

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

185,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Swarm Intelligence-Based Bio-Inspired Framework for Wireless Sensor Networks

*Abdul Rahim Naseer, Vontela Neelima
and Gugulothu Narsimha*

Abstract

Wireless Sensor Networks (WSNs) are gaining immense popularity as a result of their wide potential applications in industry, military, and academia such as military surveillance, agricultural monitoring, industrial automation, and smart homes. Currently, WSN has garnered tremendous significance as it has become the core component of the Internet of Things (IOT) area. Modern-day applications need a high level of security and quick response mechanism to deal with the emerging data trends where the response is measured in terms of latency, throughput, and scalability. Further, critical security issues need to be considered due to various types of threats and attacks WSNs are exposed to as they are deployed in harsh and hostile environments unattended in most of the mission critical applications. The fact that a complex sensor network consisting of simple computing units has similarities with specific animal communities, whose members are often very simple but produce together more sophisticated and capable entities. Thus, from an algorithmic viewpoint, bio-inspired framework such as swarm intelligence technology may provide valuable alternative to solve the large scale optimization problems that occur in wireless sensor networks. Self-organization, on the other hand, can be useful for distributed control and management tasks. In this chapter, swarm intelligence and social insects-based approaches developed to deal with a bio-inspired networking framework are presented. The proposed approaches are designed to tackle the challenges and issues in the WSN field such as large scale networking, dynamic nature, resource constraints, and the need for infrastructure-less and autonomous operation having the capabilities of self-organization and survivability. This chapter covers three phases of the research work carried out toward building a framework. First phase involves development of SIBER-XLP model, Swarm Intelligence Based Efficient Routing protocol for WSN with Improved Pheromone Update Model, and Optimal Forwarder Selection Function which chooses an optimal path from source to the sink to forward the packets with the sole objective to improve the network lifetime by balancing the energy among the nodes in the network and at the same time selecting good quality links along the path to guarantee that node energy is not wasted due to frequent retransmissions. The second phase of the work develops a SIBER-DELTA model, which represents Swarm Intelligence Based Efficient Routing protocol for WSN taking into account Distance, Energy, Link Quality, and Trust Awareness. WSNs are prone to behavior related attacks due to the misbehavior of nodes in forwarding the packets. Hence, trust aware routing is important not only to protect the information but also to protect network performance from

degradation and protect network resources from undue consumption. Finally, third phase of the work involves the development of SIBER-DELTAKE hybrid model, an improved ACO-KM-ECC trust aware routing protocol based on ant colony optimization technique using K-Medoids (KM) algorithm for the formation of clusters with Elliptical Curve Cryptography (ECC). KM yields efficiency in setting up a cluster head and ECC mechanism enables secure routing with key generation and management. This model takes into account various critical parameters like distance, energy, link quality, and trust awareness to discover efficient routing.

Keywords: wireless sensor networks, swarm intelligence, ant colony-based routing, node misbehavior, non forwarding attacks, pheromone update model, reputation system, trust aware routing, K-Medoids clustering algorithm, ECC based secure routing, energy balancing, network life maximization

1. Introduction

WSN is an emerging research area that promotes wireless communication across the nodes in a network in a random fashion. A huge set of parameters relevant to natural weather conditions pertaining to spatial and temporal domains is prominent to assess the performance of WSNs. Hence, in comparison with the normal ad-hoc networks, WSN exhibits more restricted constraints and critical conditions. WSNs are designed with a wide variety of sensors designed to tune in consistent with the particular application based domain. In WSNs, each node is mostly equipped with a restricted battery, a rather tiny memory unit, a simple processing unit, and a radio transceiver. Communication through these devices leads to the actual fact that a sensor network is a wireless ad-hoc network. Each sensor node generally supports multi-hop routing where nodes act as forwarders, relaying data packets to sink or a base station. Apart from monitoring the environment, the biggest challenge posed in WSN is the computation capability. Some of the algorithmic issues that need to be tackled in a sensor network are routing, object tracking, data gathering, power saving, base station initiated querying, etc. Solutions to the aforementioned problems hence demand an innovative computing paradigm [1].

One of the main challenges in WSNs is the large scale networking that is the sheer size exhibited by the wireless sensor networks. WSNs have an extensive collection of present and future applications ranging from a few hundred to several hundred thousand, comprising of low-end sensor nodes. The first direct consequence of such a large scale is the huge amount of traffic load incurred across the network. This could easily exceed the network capacity, and hence, hamper the communication reliability due to packets loss by collisions and congestion along the chosen path to the destination from the event field [2]. The other major aspect to deal with WSNs is the growth of the network, which impacts the overall performance and functionality. In such a scenario, it becomes essential to find the optimal routes and to maintain the communication overhead at tolerable levels when data broadcasting over a large network. This plays a prominent role to assess the scalability aspect of WSN in terms of time and space complexity. As the network scales up, the routing tables and traffic to maintain these tables also increase. For this reason, networking systems must be adaptive and scalable to variation in the size of the network. Bio-inspired mechanisms such as Ant Colony Optimization (ACO) techniques provide efficient routing mechanisms for large-scale mobile ad-hoc networks. Another major challenge to be considered is the dynamic nature of WSNs. Early communication systems comprising of transmitter/receiver pairs and communication channel are all static, whereas current networking systems are dynamic

due to their node behavior, mobility, bandwidth channels, demand patterns, traffic and networking conditions. It is essential to take into account the communication mode adopted across the nodes within a particular range to estimate the overall network quality. In a target tracking application, the amount of traffic generated may increase or decrease with the time which depends upon the target behavior and monitored area. This imposes a varying load on the network resulting in inefficient capacity utilization if static approaches are used. To solve this problem, the bio-inspired solutions are known to be proficient in adapting themselves to changing circumstances towards survival.

The ability to deal with resource constraints also adds up to a major challenge in WSNs. As the number of resources acquired by the nodes increases, the overall cost in terms of bandwidth utilization also increases. More specifically, for the WSNs composed of nodes that are inherently constrained in terms of energy and communication resources, these limitations directly bound their performance and mandate for intelligent resource allocation mechanisms. The biological systems help researchers by providing solution approaches to deal with the trade-off between high demand and a limited supply of resources. For example, in the foraging process [3], ants use their individual limited resources towards optimizing the global behavior of colonies in order to find a food source in a cost-effective way. The behavior of ant colonies in the foraging process inspires many resource-efficient networking techniques. The need for autonomous operation without infrastructure also contributes to a major challenge in WSNs. Infrastructure free environment calls for a mechanism to track the growing number of nodes in the network to overcome adverse impact of overall network failure. The performance of the network must be assessed before and after every operation executed either statically or dynamically across the network so that networks continue their operations without any interruption due to the potential failures. This adds up a major responsibility on the network towards self-organization, self-evolution, and survivability. In order to tackle these challenges, biological systems provide promising solutions in the context of WSNs.

Swarm Intelligence is based on the study of the collective behavior of distributed and self-organized systems such as ant colonies, swarms of bees or birds, flocks of fishes. Ant colonies exhibit interesting characteristics which are most desirable in the context of WSN management and control. Ant colonies are able to effectively coordinate themselves to achieve specified global objectives without centralized planning or organizational structure. These cooperative behaviors to accomplish the complex tasks emerge from individual ant's much simpler behaviors and local rules which they follow by instinct. It is evident that the adaptability, flexibility, and robustness exhibited in their behaviors made them capable to solve real-world problems. In the literature [4, 5], several routing protocols with various metrics that use ant colony optimization have been reported. Ant colony optimization is a meta-heuristic approach inspired by the behavior of real ants seeking the path from their colony to the food source. Real ants explore the possible paths between a food source and their colony by depositing pheromones on their return journey to the colony and then follow the shortest path, that is, the path having the highest pheromone trails from colony to the food source. ACO is used to find the optimal path from the source (nest) to the destination (food). Forward ants select the next node randomly. Upon reaching the destination, the forward ant gets converted into backward ant and deposit pheromone trail on the path traversed. The pheromone trail will be more on the shortest path towards food. Here, the mechanism implied by the ants is said to be either random probability based or a heuristic based approach. If the mechanism followed by an ant is found to be successful, then it is adopted; else it is discarded and another path is discovered.

Secure routing is highly demanding in Wireless Sensor Networks due to the nature of routing operation in an infrastructure less environment wherein resource-constrained nodes need to cooperate with each other to route the packets. For most of the mission-critical applications, WSNs are to be deployed in harsh and hostile environments unattended where critical security issues need to be considered due to various types of threats and attacks they are exposed to. In addition to the robust key management schemes used to secure the network from external attacks [6], WSN requires strategies to mitigate the effect of insider attacks by detecting the misbehavior nodes refusing to participate in packet delivery thereby launching non-forwarding attacks. These behavior related attacks can be thwarted by assigning trust rating to nodes in the network based on the reputation they build over a period of time by being trustworthy in participating in the packet delivery. There are several insider attacks or behavior level attacks that target the routing operation in WSN [6]. In the black-hole attack, adversary nodes do not forward packets completely, whereas in a gray-hole attack, malicious nodes selectively forward some packets. Most of the insider attackers are Denial of Service (DOS) attacks [7]. Behavioral level attacks can be mitigated by providing trust enabled routing to prevent non-forwarding attacks by insider misbehaving nodes. Identity-related attacks can be avoided by providing security services based on efficient cryptography approaches to secure data confidentiality and data integrity. The various routing attacks possible against WSN can be stated as follows: Worm Hole Attack where in there is a threat on confidentiality and authenticity; Denial of Service attack (DoS) attack, where there is a threat on the availability, integrity, confidentiality and authenticity; Selective forwarding attack, which creates threat towards availability and integrity; Sink hole, gray hole and Sybil attacks posing threat on availability, integrity and authenticity; Carousel attacks holding a threat on availability, confidentiality and authenticity. Hence, there is a need to use appropriate techniques to protect data and overall network functionality from the aforementioned attacks. The number of packets dispatched correctly from source to destination, the number of packets lost, the amount of energy consumed, the fake addresses generated during the routing process, etc. are various parameters to be considered to deal with WSN attacks.

