization is the main constraint in WSN and this limitation with a typical deployment of huge number of nodes has added challenges to the design and management of WSN. WSN are typically used for remote environment monitoring in areas where providing electrical power is difficult. Therefore, the devices need to be powered by batteries and alternative energy sources. The energy of battery is limited in Wireless sensor Networks. They gave New Power Optimization Techniques as: Authentication Scheme based power optimization technique and special reference to New Ant Colony Optimization (nACO) technique, Data mining technique (Decision tree algorithm) in ZRP protocol for WSN and compared some old power optimization WSN techniques.

Table 11. Comparison of Few Power Optimization WSN Techniques

S. No.	Technique	Power Efficiency
1	LEACH	Saves 50 % of Power
2	Dynamic en-route filtering	Saves 60 % of Power
3	DMAC protocol used	Saves 50 % of Power
4	Authentication Scheme	Saves 80 % of Power
5	nACO	Saves 60 % of Power
6	Using Data mining technique	Saves 70 % of Power

Parminder Kaur *et. al.,* [56] in the paper, "A Survey of Energy Optimization Techniques In Wireless Sensor Networks", presented a review of major techniques to conserve power in WSNs. Special focus was given on AI based power optimization techniques including Clustering, Fuzzy Logic, Nueral Network based techniques etc.

They reviewed that Power optimization techniques can be broadly classified into five distinct categories:

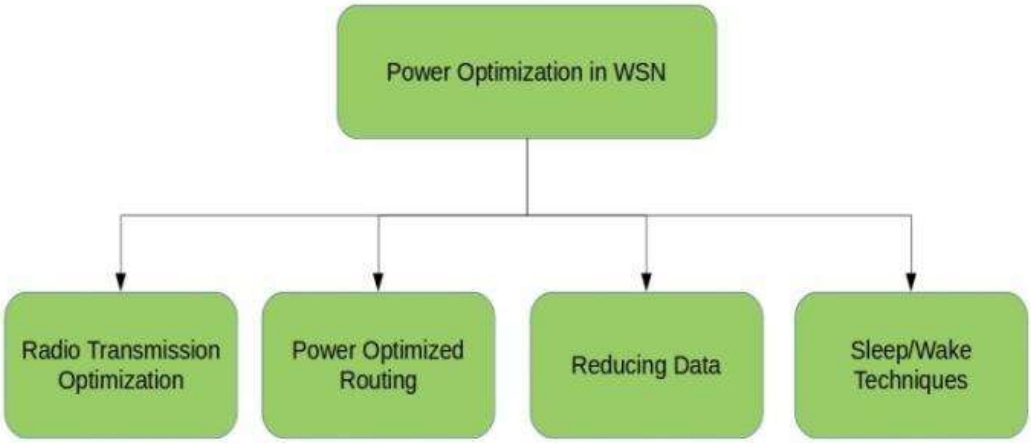

Figure 3. Power Optimization in WSN

5. Need for Routing Techniques

Routing [57] is the act of moving information across an inter-network from a source to a destination. Along the way, at least one intermediate node typically is encountered. It's also referred to as the process of choosing a path over which to send the packets. Routing is often contrasted with bridging. The primary difference between the two is that bridging occurs at Layer 2 (the data link layer) of the OSI reference model, whereas routing occurs at Layer 3 (the network layer). This distinction provides routing and bridging with different information to use in the process of moving information from source to destination, so the two functions accomplish their tasks in different ways. Routing tries to find out the least-cost or the optimized path between the source and the destination nodes. If routing is not done properly, congestion may take place.

.

5.1. Routing Challenges in Wireless Sensor Network [50]

Factors that influence the design of routing protocol in WSN are summarized below:

• Node Deployment: Sensor nodes are densely deployed in the area of interest depending upon the application which affects the performance of routing protocol. Nodes can be deployed either manually or randomly. When nodes are manually placed data is routed through pre-determined paths.

• Network topology: It must be maintained even with high node density.

• Data aggregation: It is a combination of data from different sources. Similar packets from multiple nodes can be aggregated to reduce transmission.

• Transmission media: Generally, communication takes place through wireless media, which is affected by fading which affect the operation of WSN.

• Node Capability: Depending on the application, a sensor node can have a different role or capabilities such as relaying, sensing and aggregation if all these functions are performed by the same node the energy of that node would be drained more quickly.