Most of the conventional networking paradigms are unable to accommodate the scalability, complexity and heterogeneity of modern world real-time scenarios. These challenges are new by-products of evolution in communication technologies in the last few decades. Hence, there is a need to identify the mechanisms that perform suitably well when dealing with a huge set of nodes, with dissimilar behavioral aspects. Particularly when dealing with WSN for insect colonies, individual node responses account for more loads and degrade the performance of the overall network. Hence, to achieve optimality in terms of resource utilization and scalability, there is a need to switch from static to dynamic access strategy. At the other end, the characteristics such as adaptive to the varying environmental circumstances, robust and resilient to failures caused by internal or external factors and self-organization lead to different levels of inspiration from biological systems towards deriving different algorithm approaches and designs at network layer for effective, robust and resilient communication. Majority of the work in the literature captures the laws of dynamics to deal with aforementioned scenarios in the modern world that may result in a probabilistic outcome. The common rationale behind this research is to capture the governing dynamics and understand the fundamentals of biological systems in order to devise new methodologies and tools for designing and managing WSNs that are inherently adaptive to dynamic environments, heterogeneous, scalable, self-organizing and evolvable. Many of the existing works in literature in the WSNs area focus on achieving better outcomes in terms of energy

efficiency or optimal routing paths based on the shortest distance or scalability aspect to deal with a huge crowd of packets and nodes or distance based minimization with limited security aspects. In this work, various essential parameters like distance, threshold, energy, link quality with security are integrated to achieve productive outcomes across the network traversal. These solutions are addressed in the proposed methodology in the form of SIBER-XLP with TECB, SIBER-DELTA, and SIBER-DELTAKE.

This chapter is organized as follows—Section 2 provides brief review on the related work in the area of swarm intelligence based secure and trust enabled energy efficient routing for WSNs. Section 3 discusses the SIBER-XLP model which represents Swarm Intelligence Based Efficient Routing protocol for WSN with Improved Pheromone Update Model and Optimal Forwarder Selection Function. This section also presents the Threshold Energy Conservation and Balancing (TECB) approach developed in SIBER XLP model for static and dynamic environments. Section 4 proposes SIBER-DELTA model which is Swarm Intelligence Based Efficient Routing protocol for WSN with Distance, Energy, Link Quality, and Trust Awareness designed to suit the harsh and hostile environment where the WSN nodes are deployed. Section 5 presents SIBER-DELTAKE model, an improved ACO-KM-ECC trust aware routing protocol based on ant colony optimization technique using K-Medoids (KM) algorithm for the formation of clusters and setting up of cluster heads, and Elliptical Curve Cryptography (ECC) mechanism for secure routing with key generation and management which further takes into account Distance, Energy, Link Quality and Trust Awareness in the routing decision. In this hybrid model, both the identity and behavior related attacks are tackled with effective results depicting the overall performance of the proposed work. This is followed by a section on conclusion and future research directions.

2. Related work

Swarm Intelligence area, on which the routing protocols of WSN are based, leads to optimal use of resources in a distributed way. The routing capacity of a protocol is effective if it leads to the minimization of energy and cost of traversal across the nodes. Swarm intelligence based efficient routing (SIBER) is an Ant Colony Optimization (ACO) [8] based routing algorithm for WSN where the forward ants are launched at regular intervals from source node with the mission to locate the sink node with equal probability by using neighbor nodes with minimum cost along the path from source to sink. ACO in integration with WSN achieves better energy saving and reduction in communication overhead. Using variants of the basic ACO, several approaches with different constraints were proposed in the area of ACO based routing algorithms for WSN. In the Energy Efficient Ant Based Routing (EEABR) Protocol proposed in [9], pheromone distribution is used in such a way that nodes nearer to the destination have high pheromone when compared to the other nodes. It suffers from excessive packet delivery delay as it does not take into account link quality. IEEABR [5] is an improved version of EEABR which allows non-optimal paths to be selected for packet transmission, increasing network lifetime and preserving network connectivity, but incurs excessive delay in packet delivery. Sensor Driven and Cost-Aware Ant Routing (SC), Flooded Forward Ant Routing (FF) and Flooded Forward Ant Routing (FF) protocols are proposed in [10]. The SC algorithm is energy efficient but suffers from a low success rate. Flooded Forward Ant Routing, FF Protocol is a multipath routing protocol which uses broadcast method to route packets to the sink by flooding forward ants to the sink. The FF algorithm exhibits shorter time delays, but suffers from generation of

significant amount of traffic. Flooded Forward Ant Routing, FF Protocol utilizes constrained flooding of both forward and data ants to route the data and to discover optimal paths. It exhibits high success rate when compared to SC and FF but suffers from high energy consumption. It has been seen from the detailed analysis of various-reported ant colony based routing algorithms for WSN in the literature [4, 5], most of the ant colony based routing techniques do not consider all the parameters to select the best quality path in terms of energy, distance, link quality and other metrics thereby leading to the selection of sub-optimal paths. WSNs form a major source for Internet of Things (IoT) due to their ability to adapt dynamically with the modern world gadgets. The computational capacity of a sensor network depletes while progress is made to transmit data across the nodes in a network. Hence the protocols to route data across the network need to be highly dynamic in nature with the ability to adapt to changes in the environment. Clustering relevant data into similar entities, ability to reduce the size of data by applying mining techniques, increasing the network life time in a robust fashion, dealing with power and network outages across widely distributed geographical locations are some of the parameters that need to be considered while the development of the routing algorithms.

A Reputation system based framework for Energy Efficient, Trust-enabled Secure Routing for Wireless Sensor Network proposed in [10, 11] incorporates a customized reputation system defined as Sensor Node Attached Reputation Evaluator (SNARE). SNARE is a collection of protocols that communicates directly with the network layer and adopts geographical routing principle to cope up with large network dimensions and relies on a distributed trust management system for the detection of malicious nodes. The system consists of three main components—monitoring component, rating component and response component. The monitoring component, observes packet forwarding events. Here a monitoring node will not be in a continuous monitoring mode of operation, rather, it will monitor the neighborhood periodically and probabilistically to save resources. When a misbehaving event is detected, it is counted and stored until an update time and then a report is forwarded to the rating component. The rating component at the other end, evaluates the amount of risk an observed node would provide for routing operation. The risk value is a quantity that represents the previous misbehaving activities that a malicious node (a node that drops packet) obtained. This value is used as an expectation for how much risk would be suffered by selecting that malicious node as a router. Risk values are updated based on the first hand information every time a new misbehavior report is received from the monitoring component. Additionally, if an observed node behavior is idle for a certain period of time, then its risk value is reduced. A monitoring node also updates the risk values of its neighbors by second hand information received periodically from some announcers. Based on the trust relations, a node will try to avoid malicious nodes based on the routing decision made by the routing protocol—Geographic, Energy, Trust Aware Routing protocol (GETAR) [11]. GETAR incorporates the trust information along with distance and energy information (routing decisions are based on a weighted routing cost function which incorporates trust, remaining energy and location attributes) to choose the best next hop for the routing operation thus allowing for better load balancing and network lifetime extension. To design a framework based on reputation for sensor networks, nodes maintain reputation for other nodes and use it to evaluate their trustworthiness. This results in the development of a robust and scalable model in a generalized fashion to deal with defects across the data transmission process. This approach employs Bayesian formulation where probability is of at most significance. Social networking plays a prominent role to determine the trust factor based on reputation of a node. The present and

future behavior of nodes in the network can be judged based on the reputation of a particular node [12]. Beta reputation based system is a strong inference based system that enables to set foundation of trust between the people in e-biz world. The performance of such a system can be evaluated by changing the weight across the nodes (small or large), by changing the feedback factor (positive or negative), by changing the discount and forgetting factors (old or new), and an integration of either of these factors, all based on reputation factor of a node. The goodness of this approach is that it is not adhered to any single environment [13]. However, as it also uses probability to calculate the aforementioned parameters, the working of this system cannot assure effective results in real time.

At the other end, authentication and key management schemes are the most important security services to provide data security and data confidentiality in WSN. Techniques such as random key pre-distribution for pair wise key establishment and broadcast authentication to provide security without the expensive Public key cryptography operations is preferable for deployment in traditional networks. However, random key pre-distribution techniques cannot ensure key establishment among any two nodes and endure arbitrary node compromises at the same time. Moreover, it has become highly challenging task to achieve loose time synchronization required by all broadcast authentication schemes in WSNs [14]. In recent years, application of Public key cryptography on resource-restricted sensor networks in the form of Elliptic Curve Cryptography (ECC) has emerged as highest preferred approach among several PKC options as a result of its fast computation, small key size, and compact signatures. ECC is based on mathematical formulation of discrete logarithmic problem that performs scalar computations among the points on the curve. With this kind of computation, it is difficult for the intruders to extract the original message in WSN environment. ECC uses discrete log approach to generate key and to perform encryption and decryption techniques. A data packet can be encrypted using ECC upon discovery of route to the sink node [15]. ECC is further strengthened by the addition of a predetermined threshold values in the method that transmits the information by splitting the original information into several small pieces of information, based on which the appropriate secret key will be generated, making it difficult for third parties to tamper over the network. This method was found to be effective as compared to RSA algorithm for sensor networking environment. However, the size of message piece was chosen in random, without describing any standard methodology to achieve effective threshold based outcomes [16]. An efficient integrity-preserving data aggregation protocol yields better performance in terms of reduction of the communication overhead as compared to the modulo addition based methods. This integrity preserving method in conjunction with Elliptic Curve Cryptography results in achieving the maximum optimum higher bound in a secure way. The proposed work in [17] allows the verification of the authenticity of aggregated data both at the base station and aggregators. However, due to the decryption at aggregators, both these approaches suffer leakage of data privacy. Also, the method developed is applicable to hierarchical structures with level wise arrangement. The algorithm proposed in [18] to construct the optimal network architecture in a cluster form employs Elliptic Curve Cryptography to commute public and private keys using a 176-bit encryption key consisting of combining the node ID, Elliptic curve encryption key, and the distance to its cluster head. Homomorphic encryption is used to allow cluster head to aggregate the encrypted data without having to decrypt them thereby reducing the energy consumption of cluster heads. This proposed technique greatly improves the network lifetime, memory requirements, communication overhead, and energy consumption. The ECC can in turn be integrated with other Message Authentication Code (MAC) to enhance the level of security through authentication [19].

WSNs where the sensor nodes combine their data to form a global environment include base stations that process the data collected across various nodes. This may result in depletion of huge amounts of energy and scalability issues. The solution to overcome this problem is through integration of clustering algorithms. Various heuristic based clustering methods that enable the reduction in energy consumption include linked clustering, hierarchical clustering and weighted clustering algorithms like highest connectivity based clustering, Max-Min Clustering, LEACH method, etc. The linked clustering algorithms like LCA and LCA2 work well in the scenarios where there is a unique identity assigned to each node in the cluster. However, there may be limited number of clusters or nodes per cluster, making it difficult to work in dynamic environment [20]. In Highest Connectivity clustering method, the cluster head is selected based on the highest degree of a node. The clusters once chosen to act as a master may in turn act as a slave if new cluster head is elected. At the other end, in max-min clustering, stable masters and large clusters can be created with huge set of messages delivered across each node from source to destination. In weighted clustering algorithm, the mobility and transmission energy of a node enable to elect a cluster head. Large amount of energy is consumed as the cluster head is selected based on the combined weight of each node. In Low Energy Adaptive Clustering Hierarchy (LEACH) and Two Level LEACH, cluster head is chosen dynamically with local computation being carried out at each node. At the other end, distributed cluster head is elected at consuming more power in Energy Efficient Clustering Scheme. There is little or no control over the cluster head in this clustering method. In Power Efficient Gathering in Sensor Information Systems (PEGASIS), large number of nodes in a cluster can be formed, which leads to high energy efficiency but leads to long delays when the chain (huge number of connected nodes) is long. In our proposed model, k-medoids clustering is chosen that overcomes the drawbacks of the aforementioned methods, as the appointment of cluster head is done based on the distance of the data points from cluster center and hence there is no consumption of higher energy or dissipation of high power, resulting in constant performance across the nodes suitable for wireless sensor networking environment. The selection of a cluster head varies from one protocol to the other, with probability based approach being the most common one to estimate the energy level and power consumption level of a particular node in heterogeneous environment [21]. Efficient routing technique is regarded as the one that develops shortest path between the cluster head and sink, leading to the development of optimal path. Also, the energy consumption of sensor nodes in WSN can be minimized using clustering techniques where nodes with similar properties form a cluster and are close in resemblance to each other. The election of a cluster head in various clustering techniques can be made based on either a probability model or a fuzzy rule selection [22]. Fuzzy logic is built around a set of inference rules that enable to measure various parameters like distance, probability, density of a node, etc.

3. SIBER-XLP model

This section deals with the proposed model SIBER-XLP: Swarm Intelligence based Efficient Routing for WSN with Improved Pheromone Update Model (PUM) and Optimal Forwarder Selection Function (FSF). SIBER-XLP model considers the link quality of the path along with energy and distance to select the shortest path from source to destination. It has been observed from our detailed analysis of various reported ant colony based routing algorithms for WSN that the Forwarder Selection Function to select a node for packet forwarding and Pheromone update model need to be revisited. SIBER-XLP includes two variants named as SIBER-ELP

the sink node. The Forwarder Selection Function must always choose an optimal path from source to the sink to forward the packets with the sole objective to improve the Network Lifetime by balancing the energy among the nodes in the network to ensure that some nodes along the path do not get depleted fast (resulting in Network disconnections or partitioning) and at the same time selecting good quality links along the path to guarantee that node energy is not wasted due to too frequent retransmissions. Further, selection of shortest paths involving less number of nodes results in saving of energy due to the participation of few set of nodes in packet forwarding. FSF uses a probabilistic approach to select the best node among neighboring nodes to forward the information based on Pheromone Trail (PT), Node Energy level (EN) and node link quality (LP). PT function represents the concentration of pheromone deposited on the path between the nodes, that is, current node and its neighbor node considering Energy, distance and link quality along the path from source to destination. In other words, higher PT represents the better quality path from source node to the destination in terms of energy, distance and link quality. EN function represents the energy level of the neighbor node and LP function represents the quality of the link between the current node and the neighbor node.

Hence, FSF (n_i, n_j) selects the best node n_j among neighboring nodes to forward information from the current node n_i can be defined as:

$$FSF(n_i, n_j) = \begin{cases} \frac{[PT(n_i, n_j)]^\alpha [EN(n_j)]^\beta [LP(n_i, n_j)]^\gamma}{\sum_{j \in NBS(n_i)} [PT(n_i, n_j)]^\alpha [EN(n_j)]^\beta [LP(n_i, n_j)]^\gamma}, & \text{if } j \in NBS(n_i), \\ 0, & \text{otherwise,} \end{cases} \quad (1)$$

where $NBS(n_i)$ represents the set of neighboring nodes of n_i , $PT(n_i, n_j)$ represents the amount of pheromone trail between the nodes n_i & n_j , $EN(n_j)$ represents the energy associated with the neighbor node n_j . $LP(n_i, n_j)$ represents the link quality between nodes n_i & n_j or link probability.

Link Probability $LP(n_i, n_j)$ between nodes n_i & n_j is given by the expression:

$$LP(n_i, n_j) = \frac{1}{ETX(n_i, n_j)} \quad (2)$$

where ETX is an Expected Transmission Count, calculated based on the past events occurred along that link. α, β, γ are the tunable parameters to control the importance of node energy level, pheromone trail, and link quality of the path. When $\alpha = \beta = \gamma = 1$, all three parameters PT, EN, LP are given equal importance in the selection of the forward node. If higher priority is to be assigned to PT that represents pheromone trail of the path, then assign the values as $\alpha = 1, \beta = \gamma = 2$. Likely, to prioritize EN level of node, assign the values as $\alpha = 2, \beta = 1, \gamma = 2$. Finally, to give high priority to LP parameter, assign the values as $\alpha = 2, \beta = 2, \gamma = 1$ in the selection of forward node.

Let $EI(n_j)$ be the node n_j —initial energy and $ER(n_j)$ be the node n_j —remaining energy; then energy level of the node n_j , $EN(n_j)$ is given by:

$$EN(n_j) = \frac{ER(n_j)}{EI(n_j)} \quad (3)$$

where

$$ER(n_j) > E_{th}$$

Threshold Energy E_{th} is associated with each and every node. E_{th} is defined as the minimum threshold energy needed for a node to participate in packet forwarding. Another possibility provided is to set E_{th} to the least minimum threshold ($E_{th_{min}}$) at which point the nodes will discontinue in packet forwarding because of energy exhaustion or detachment from the network.

3.1.2. Pheromone update model (PUM)

It is observed that the amount of pheromone computed to be placed on the path during return journey is not efficient to reflect that path as an optimal one, during the simulation period. Strongest path should have largest amount of pheromone whereas weakest path should have least amount of pheromone or almost zero. Among the competing stronger paths for selection, the variations in pheromone concentration should be such that always strongest path (i.e., optimal) is selected. Taking this into consideration, improved PUM model with the following parameters collected by the forward ant is developed— E_{avg} , Average energy of the nodes involved in the path traveled by forward ant, E_{min} , Minimum energy of the nodes involved in the path traveled by forward ant, Nh_{sd} , Number of hops from source to sink traveled by the forward ant, $LP(Pt_k)$, Link Probability of the nodes involved in the path from source to sink traveled by the forward ant. Average ETX of the links in the path Pt_k , is given as:

$$ETX_{avg}(Pt_k) = \frac{\sum_{i=1}^{Nh_{sd}(Pt_k)} ETX_i}{Nh_{sd}(Pt_k)} \quad (4)$$

$$\text{Link quality of the path } Pt_k, LP(Pt_k) = \frac{1}{ETX_{avg}(Pt_k)} \quad (5)$$

$$\text{Path Link Quality, } PLQ(Pt_k) = \frac{LP(Pt_k)}{Nh_{sd}(Pt_k)} \quad (6)$$

$$\text{Path Energy Quality, } PEQ(Pt_k) = \frac{E_{avg}}{E_{in}} - \left(1 - \frac{E_{min}}{E_{avg}}\right) \quad (7)$$

Higher average and minimum energy of nodes along the traversed path would result in a good quality path in terms of Energy.

Pheromone Update Function,

$$\Delta PT = \text{PathEnergyQuality} * \text{PathLinkQuality}$$

$$\Delta PT = \left(\frac{E_{avg}}{E_{in}} - \left(1 - \frac{E_{min}}{E_{avg}}\right) \right) * \frac{LP(Pt_k)}{Nh_{sd}(Pt_k)} \quad (8)$$

Equation (8) extracts the impact of average and minimum energy of the nodes along the optimal path. In other way, good quality optimal paths having high average and minimum energy will result in large amount of pheromone deposition on the path. If destination node is reached, then forward ant is converted to backward ant and the traversed path is updated by improved Pheromone Update Function (ΔPT).

At instances where nodes nearer to the destination are supposed to have higher pheromone deposition as compared to the nodes nearer to source, ΔPT computed in (8) is updated by the backward ant in the following fashion:

$$\Delta PT = \Delta PT * \left(1 - \frac{Nh_{cd} - 1}{Nh_{sd}}\right) \quad (9)$$

where Nh_{cd} is the number of hops from current node to the destination node during the traversal of backward ant from destination to the source node.