• Scalability: The deployment of sensor nodes is dependent on the nature of the application. Sensor node deployment varies with respect to the demand of the application,

therefore the number of sensor nodes can be hundreds, thousand or even more. To handle network scalability, routing algorithm should have the capability to cope with scalable network.

5.2. Review of Work Already Done in Routing Optimization Approaches in Wireless Sensor Network (Literature Review)

Shio Kumar Singh *et. al.*, [58] in their paper "Routing Protocols in Wireless Sensor Networks – A Survey", stated that Routing in wireless sensor networks differs from conventional routing in fixed networks in various ways. There is no infrastructure in WSN, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet strict energy saving requirements. Many routing algorithms were developed for wireless networks in general.

Table 12. Categories of Major Routing Protocols

S. No.	Category	Representative Protocols
1	Location-based Protocols	MECN, SMECN, GAF, GEAR, Span, TBF, BVGF, GeRaF
2	Data-centric Protocols	SPIN, Directed Diffusion, Rumor Routing, COUGAR, ACQUIRE, EAD, Information-Directed Routing, GradientBased Routing, Energy-aware Routing, Information-Directed Routing, Quorum-Based Information Dissemination, Home Agent Based Information Dissemination
3	Hierarchical Protocols	LEACH, PEGASIS, HEED, TEEN, APTEEN
4	Mobility-based Protocols	SEAD, TTDD, Joint Mobility and Routing, Data MULES, Dynamic Proxy Tree-Base Data Dissemination
5	Multipath-based Protocols	Sensor-Disjoint Multipath, Braided Multipath, N-to-1 Multipath Discovery
6	Heterogeneity-based Protocols	IDSQ, CADR, CHR
7	QoS-based protocols	SAR, SPEED, Energy-aware routing

Avni Kaushik [59], in her research paper, "Proactive routing protocols routing scheme A review on Routing Techniques in Wireless Sensor Networks", gave an overview on routing techniques in WSN. She focused on their classification. The routing protocols are broadly classified into two categories as route selection based routing protocols and network architecture based routing protocols

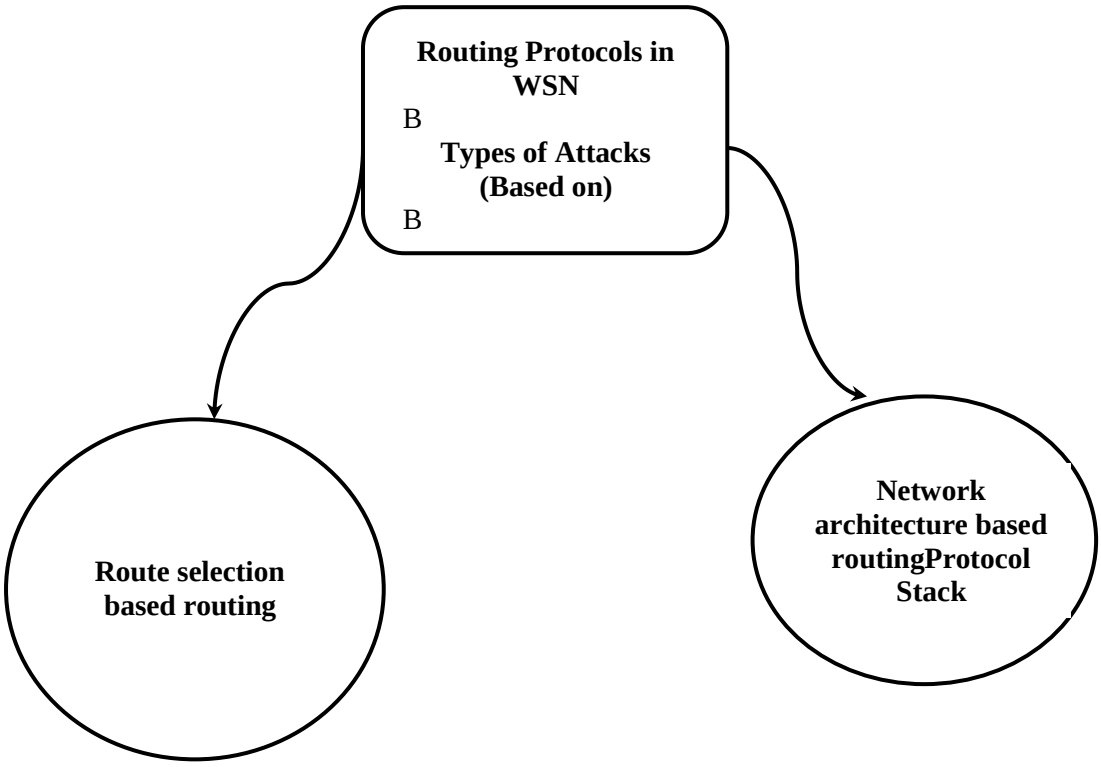

Figure 4. Routing Protocols in WSN

She also gave comparative chart of Architectural Routing Protocols and Route Selection based Routing Protocol.