Whenever a node n_i receives a backward ant coming from a neighboring node n_j , it updates $PT(n_i, n_j)$ in its routing table in the following manner:

$$PT(n_i, n_j) = (1 - \rho)PT(n_i, n_j) + \Delta PT \quad (10)$$

where, ρ is a decay coefficient and $(1 - \rho)$ represents the evaporation of Pheromone trail since the last time $PT(n_i, n_j)$ was updated.

3.2 Performance evaluation

SIBER-XLP model with static and dynamic deployment of nodes is implemented and simulated using NS-2. To evaluate the performance of proposed model, initial scenario with random network topology is chosen to carry out the experiment with random way point mobility model selected to progress at a specified speed. The network size with 25, 50, 75 and 100 nodes is considered to demonstrate the effectiveness of results. The results obtained by the implementation of the proposed work are compared against the existing EEARB model in [9] to evaluate the efficiency of the proposed work. The parameters chosen to determine the effectiveness of the proposed model are Energy efficiency abbreviated as EE, Minimum Available Energy represented as ME, Latency shown as LT, Packet Delivery Ratio represented as PDR. The behavior of nodes in static and dynamic environments against parameters EE, ME, PDR, LT is shown in **Figures 2** and **3**. The results show the effectiveness of SIBER-VLP model against the other models like SIBER-ELP and EEABR for a maximum of 100 nodes. **Figures 2(a)** and **3(a)** show a significant increase in energy efficiency for both SIBER-ELP and SIBER-VLP models when compared with EEABR in static environment, while still showing greater increase in energy efficiency in dynamic environment. As evident from **Figures 2(b), (d), and 3(b), (d)**, the PDR and ME values are more in dynamic than in static mode and have much higher value compared to EEABR. It is observed from the **Figures 2(c)** and **3(c)** that the latency variation is similar irrespective of the kind of environment in which the nodes are deployed. From the simulations results, it is clear that SIBER-VLP recording best performance over EEABR and SIBER-ELP recording average performance as compared to SIBER-VLP but better than EEABR model.

3.3 Energy conservation and balancing in WSN

Extending the life of a wireless sensor network is critical to important applications such as battlefield surveillance where the nodes of the network must continue to be monitored and reported for a maximum period rather than getting exhausted in a less span of time, leading to interruptions in the network, division due to depletion of energy, etc. Due to the constraints exhibited by nodes of the WSN, it is necessary to utilize energy in an efficient way by introducing novel techniques and approaches to extend the lifetime of the WSN [25, 26]. In this section, the significance of the

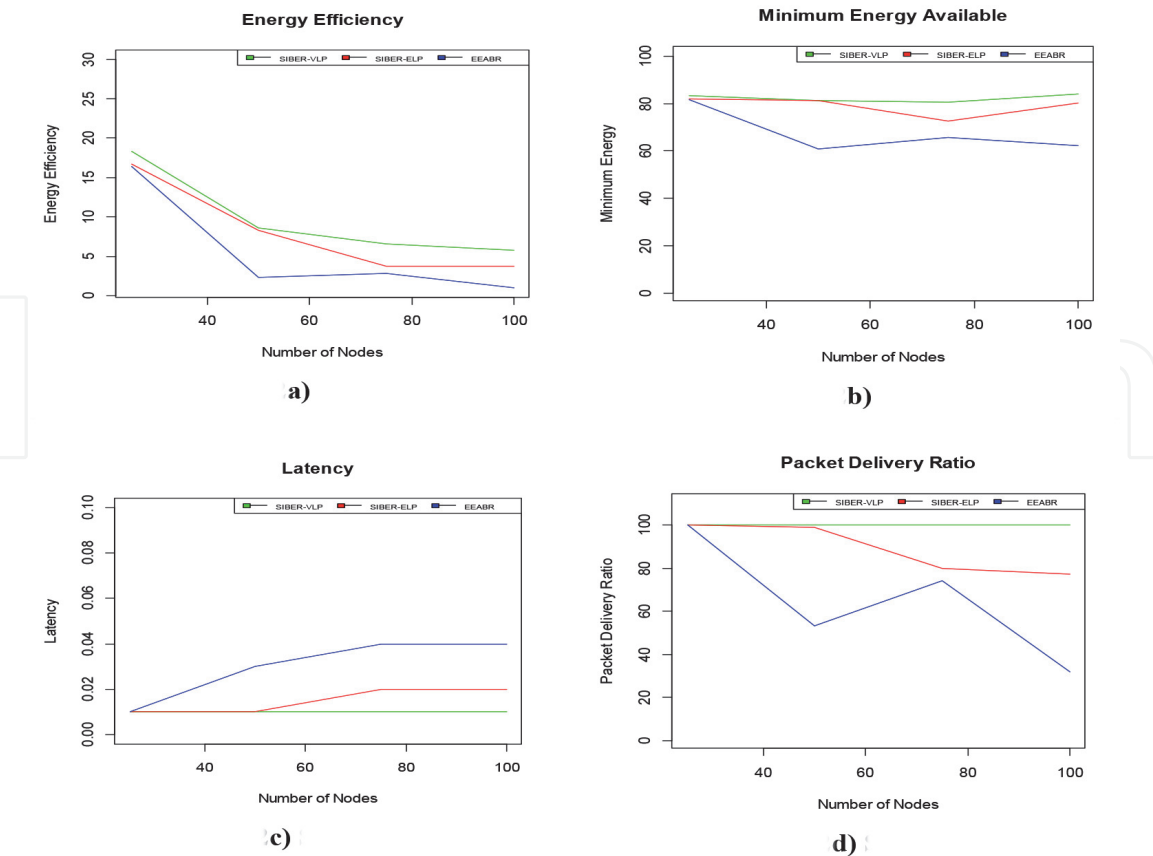


Figure 2.
(a) Static EE evaluation. (b) Static ME evaluation. (c) Static LT evaluation. (d) Static PDR evaluation.

conservation of energy and its balancing using threshold energy concept (TECB) among nodes [27, 28] in SIBER-XLP is presented. The basic assumption taken here is that every node can participate in packet forwarding process if and only if it has sufficient energy larger than the threshold energy (E_{th}). Also, the least minimum threshold ($E_{th_{min}}$) is introduced which is set to a minimum value. If any node's energy reaches $E_{th_{min}}$, this bottom point disables the node in the packet forwarding process. E_{th} is a tunable parameter that means based on the traffic occurring on the network, E_{th} can be set to a value by which all the nodes get an opportunity to participate in the packet forwarding process by which the network life time will be extended. Initially, E_{th} is chosen a high percentage value of the node's total energy, so that every node involves in the routing. Once the energy of the node reaches the E_{th} , it can be reduced to a suitable value by which one of the neighboring nodes with good quality participate in forwarding packets or to a least minimum threshold ($E_{th_{min}}$) at which point node is disabled to participate in forwarding packets.

In general, any application can be viewed with three different kinds of traffic—low level, medium level and high level. E_{th} can be set to these three levels in different scenarios. For low level traffic scenario, E_{th} can be raised to a high value, i.e. 70–80% of the energy, for the active nodes participating in the forwarding process with the intention that only little fraction of their energy can be utilized. Likewise, medium level traffic, E_{th} can be adjusted to a medium level value, i.e., 50% of the available energy, and then only 50% of the battery energy will be utilized. For high level traffic scenarios, a small value can be fixed for E_{th} , i.e. 20–30%, as a result nodes participating in packet forwarding process will have more energy available for utilization.

The role of E_{th} is to limit the amount of power from the nodes that will be provided for use in accordance with the capabilities in a heterogeneous network.

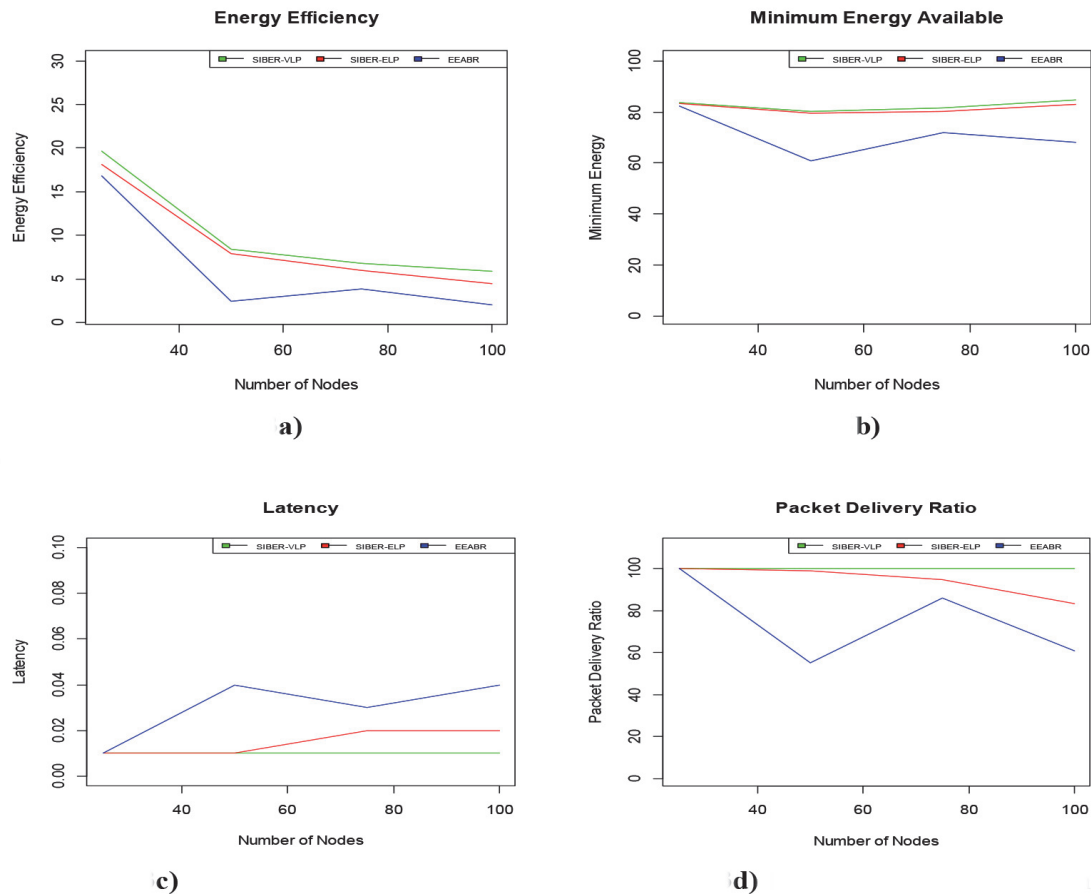


Figure 3. (a) Dynamic EE evaluation. (b) Dynamic ME evaluation. (c) Dynamic LT evaluation. (d) Dynamic PDR evaluation.

This would help to maintain the capacity of the less proficient nodes by involving them only when needed. In addition, nodes with higher capacity are involved in routing until its capacity reaches E_{th} . One may not generally have balanced paths to reach the sink with a nearly identical hop count or latency in a multipath routing. Because of the preference given to smaller distance paths with nodes having high power, the shorter paths will be chosen normally, as a result a fast decrease in the node's power in the path selected caused by the improper energy or load balance. Here, E_{th} parameter helps neighboring nodes to non-participate in forwarding packets if node's energy becomes equal/or less than E_{th} . This E_{th} control attribute conserves energy in the nodes for nearly future purpose and allows less leading nodes in the neighborhood to involve in the routing process until their levels of capacity attain E_{th} , hence conservation and balancing of energy is achieved among the neighbor nodes all the time. NS-2 Simulator is used to find the performance of the network under varying load or traffic. Based on the load, it is decided to adjust the E_{th} value of the nodes in order to conserve and balance energy by involving all the nodes alternatively in data forwarding process. In this simulation, three different kinds of traffic – low level, medium level and high level are considered. E_{th} can be set to these three levels in different scenarios. For low level traffic scenario, E_{th} can be raised to a high value (20 J) as initial energy is set to 30 J, i.e. 70% of the energy, for the active nodes participating in the forwarding process with the intention that only little fraction of their energy can be utilized. Likewise, medium level traffic, E_{th} can be adjusted to a medium level value, i.e., 50% of the available energy (15 J), and then only 50% of the battery energy will be utilized. For high level traffic scenarios, a small value can be fixed for E_{th} (10 J), i.e. 30% of the initial energy, as a

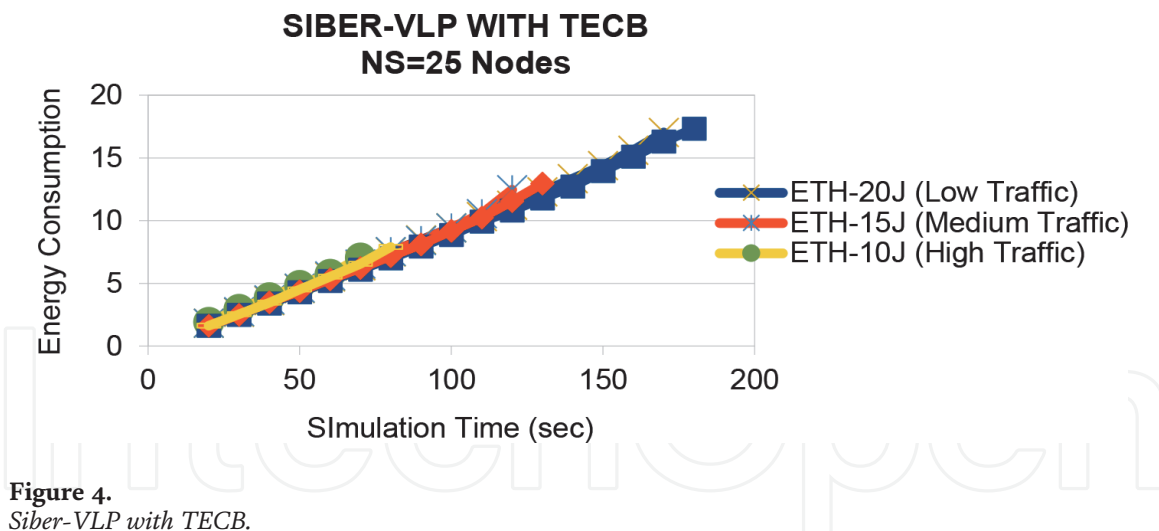


Figure 4.
Siber-VLP with TECB.

result nodes participating in packet forwarding process will have more energy available for utilization. In this simulation, the network performance, i.e. energy consumption is computed and how long the network is alive is seen based on the E_{th} value for different types of applications based on the traffic or load. Energy consumption graphs in **Figure 4** show that with the increase in simulation time, energy consumption increases which is not beyond E_{th} and number of nodes involved in forwarding the packet also increases. It is clear from the graphs that the nodes balance energy along both shorter and longer paths by setting E_{th} to only a particular value such as 10 J of energy, 15 J of energy or 20 J of energy which is accessible at each node. Same amount of energy is available on all the participating nodes at the end of the simulation period. This results in balancing energy and conserving energy, thus prolonging the lifetime of the network. There is 66% of initial energy conservation in the network for $E_{th} = 20$ J. For $E_{th} = 15$ J, there is 50% and 33% for high traffic scenarios having $E_{th} = 10$ J. Energy decreases with the rise in time, but does not fall below threshold energy in each and every case.

4. SIBER-DELTA model

Prolonging the network lifetime with the introduction of Threshold Energy concept alone is not sufficient for WSN as seen in the SIBER-XLP Model because of their constraints such as limited battery energy, limited memory, security threats, etc. As all the nodes are involved in the packet forwarding process, there is a security threat occurring from the insider nodes. In mission critical applications like military, health or commercial applications, nodes play a vital role to carry and deliver very critical and secret data. But, when a node gets compromised and misroutes the data to a wrong destination, it leads to loss of information. Also, misbehavior of nodes in the network can cause performance degradation resulting in non-forwarding attacks. There will be reduction in the system throughput with these attacks as packets need to be retransmitted many times if they are not delivered. Denial of service attacks can increase the delay in delivering the packets because some nodes which are used as forwarders may be busy in replying to the attacks and forced to delay the processing of other packets. With such attacks, network can be partitioned and communication may not take place. Finally, misbehaving nodes could also affect resources of the network by making the resource unavailable for routing. Denial of Service attacks force the adversary nodes to consume more energy during packet reception and processing unnecessarily. To tackle these misbehaving nodes in the network, SIBER-DELTA (Swarm Intelligence Based Efficient Routing protocol for WSN with Distance, Energy, Link quality and Trust Awareness) is developed as an extension to

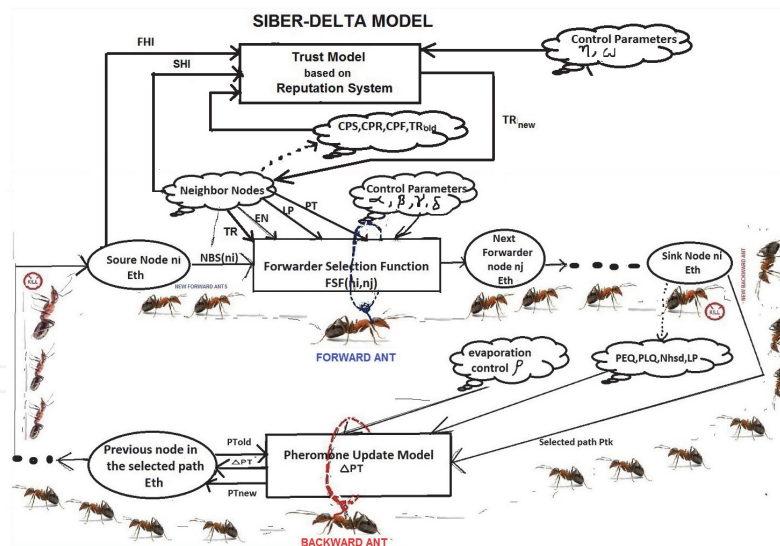


Figure 5.
SIBER-DELTA model.

SIBER-XLP to safeguard data exchange and secure data delivery. The concept of trust comes into picture in an open environment where the nodes are exposed to different types of attacks such as eavesdropping, non-forwarding attacks, denial of service attacks, etc. Hence, it is now essential to design a trust enabled routing model taking into consideration distance, energy and link quality. The proposed SIBER-DELTA Model [29] is shown in **Figure 5**.

SIBER-DELLTA Model has three components such as FSF, PUM and Trust Model (TM). The trust evaluation starts by an assumption that links in the network are bidirectional. Initially each node is associated with a trust value of 1 as no data transmission happens. As and when data forwarding takes place, there comes the trust model for evaluating a node's performance. There are two types of information obtained from the nodes of the network by the source node. One is the information received from its direct interaction with the neighbor whom it is sending data which is stated as First Hand Information (FHI). The other is the information received from the remaining neighbors of the source node except the direct neighbor which is stated as Second Hand Information (SHI). The source node calculates the Forwarding Misbehavior Index (FMI) of a node by recording all the information regarding data forwarded and data received. Mistrust Index is then calculated with the help of weighted average of FMI based on FHI and SHI. With these calculations, current trust rating of a node is depicted. Over a period of simulation time, a new current trust rating is also calculated based on their behavior in the past, so as to provide some incentives to the node for active participation or punishments to the node for misbehaving such as packet dropping. At last, final trust value of a node is calculated based on weighted average of the new current trust value and average of its trust rating in the past history. This allows handling of selective forwarding attacks in a smooth fashion. Instead of completely avoiding nodes in the routing process as done in the case of Black Hole attacks, the final trust calculation helps the selective forwarding nodes to improve their trust values based on their past history.