Table 13. Comparison of Architecture Routing Protocols

Routing protocols	Classification	Power usage	Data Aggregation	Scalability	Query based	Over head
GEAR	Location	limited	NO	Limited	NO	Mod
DD	Flat/Data centric	limited	Yes	Limited	Yes	Low
LEACH	Hierarchical/ node centric	High	Yes	Good	No	High
SPIN	Flat/Data centric	limited	Yes	Limited	Yes	Low
GAF	Hierarchical/location	limited	No	Good	No	Mod
PEGASIS	Hierarchical	High	No	Good	No	Low
TEEN & APTEEN	Hierarchical	High	Yes	Good	No	High

Table 14. Comparison of Route Selection based Routing Protocols

Metrics	DSDV	AODV	DSR
Muticasting	No	Yes	Yes
Routing metric	Shortest path	Freshest & Shortest path	Shortest path
Mobility	Does not Perform well in High mobility	Perform well in High mobility	Does not Perform well in High mobility
Loop free	Yes	Yes	Yes
Communication	Unidirectional	Bidirectional	Bidirectional
Resource consumption	Maximum	Lesser than DSR	Greater tha AODV
Suitable in WSN	No	Yes	No
Delay	Least	Lesser than DSR	Greater than AODV
Network size	Not Suitable in large network	Suitable for Large network	Suitable for Network of less than 200 nodes
Repair of Broken links	Handled in Least time	Time consuming	Consumes less time
Routing overload	Least	Greater than DSR	Lesser than AODV

Jamal N. Al-Karaki *et. al.*, [60] in their paper, "Routing Techniques in Wireless Sensor Networks: A Survey", gave a comprehensive survey of the state-of-the-art routing techniques in WSNs. They highlighted challenges for routing protocols in WSNs and different routing techniques. Overall, the routing techniques are classified into three categories based on the underlying network structure: flat, hierarchical, and location-based routing. These protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, and coherent-based depending on the protocol operation. In flat-based routing, all nodes are typically assigned equal roles or functionality. In hierarchical-based routing, nodes play different roles in the network. In location-based routing, sensor nodes' positions are exploited to route data in the network. A routing protocol is considered adaptive if certain system parameters can be controlled in order to adapt to the current network conditions and available energy levels. These protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, or coherent-based routing techniques depending on the protocol operation. Routing protocols can also be classified into three categories, proactive, reactive, and hybrid protocols depending on how the source finds a route to the destination. In proactive protocols, all routes are computed before they are really needed, while in reactive protocols, routes are computed on demand. Hybrid protocols use a combination of these two ideas. When sensor nodes are static, it is preferable to have table driven routing protocols rather than using reactive protocols. A significant amount of energy is used in route discovery and setup of reactive protocols. Another class of routing protocols is called the cooperative routing protocols. In cooperative routing, nodes send data to a central node where data can be aggregated and may be subject to further processing, hence reducing

route cost in terms of energy use. Many other protocols rely on timing and position information.

Sanjolly Jain *et. al.*, [61], in their paper, "Routing Techniques in Wireless Sensor Networks stated that sensors in the wireless sensor network are powered with battery and its difficult to replace or recharge their batteries. Therefore, energy efficient routing has become the major concern in the field of wireless sensor network to enhance the lifetime of the network. As already evaluated, number of routing techniques has been proposed for wireless sensor network to make longer life time and low energy consumption and major three categories are: Flat and data centric routing, Hierarchical routing, Location based routing. They presented a review of some major work in area of flat and data centric routing technique and hierarchical routing technique for WSNs. They also compared different routing protocols in WSN.