4.1 Trust evaluation

The nodes in the network are initially assigned a trust value of 1. Upon the data forwarding from one node to another node, trust values are altered. The information received from direct neighbors and indirect neighbors allows calculating Forwarding Misbehavior Index of each neighbor node.

Forwarding Misbehavior Index (FMI) based on Direct Interaction (FHI) is given by:

$$DIFMI(n_i, n_j) = \frac{CPR(n_i, n_j) - CPF(n_j, n_i, n_k)}{CPS(n_i, n_j)} \quad (11)$$

where n_i is source node, n_j is the direct neighbor and n_k is the next neighbor of n_j .

FMI based on Indirect Interaction (SHI) is given by:

$$IDFMI(n_i, n_j) = \frac{\sum_{n_k \in NBS(n_i)} FMI(n_k, n_j) * TR(n_k)}{|NBS(n_i)| - 1} \quad (12)$$

Mistrust Index (MI) is a weighted average calculation of both FMI based on FHI and SHI. Based on value of the weighted coefficient used, importance will be given to either FHI or SHI. For equal importance of FHI and SHI, the weighted coefficient must be assigned 0.5, as it lies between 0 and 1.

$$MI(n_j, n_i) = \eta * DIFMI(n_i, n_j) + (1 - \eta) IDFMI(n_i, n_j) \quad (13)$$

Current Trust Rating (CTR) of a node n_j upon n_i is calculated by just subtracting the mistrust value from 1.

$$TR(n_j, n_i)^{curr} = 1 - MI(n_j, n_i) \quad (14)$$

New Trust Rating based on previous Trust Rating (NTR) is a weighted average calculation of the previous trust rating of a node n_j in the previous update interval and the Current Trust Rating of a node n_j .

$$TR(n_j, n_i) = \omega * TR(n_j, n_i)^{curr} + (1 - \omega) * TR(n_j, n_i)^{old} \quad (15)$$

This is calculated because, upon the time consumption, there may be changes taking place in the node behavior. So as to provide some incentives to the node for active participation or punishments to the node for misbehaving such as packet dropping, this NTR is framed.

Final Trust Rating based on Past History (FTR) of a node is calculated based on weighted average of the New Current Trust Rating value and Average Trust Rating of node n_j (ATR) in the past history, by which selective forwarding attacks can be handled.

$$TR_{avg}^m(n_j) = \frac{\sum_{ph=k-m}^{k-1} TR(n_j, ph)}{m} \quad (16)$$

$$TR(n_j, n_i) = \omega * TR(n_j, n_i)^{curr} + (1 - \omega) * TR_{avg}^m(n_j) \quad (17)$$

Instead of completely avoiding nodes in the routing process, as of Black Hole attacks, the Final Trust Calculation helps the selective forwarding nodes to improve their trust values based on their past history.

Forwarder Selection Function is similar to the previously described Forwarder Selection Function in the SIBER-XLP model but with an additional trust parameter included.

$$FSF(n_i, n_j) = \begin{cases} \frac{[PT(n_i, n_j)]^\alpha [EN(n_j)]^\beta [LP(n_i, n_j)]^\gamma [TR(n_i, n_j)]^\delta}{\sum_{j \in NBS(n_i)} [PT(n_i, n_j)]^\alpha [EN(n_j)]^\beta [LP(n_i, n_j)]^\gamma [TR(n_i, n_j)]^\delta}, & \text{if } j \in NBS(n_i), \\ 0, & \text{otherwise,} \end{cases} \quad (18)$$

The Pheromone Update Function is also similar to the previously described Pheromone Update Function in the SIBER-XLP model but with an additional Path Trust Rating parameter included.

$$\Delta PT = PathEnergyQuality * PathLinkQuality * PathTrustRating$$

$$\Delta PT = \left(\frac{E_{avg}}{E_{in}} - \left(1 - \frac{E_{min}}{E_{avg}} \right) \right) * \frac{LP(Pt_k)}{Nh_{sd}(Pt_k)} * \frac{\sum_{n_k \in NS(Pt_k)} TR(n_k)}{|NS(Pt_k)|} \quad (19)$$

4.2 Performance evaluation

Our proposed system, SIBER-DELTA was simulated using open source NS-2 simulator. In this simulation, we have considered static and dynamic network scenarios with random topology with nodes randomly distributed. Random way-point mobility model is used for dynamic network with the nodes having the ability to move with a specified speed.

Our proposed trust enabled routing approach SIBER-DELTA is compared with SIBER-VLP [24] without trust awareness for varying network sizes (dimension)—50 and 100 nodes by introducing 10, 20, and 30% non-forwarding attackers in the network. It is assumed that all the methods use the same data rate. The performance evaluation metrics used in this simulation are Packet Delivery Ratio, Latency, Dropped packets, Average Energy Consumed, Average Energy Remaining, Minimum Energy, Energy Efficiency(Kb/J), and Standard Deviation. In our model, all nodes are assigned initially equal trust rating during the initialization and setup phase. The Performance of the network with 50 nodes and 100 nodes in both static and dynamic scenarios are shown in **Figures 6** and 7, respectively. It is clearly seen from the simulation results that SIBER-DELTA model with trust implementation exhibits high packet delivery ratio. By avoiding completely untrusted nodes and considering only trusted nodes (i.e., nodes with higher trust rating) along the paths from source to sink, SIBER-DELTA is able to achieve a high success rate of 99.51%

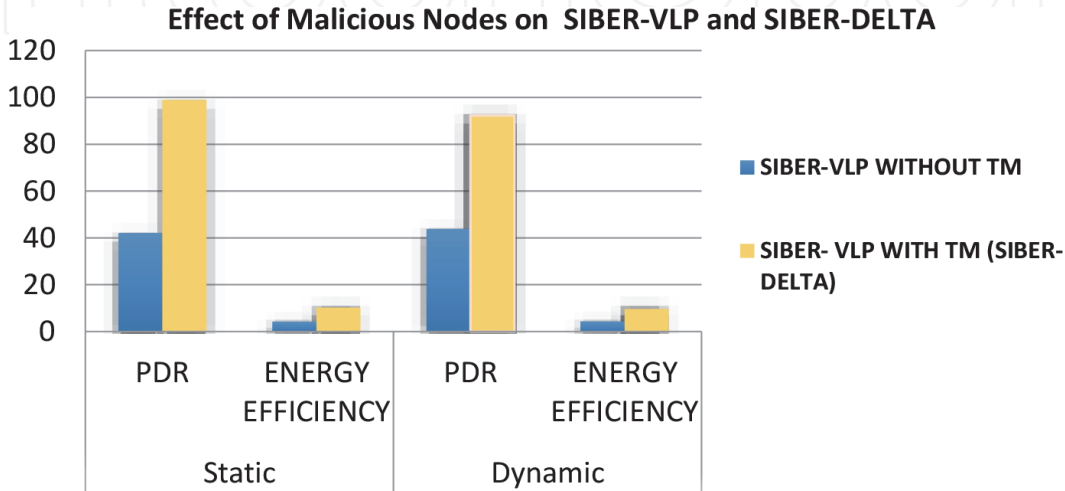


Figure 6.
Performance of the network (NS = 50 nodes).

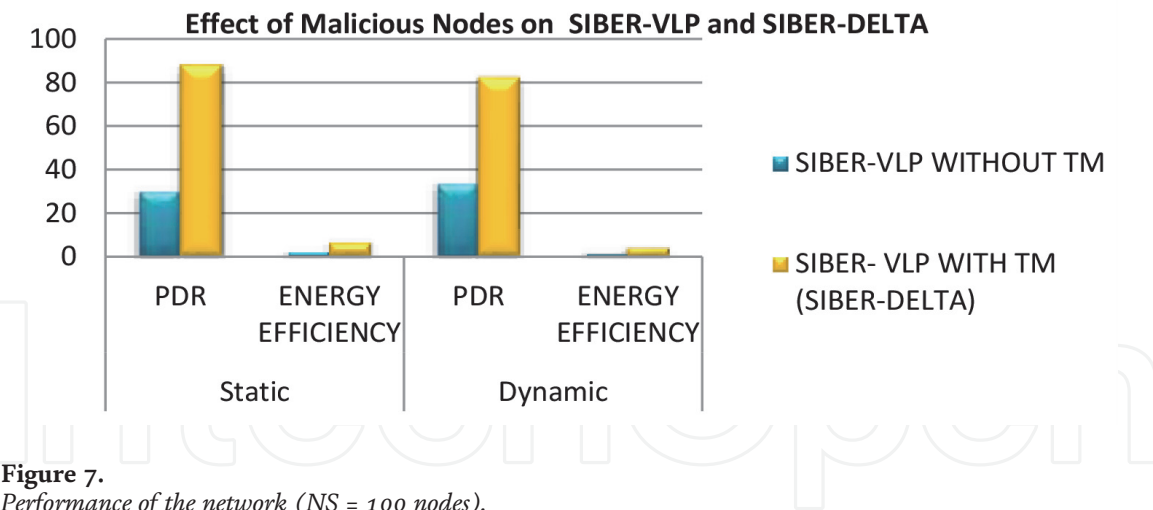


Figure 7.
Performance of the network (NS = 100 nodes).

with 10% attackers, 98.88% with 20% attackers and 98.35% with 30% attackers in the network. Since very less number of packet drops are observed during the entire simulation, it can be concluded that SIBER-DELTA performs extremely well by detecting all malicious nodes along the paths from source to sink and preventing these untrusted nodes from packet forwarding completely to achieve higher observed success rate. As evident from simulation results, SIBER-DELTA shows higher Energy Efficiency in the case of 10 and 20% attackers and slightly lower Energy Efficiency for 30% attackers as it consumes slightly higher energy due to the selection of longer alternate paths with more nodes to avoid black holes.