Table 15. Comparison of Different Routing Protocols in WSN

Routing Protocols	Classification	Position awareness	Scalability	Mobility	Power usage	Data Aggregation	Query based	QoS
Flooding	Flat	No	Limited	No	High	No	No	No
Gossiping	Flat	No	Limited	No	High	No	No	No
Direct Diffusion	Data centric/ flat	No	Limited	Limited	Limited	Yes	Yes	No
LEACH	Hierarchical	No	Good	Fixed BS	Maximum	Yes	No	No
PEGASIS	Hierarchical	No	Good	Fixed BS	Maximum	No	No	No
TEEN & APTEEN	Hierarchical	No	Good	Fixed BS	Maximum	Yes	No	No

6. An Introduction to Ant Colony Optimization

Many optimization algorithms have been developed based on nature-inspired concepts. Evolutionary Algorithms (EA) and swarm optimization algorithms are two categories of nature inspired algorithms. EA attempts to simulate the phenomenon of natural evolution. In natural evolution, each species search for beneficial adaptations in an ever changing environment. Genetic Algorithms (GA) and Differential Evolution (DE) algorithms are the example of EA. Swarm optimization algorithms includes Particle Swarm Optimization, Bee Colony Optimization and Ant Colony optimization.

The Ant Colony optimization (ACO) [39] Algorithm is a probabilistic technique for solving computational problems which can be reduced to finding good paths through graphs. This algorithm is a member of the ant colony algorithms family, in swarm intelligence methods, and it constitutes some meta-heuristic optimizations. It was proposed by Marco Dorigo in 1992. This was the first algorithm with an aim to search for an optimal path in a graph, based on the behavior of ants seeking a path between their colony and a source of food. The original idea has since diversified to solve a wider class of numerical problems, and as a result, several problems have emerged, drawing on various aspects of the behavior of ants.

Ant colony optimization (ACO) [39] is a population-based meta-heuristic that can be used to find approximate solutions to difficult optimization problems. In ACO, a set of software agents called artificial ants search for good solutions to a

given optimization problem. ACO is a working example Algorithm of Swarm Intelligence. The Paradigm for optimization problems using Ant colony optimization (ACO) can be expressed as finding short paths in a graph.

The basic working steps can be incorporated by ant's behavior, as follows:

1. The first ant wanders randomly until it finds the food source (F), then it returns to the nest (N), laying a pheromone trail.
2. Other ants follow one of the paths at random, also laying pheromone trails. Since the ants on the shortest path lay pheromone trails faster, this path gets reinforced with more pheromone, making it more appealing to future ants.
3. The ants become increasingly likely to follow the shortest path since it is constantly reinforced with a larger amount of pheromones. The pheromone trails of the longer paths evaporate.

To summarize the ACO, it can be summed up as:

1. General paradigm for optimization problems
2. Inspiration from nature, but with smarter agents
3. Paths found by ant represent solutions for the problem
4. Choice of path influenced by previous experience
5. Pheromones as model of collective memory of a swarm
6. Tunable parameters that affect performance

6.1. General Ant Colony Pseudo Code

```
Initialize the base attractiveness, τ, and visibility, η, for each edge;
for i < IterationMax do:
        for each ant do:
                choose probabilistically (based on previous equation) the next state to
        move into;
                add that move to the tabu list for each ant;
                repeat until each ant completed a solution;
        end;
        for each ant that completed a solution do:
                update attractiveness τ for each edge that the ant traversed;
        end;
        if (local best solution better than global solution) save local best solution as
        global solution;
        end;
end;
```

6.2. Review of work already done in Ant Colony Optimization Approach in Wireless Sensor Network (Literature Review)

Benu *et. al.*, [62] in their paper, "Ant Colony Optimization for Wireless Sensor Network: A Review", introduced a new probability function for routing, introduced Intensity based wake up selection in the cluster and used it to find effected area in the cluster & also find efficiency routing for affected clusters. According to them, once the food is found, the ant will release pheromone. The communication, nullification, and combination of target data were displayed as the techniques of pheromone dissemination, misfortune, and aggregation. Since the aggregated pheromone could measure the presence of a target, it was utilized to focus the likelihood of ant-searching activity movement in the following round.

Anjali *et. al.,* [63] in their paper, "Routing Based Ant Colony Optimization in Wireless Sensor Networks", introduced a heuristic way to reduce energy consumption in WSNs routing process using Ant Colony Optimization. They introduced three Ant Colony Optimization algorithms, the Ant System, Ant Colony System and improved AS and their application in WSN routing process. The simulation results showed that ACO is an effective way to reduce energy consumption and maximize WSN lifetime.