5. SIBER-DELTAKE model

SIBER-DELTAKE [30] Hybrid Routing protocol for WSN, an extension to trust aware routing model SIBER-DELTA is presented in this section which uses K-medoids clustering technique integrated with ECC to enhance security while selection of cluster head. This prevents the intruders from tampering the confidential information traversed across the network. This enables the early detection and termination of malicious nodes, based on the computation of values. WSN in IoT era is highly susceptible to security attacks due to huge data generation in modern era. To achieve better security, ECC is used in conjunction with authentication, key generation, group management, random number generation and key distribution techniques there by strengthening the existing security options. This will also result in better energy utilization when considering big data environment [31]. The system flow diagram of the proposed model is shown in **Figure 8**. In this approach, k-medoid clustering algorithm is chosen to select the cluster head and other members of the cluster family based on the calculation of distance between the midpoint and the sink node of the cluster. Once this is done, SIBER-DELTA mechanism is applied to update the FSF and PUM of a node. Finally, a node is permitted to transmit data based on its trust value. If the trust value of a node ready to transmit is high, then before transmission of data, it is encrypted using ECC algorithm. At the other end, if the trust value is obtained low, then the node under consideration is discarded, being regarded as a malicious node. The proposed model deals with identification of attacks and performs the following simplified steps—Initialization Phase involving network deployment, Clustering Phase using K-Medoids Algorithm, Routing Phase using SIBER-DELTA Protocol and Packet Forwarding Phase using Elliptic Curve Cryptography Technique.

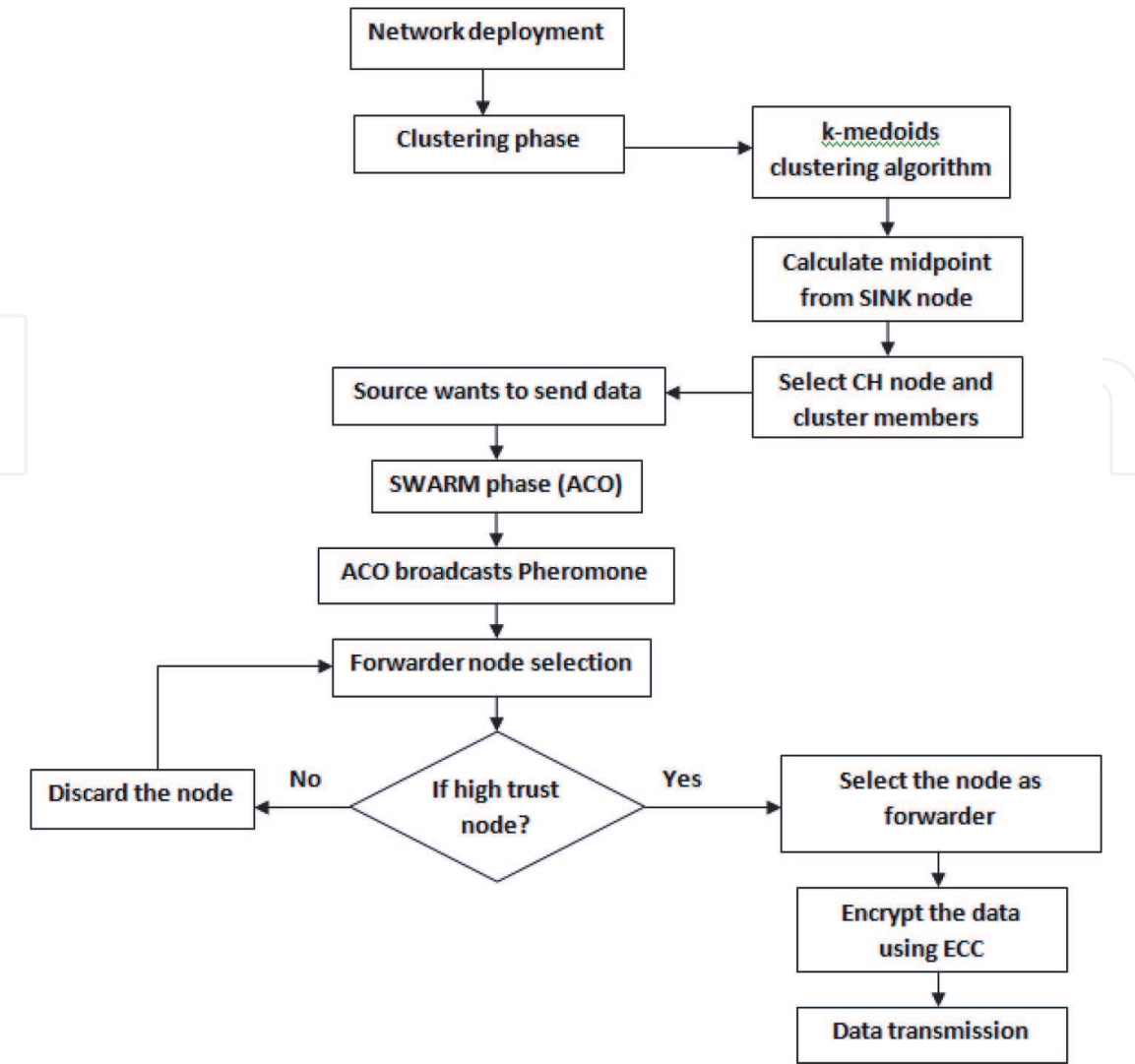


Figure 8.
SIBER DELTAKE system model.

5.1 K-Medoids algorithm (KM)

Our model SIBER-DELTAKE uses K-medoids algorithm for the formation of clusters and selection of cluster heads. *K*-medoids clustering [32] is a variant to *K*-means approach which is more robust to noises and outlier that are commonly recorded in the data generated in modern world, particularly sensor data. *K*-medoids approach uses an actual point in the cluster to represent the center of a cluster instead of using the mean point. The object, medoids with the minimum sum of distances to other points is most centrally located. The *K*-medoids algorithm is a partitioned clustering algorithm or segregating around medoids where data points are chosen to be the medoids. The object of a cluster which is known as mediod, where the average dissimilarity to all the objects in the cluster, is minimal. The representative objects *K* is first computed by this algorithm are called as *K*-medoids. Each data set object is assigned to the nearby medoid after finding the set of medoids. The various steps used in the *K*-Medoids algorithm are as follows: Step 1: Select *k* random points as the medoids initially from the given data set of *n* data points. Step 2: Each data point is associated with the closest medoid using the most common distance metrics. Step 3: Calculate the total swapping cost TC_{ih} for each pair of selected object *i* and non-selected object *h*. Step 4: Replace selected object *i* by object *h* if $TC_{ih} < 0$. Step 5: Repeat the steps 1 to 4 until there is no change in the medoids.

5.2 Elliptic curve cryptography(ECC)

The most desired approach in WSN to implement public key cryptography is ECC which is based on the algebraic structure of elliptic curves over limited fields [33]. An elliptic curve over prime field F_p , where p is a large prime number, is defined by a cubic equation of the form $y^2 = x^3 + ax + b$ where $a, b \in F_p$ are integers that satisfy the equation $4a^3 + 27b^2 \neq 0$. To have ECC based secure communication, every sensor node in the network must know an elliptic curve in addition to base point p which lies on the curve. It is assumed here that during the initial setup or the initialization phase, the elliptic curve parameters and also the base point p are loaded before only into the memory of every sensor node. Every node chooses a random prime integer as its private key and generates its public key by multiplying the private key by the base point p in order to have a secure communication between a pair of nodes. As cluster heads are involved in receiving the encrypted data from their members of cluster, then processing the data to perform data aggregation and finally forwarding the aggregated data to the base station, they consume more energy when compared to the member nodes. In order to reduce the energy consumption by cluster heads, cluster heads combine the encrypted message arriving from the members of the cluster and use Homomorphic encryption to perform aggregation of the encrypted data with no decryption thereby reducing the energy consumption of cluster heads. This results in saving of more energy and much stronger privacy of data as attackers will not be capable to hack data from intermediary nodes.

5.3 Performance evaluation

Our proposed hybrid model SIBER-DELTAKE was simulated using NS-2 simulator by considering static network scenarios with network sizes of 25, 50 and 100 nodes randomly distributed in the network area of $1000 \times 500 \text{ m}^2$. Our proposed SACO-KM-ECC based SIBER-DELTAKE system is compared with SIBER-DELTA [28] with trust awareness and SIBER-VLP [22] without trust awareness for varying network sizes by introducing 10, 20, and 30% attackers in the network. The performance of the network is evaluated using the following metrics—Packet Delivery Ratio, End to End Delay, Energy Consumption and Throughput. It is evident from the plots in **Figure 9(a)** that SIBER-DELTAKE and SIBER-DELTA models exhibit high packet delivery ratio and SIBER-DELTAKE performing better than SIBER-DELTA as more trusted and secure optimal paths are selected to forward the packets resulting in higher performance. As it is seen from simulation results, SIBER-VLP model exhibits performance degradation as malicious nodes are introduced in the network. As the number of malicious nodes increase, an increase in packet drops is observed due to the presence of more malicious nodes in the paths selected by the ants. It can be seen from **Figure 9(d)** that SIBER-DELTAKE consume little more energy when compared to SIBER-VLP and SIBER-DELTA but it is reasonable considering the fact that hybrid model needs to perform ECC computation to provide data confidentiality and data Integrity in the presence of trust awareness. Though packet delivery ratio is less in SIBER-VLP, but the comparable energy consumption in this case may be due to both packet routing and packet retransmissions. As far as the end to end delay is considered, it can be seen from **Figure 9(c)** that hybrid model has low delay when compared to other models as it selects always the most trusted and secure optimal paths. Moreover, as the number of nodes increases, there will be more number of alternate paths available to route the packets so that the malicious nodes along the selected paths can be avoided. It is clear from the **Figure 9(b)** that SIBER-DELTAKE has higher throughput when