Devee Prasan *et. al.,* [64] in their paper, "Energy Efficient and Qos Aware Ant Colony Optimization (Eq-Aco) Routing Protocol for Wireless Sensor Networks", calculated QoS in Average, Worst and Best Case using Simulation environment. They came up with conclusion that the performance of ACO is optimal in engineering applications and their research showed optimality in all aspects by offering energy efficient routing as well as QoS aware routing.

Hiba Al-Zurba *et. al.,* [65] in, "On The Suitability Of Using Ant Colony Optimization For Routing Multimedia Content Over Wireless Sensor Networks", used Ant colony algorithm is used to find the optimal routing path. Optimality according to their definition is in the sense of minimizing energy consumption and increasing link quality and reliability. The proposed approach by them resulted in minimizing energy consumption and prolonging the lifetime of the network. Optimal path also had a high link quality and reliability which enhanced video frame quality and ensured high probability of successful delivery of video frames.

Ajeet Pandey *et. al.,* [66] in their research paper, "Ant Colony Optimization Based Routing Algorithm in Various Wireless Sensor Network- A Survey", reviewed ACO based algorithms for routing in Wireless Sensor Networks and Mobile AdHoc Networks. Some of the key features of routing protocols were presented, compared and summarized. The advantages and disadvantages of Ant Colony Optimization (ACO) based Routing algorithms over the traditional Routing Algorithms were also summarized. Few Aco Based Routing in Wireless Sensor Networks are: Algorithms adapting AntNet to WSNs, Energy Efficient Ant-Based Routing (EEABR), ACO-based Quality-of-Service Routing (ACO-QoSR), Ant-based service-aware routing algorithm (ASAR), Self-organizing Data Gathering for multi-sink sensor networks (SDG), AntChain and Energy-Delay ant-based (E-D ANTS).

K. Syed Ali Fathima *et. al.,* [67] in their research paper, "Ant Colony Optimization Based Routing in Wireless Sensor Networks,", did implementation of WSN and compared its performance with AODV routing protocol based on Ant Algorithm in terms of packet delivery ratio, throughput and energy level. They came up with conclusion that performance of their algorithm was much better than AODV.

Nuria Gomez Blas *et. al.,* [69] in the paper, "Self-Organizing Routing Algorithm for Wireless Sensors Networks (WSN) Using Ant Colony Optimization (ACO) With TinyOS", stated that in-car entertainment systems, wireless sensors can obtain information from Internet, but routing protocols must be implemented in order to avoid problems. They concluded that Ant Colony algorithms can be useful in such cases. Therefore they can be embedded into the sensors to perform routing task.

7. Conclusion

With the study and statistics, comparison of few nature inspired algorithms can be stated. Ant Colony Optimization is good and efficient, but, Energy-Efficient adaptive harmonic optimization efficiently maximizes the lifetime and improves the stable period of Wireless Sensor Networks. It works by finding the optimum number of cluster heads (CHs) and their locations based on minimizing the energy consumption of the sensor nodes using genetic algorithm. The operation is broken up into rounds, where each round begins with a set-up phase, when the base station finds the optimum number of CHs and assigns members nodes of each CH, followed by a steady-state phase, when the sensed

data are transferred to CHs and collected in frames, and then these frames are transferred to the base station. It also increases the reliability of clustering process because it expands the stability period and compresses the instability period. Yet it is open for more future work.

References

[1] A. D. Wood, J. A. Stankovic and S. H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks", 24th IEEE Real-Time Systems Symposium, RTSS 2003, pp. 286-297.
[2] Cagalj M., Capkun S., and Hubaux J.-P., "Wormhole-based Anti-Jamming Techniques in Sensor Networks", from http://www.epfl.ch/Publications/Cagalj/CagaljCH05-worm.pdf
[3] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks", IEEE Journal on Selected Areas in Communications, vol. 23, Issue 4, **(2005)** April, pp. 839-850.
[4] J. Newsome, E. Shi, D. Song and A. Perrig, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259-268.
[5] M. A. Hamid, M.-O. Rashid and C. S. Hong, "Routing Security in Sensor Network: Hello Flood Attack and Defense", to appear in IEEE ICNEWS 2006, 2-4 January, Dhaka.
[6] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck and M. B. Srivastava, "On communication security in wireless ad-hoc sensor Networks", 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002, **(2002)** June10-12, pp. 139-144.
[7] Y.-C. Hu, A., Perrig and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, vol. 3, **(2003)** 30 March-3 April, pp. 1976-1986.
[8] W. Du, J. Deng, Y. S. Han and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks", Proc. of the 10th ACM conference on Computer and communications security, **(2003)**, pp. 42-51.
[9] C. C. Oniz, S. E. Tasci, E. Savas, O. Ercetin and A. Levi, "SeFER: Secure, Flexible and Efficient Routing Protocol for Distributed Sensor Networks".
[10] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks", In IEEE Symposium on Security and Privacy, Berkeley, California, **(2003)**, May 11-14, pp. 197–213.
[11] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", Proc. ACM CCS'02, **(2002)** November18-22, pp. 41-47.
[12] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), Stockholm, Sweden, **(2005)** June 20-21.
[13] C. Karlof, N. Sastry and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks", Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, **(2004)**, pp. 162 – 175.
[14] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, **(2002)**, pp. 521-534.
[15] C. Lin and G. Wu, "Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach", Springer Science & Business Media, New York, **(2013)**.
[16] Hong S. and Lim S., **(2010)**, "Analysis and attack models via unified modeling language in wireless sensor networks: a survey study", In: Proc 2010 IEEE international conference on wireless communications, networking and information security (WCNIS), pp. 692–696
[17] Hong S., Lim S. and Song J., **(2011)** "Unified modeling language based analysis of security attacks in wireless sensor networks: a survey", KSII Trans Internet Inf Syst, vol. 5, no. 5, pp. 805–821.
[18] Chan K. and Fekri F., **(2011)** "Node compromise attacks and network connectivity", Defense transformation and net-centric systems.
[19] Mishra A. and Turuk A. **(2010)** "Adversary information gathering model for node capture attack in wireless sensor networks", In: Proc IEEE international conference in devices and communication, pp. 1–5.
[20] Bonaci T., Bushnell L. and Poovendran R. (2010) "Node capture attacks in wireless sensor networks: a system theoretic approach", In: Proc IEEE 49th international conference on decision and control, pp. 6765-6772.
[21] De P., Liu Y. and Das S. **(2006)** "Modeling node compromise spread in wireless sensor networks using epidemic theory", In: Proc IEEE 7th international symposium on world of wireless, mobile and multimedia networks, pp. 237–243
[22] De P., Liu Y. and Das S. **(2009)** "Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory", ACM Trans Sens Netw, vol. 5, no. 3, pp. 1–33.

[23] Tague P., Slater D., Rogers J. and Poovendran R, **(2009)** "Vulnerability of network traffic under node capture attacks using circuit theoretic analysis", In: Proc IEEE 28th international conference on computer communications, pp. 161–165.
[24] Q. Liu, J. Yin and V. C. M. Leung, "FADE: Forwarding Assessment Based Detection of Collaborative Grey Hole Attacks in WMNs", IEEE Transactions on Wireless Communications, vol. 12, no. 10, **(2013)** October.
[25] B. Cao, "Cooperative Media Access Control with Optimal Relay Selection in Error-Prone Wireless Networks", IEEE Transactions on Vehicular Technology, vol. 63, no. 1, **(2014)** January.
[26] A. Munir and A. Gordon-Ross, "Optimization Approaches in Wireless Sensor Networks"
[27] M. Iqbal, M. Naeem, A. Anpalagan, A. Ahmed and M. Azam, "Wireless Sensor Network Optimization: Multi-Objective Paradigm".
[28] P. Tague and R. Poovendran, "Modeling Node Capture Attacks in Wireless Sensor Networks".
[29] P. K. Shukla, S. Goyal, R. Wadhvani, M. A. Rizvi, P. Sharma and N. Tantubay, "Finding Robust Assailant Using Optimization Functions(FiRAO-PG) in Wireless Sensor Network", Hindawi Publishing Corporation, Mathematical Problems in Engineering, Volume 2015 (2015), Article ID 594345
[30] Tague P. and Poovendran R., "Modeling adaptive node capture attacks in multi-hop wireless networks", Ad Hoc Netw, vol. 5, no. 6, **(2007)**, pp. 801–814.
[31] Tague P., Slater D., Rogers J. and Poovendran R., "Evaluating the vulnerability of network traffic using joint security and routing analysis", IEEE Trans Dependable Secure Comput, vol. 6, no. 2, **(2008)**, pp. 111–123.
[32] De P., Liu Y. and Das S., "Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory", ACM Trans Sens Netw, vol. 5, no. 3, **(2009)**, pp. 1–33.
[33] Bonaci T., Bushnell L. and Poovendran R., "Node capture attacks in wireless sensor networks: a system theoretic approach", In: Proc IEEE 49th international conference on decision and control, **(2010)**, pp 6765–6772.
[34] Mishra A. and Turuk A., "Adversary information gathering model for node capture attack in wireless sensor networks", In: Proc IEEE international conference in devices and communication, **(2010)**, pp. 1–5.
[35] Wu G., Chen X., Obaidat MS. And Lin C., "A high efficient node capture attack algorithm in wireless sensor network based on route minimum key set", Secur Commun Netw, **(2012)**.
[36] B. Butani, P. K. Shukla and S. Silakri, "An Exhaustive Survey on Physical Node Capture Attack in WSN", International Journal of Computer Applications (0975 – 8887), vol. 95, no. 3, **(2014)** June.
[37] O. K. Sahingoz, "Large scale wireless sensor networks with multi-level dynamic key management scheme", Journal of Systems Architecture, vol. 59, **(2013)**, pp. 801–807.
[38] R. Saif ur, G. Cui and J. Bao, "Post Deployment Encryption Key Generation for a Fully Connected and Secure Wireless Sensor Network", 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing.
[39] Ed. Wong, P. Summers, R. Ku and P. Xie, "Ant Colony Optimization", SPRING, **(2011)**.
[40] B. Krishnamachari, "An Introduction to Wireless Sensor Networks".
[41] R. Berger, "Introduction to Wireless Sensor Networks".
[42] J. A. Stankovic, "Wireless Sensor Networks".
[43] A. Bagula, "Applications of Wireless Sensor Networks", UCT
[44] R. Vaish and K. K. Satapathy, "Application of wireless sensor networks for environmental monitoring and development of an energy efficient cluster based routing".
[45] Dr. G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks".
[46] M. Lamine Messai, "Classification of Attacks in Wireless Sensor Networks".
[47] K. M. Rana and M. A. Zaveri, "Techniques for Efficient Routing in Wireless Sensor Network".
[48] M. Kaur and J. Kaur, "Performance Analysis Of Energy Optimization Techniques In Wireless Sensor Networks".
[49] V. Honguntikar and G. S. Biradar, "Optimization Techniques Incorporating Evolutionary Model in Wireless Sensor Network: A Survey", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, vol. 16, Issue 5, Ver. II, **(2014)** Sep-Oct.
[50] L. Kaur and D. Kumar, "Optimization techniques for Routing in Wireless Sensor Network", Loveneet Kaur et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, 4719-4721, ISSN: 0975-9646, vol. 5, no. 3, **(2014)**.
[51] D. Ganesh, L. M. Veeramachaneni and L. Wong, "Optimization Techniques for Wireless Sensor Networks", INFS 612 – Summer 2009, PGN # 4
[52] M. Marks and E. Niewiadomska-Szynkiewicz, "Optimization Schemes For Wireless Sensor Network Localization", Int. J. Appl. Math. Comput. Sci., 2009, vol. 19, no. 2, 291–302 DOI: 10.2478/v10006-009-0025-3.
[53] U. Sharma and Pushpa, "Power Optimization Techniques in Wireless Sensor Network by using Packet Profile based Scheme", IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0814, vol. 9, Issue 3, no. 3, **(2012)** May.

[54] V. Mhatre and C. Rosenberg, "Energy And Cost Optimizations In Wireless Sensor Networks: A Survey".
[55] M. P. Singh and K. Gupta, "Techniques of Power Optimization for Wireless Sensor Network", International Journal of Computer Applications (0975 – 8887), vol. 66, no. 3, (2013) March.
[56] Er. P. Kaur and Er. V. Kumar, "A Survey of Energy Optimization Techniques In Wireless Sensor Networks", International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, Issue 5, **(2015)** May.
[57] Basics of Routing Version 2 CSE IIT, Kharagpur.
[58] S. K. Singh, M. P. Singh and D. K. Singh, "Routing Protocols in Wireless Sensor Networks – A Survey", International Journal of Computer Science & Engineering Survey (IJCSES), vol. 1, no. 2, DOI: 10.5121/ijcses.2010.1206 63, **(2010)** November.
[59] A. Kaushik, "Proactive routing protocols routing scheme A review on Routing Techniques in Wireless Sensor Networks", International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, Issue 6, **(2014)** June.
[60] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey".
[61] S. Jain and A. Grover, "Routing Techniques in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887), vol. 94, no. 6, **(2014-15)** May.
[62] C. Goel and S. Benu, "Ant Colony Optimization for Wireless Sensor Network: A Review", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, vol. 17, Issue 3, Ver. 1, **(2015)** May-Jun., pp. 89-92.
[63] Anjali & N. Kaur, "Routing Based Ant Colony Optimization in Wireless Sensor Networks", Global Journal of Computer Science and Technology Network, Web & Security, vol. 13, Issue 4, Version 1.0 Year 2013
[64] U. Devee Prasan and S. Murugappan, "Energy Efficient and QOS Aware Ant Colony Optimization (EQ-ACO) Routing Protocol for Wireless Sensor Networks", International Journal of Distributed and Parallel Systems (IJDPS), vol. 3, no. 1, **(2012)** January.
[65] H. Al-Zurba, T. Landolsi, M. Hassan and F. Abdelaziz, "On The Suitability Of Using Ant Colony Optimization For Routing Multimedia Content Over Wireless Sensor Networks", International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC), vol. 3, no. 2, **(2011)** June.
[66] A. Pandey and A. K. Singh, "Ant Colony Optimization Based Routing Algorithm in Various Wireless Sensor Network- A Survey", Journal of Advanced Computing and Communication Technologies (ISSN: 2347 - 2804) Volume No. 3 Issue No. 4, **(2015)** August.
[67] K. Syed Ali Fathima and Mr. K. Sindhanaiselvan, "Ant Colony Optimization Based Routing in Wireless Sensor Networks," Int. J. Advanced Networking and Applications Volume: 04 Issue: 04, **(2013)**, pp. 1686-1689.
[68] N. Gómez Blas, L. F. de Mingo, L. Aslanyan and V. Ryazanov, "Self-Organizing Routing Algorithm For Wireless Sensors Networks (Wsn) Using Ant Colony Optimization (Aco) With Tinyos", International Journal "Information Technologies & Knowledge", vol. 5, no. 2, **(2011)**.

Books and E-Books

[1] M. A. Perillo and W. B. Heinzelman, "Wireless Sensor Network Protocols".
[2] S. Rhee and S. Liu, "Wireless Sensor Networking, A Guide to the Fundamentals of Wireless Sensor Networks", Milleneal Net.
[3] I. F. Akyildiz and M. Can Vuran, "Wireless Sensor Networks", Series in Communications and Networking Wiley.
[4] K. Sohraby, D. Minoli and T. Znati, "Wireless Sensor Networks", Technology, Protocols and Applications, Wiley.

e- Bibliography

[1] www.sciencedirect.com/science/article/pii/S1389128608001254
[2] www.wikipedia.org/wiki/Wireless_sensor_network
[3] http://www.ni.com/wsn/whatis/
[4] http://www.ni.com/white-paper/7142/en/
[5] 5.www.usc.edu/~bkrishna/research/talks/WSN_Tutorial_Krishnamachari_ICISIP05.pdf
[6] http://wireless.ictp.it/wp-content/uploads/2012/02/Zennaro.pdf
[7] http://www.hindawi.com/journals/mpe/2015/594345/

Authors

Ruby Bhatt, received her Master's Degree in Computer Science from Rani Durgavati University, Jabalpur, India. She completed her Master in Philosophy in Computer Science from Vikram University in 2011. She is working as an Assistant Professor in Department Of Computer Science, Choithram College, Indore, India. She has published Research Papers in Her research area includes Computer Network and Wireless Sensor Network.

Piyush Kumar Shukla, received his Bachelor's degree in Electronics & Communication Engineering, LNCT, Bhopal in 2001, M. Tech (Computer Science & Engineering) in 2005 from SATI, Vidisha and Ph.D. (Computer Science & Engineering) in 2013 from RGPV, Bhopal. M.P. India. He is Member of ISTE (Life Member), IEEE, ACM, IACSIT, IAENG. Currently he is working as an Assistant Prof. in Department of Computer Science & Engineering, UIT-RGPV Bhopal. He is also I/C of PG Programs in DoCSE, UIT, and RGPV. He has published more than 40 Research Papers in various International & National Journals & Conferences.