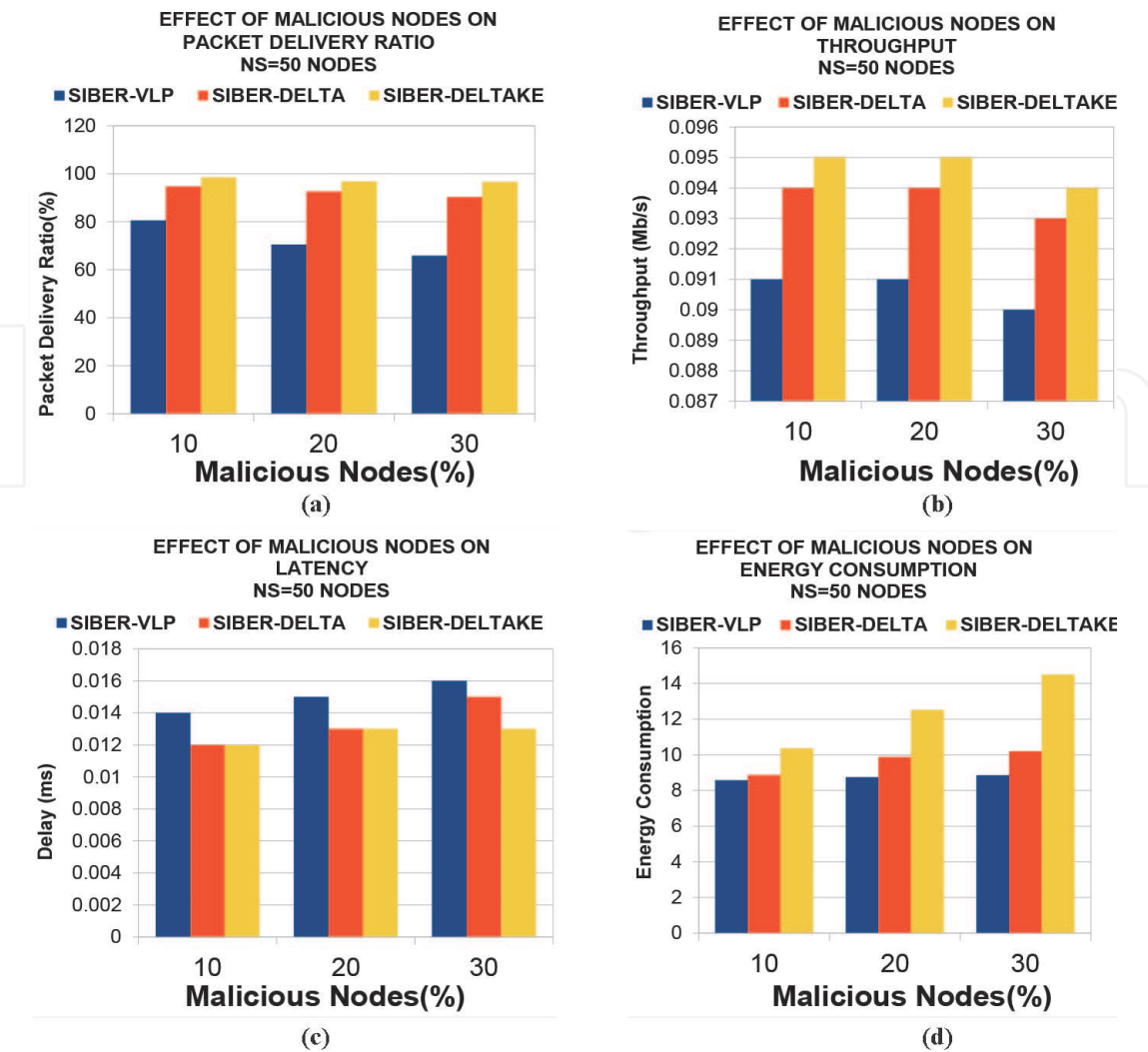


Figure 9.
(a) Effect of malicious nodes on PDR-50 nodes. (b) Effect of malicious nodes on TP-50 nodes. (c) Effect of malicious nodes on LT- 50 nodes. (d) Effect of malicious nodes on EC-50 nodes.

compared to SIBER-DELTA and SIBER-VLP. SIBER-VLP performs very poorly in the existence of larger malicious or faulty nodes in the network.

6. Conclusion and future work

In this chapter, swarm intelligence and social insects based approaches are presented to deal with bio-inspired networking framework. The proposed approaches are designed to tackle the challenges and issues in the WSN field such as large scale networking, dynamic nature, resource constraints and the need for infrastructure-less and autonomous operation having the capabilities of self-organization and survivability. This research work presents the necessity to consider a combination of evaluation parameters for efficient routing of packets from source to destination with the development of SIBER-XLP with TECB, SIBER-DELTA and SIBER-DELTAKE models, each one emerging as an improved extension over the other. NS2 simulation environment was used to develop the entire work. The outcomes achieved in terms of results can serve as a contribution to the research community in the area of WSN with further levels of security to be integrated in future due to the voluminous data generation in modern world with the development of IOT applications. Also, in this work, a set of parameters like packet delivery ratio, latency, throughput, energy

consumption, minimum available energy are evaluated against a collection of nodes. In future, a different set of parameters like load balancing across the nodes in a cluster, multi-level security aspects in WSN can be developed.

Another interesting and fascinating research direction is the application of Blockchain technology in WSN area. The blockchain technology enables peer to peer transfer of digital assets without any intermediaries and was originally created to support the famous cryptocurrency, Bitcoin. With the rapid development of Ethereum platform in recent years, the blockchain has permeated a broad range of applications across many industries and poised to innovate and transform a wide range of applications including finance, healthcare, government, manufacturing and distribution namely supply chain, digital media transfer, remote service delivery, platform for decentralized business, distributed resources, identity management, etc. The blockchain infrastructure establishes a trust among the peers in a decentralized system by having a process in place to validate, verify, and confirm transactions, record the transactions in a distributed ledger of blocks, create a tamper-proof record of blocks, chain of blocks, and implement a consensus protocol for agreement on the block to be added to the chain. Thus, validation, verification, consensus, and immutable recording lead to the trust and security of the blockchain. Though the application of block chain technology to WSN is in its initial stages, there has been research reported lately in the literature [34, 35] of using blockchain technology in peer authentication and trust level management for decentralized sensor networks. The blockchain infrastructure has shown tremendous advantages in a distributed decentralized network, but due to the limited computational power, battery life, bandwidth and more importantly storage, it may not be realistic to include all the blockchain features. In order to adopt a blockchain in WSN, we need to closely examine the operations involved in the blockchain implementation. For every transaction, a block is to be created, stored, source/sink node and transaction are to be validated & verified, broadcasted in a peer to peer network environment for block update. The role of the miners is most important to determine a valid block to be added to the blockchain using a consensus protocol based on a simplified Proof-Of-Work or Proof-Of-Stake (need to avoid biased or selfish nodes colluding to stake claim) approach which calls for having high capacity, powerful nodes to act as miners in WSN. Considering the challenges and issues with respect to the use of blockchain technology, another important network model decision would be the deployment of hierarchical sensor network with efficient clustering approach. Hence, there is a stronger need to design and develop efficient frame work and techniques to tackle the huge challenges and issues faced by blockchain technology in Wireless Sensor Network as WSN has emerged as the core component of IOT area.

Acknowledgements

We are grateful to INHA University Global Education Project Group, Incheon, South Korea for all the support and funding provided for the publication of this research work.

IntechOpen

Author details

Abdul Rahim Naseer^{1,2*}, Vontela Neelima³ and Gugulothu Narsimha⁴

1 School of Global Convergence Studies (SGCS) Inha University, Incheon, South Korea


2 School of Computer and Information Engineering (SOCIE), Inha University, Tashkent, Uzbekistan

3 Department of Computer Science and Engineering, Jyothishmathi Institute of Technology and Science, Karimnagar Affiliated to JNTUH, India

4 Department of Computer Science and Engineering, JNTUH College of Engineering, Hyderabad, India

*Address all correspondence to: dr_arnaseer@hotmail.com

IntechOpen

© 2020 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Dressler F, Akan OB. A Survey on bio-inspired networking. *Computer Networks*. 2010;54:881-900
- [2] Dressler F, Akan O. Bio-inspired networking: From theory to practice. *IEEE Communications Magazine*. 2010; 48(11):176-183
- [3] Farooq M, Di Caro GA. Routing protocols for next-generation networks inspired by collective behaviors of insect societies: An overview. In: Blum C, Merkle D, editors. *Swarm Intelligence, Natural Computing Series*. Berlin, Heidelberg: Springer; 2008. pp. 101-160. DOI: 10.1007/978-3-540-74089-6_4. ISBN: 978-3-540-74088-9(print), ISSN: 1619-7127
- [4] Saleem M, Di Caro GA, Farooq M. Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions. *Information Sciences*. 2010;181(20): 4597-4624
- [5] Zungeru AM, Ang L-M, Seng KP. Classical and swarm intelligence routing protocols for wireless sensor networks: A survey and comparison. *Journal of Networks and Computer Applications*. Elsevier; 2012;2012:1508-1536
- [6] Naseer AR, Maarouf IK, Ashraf M. Routing security in wireless sensor networks. In: *Handbook of Research on Wireless Security*. USA: Idea Group Reference; 2008. pp. 582-616. ISBN: 13: 9781599048994
- [7] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures. *Special Issue on Sensor Network Applications and Protocols*. Elsevier's Ad Hoc Network Journal.
- [8] Misra R, Mandal C. Ant-aggregation: Ant colony algorithm for optimal data aggregation in wireless sensor networks. In: *Proceedings of 2006 IFIP International Conference on Wireless and Optical Communications Networks*, Bangalore; 2006. p. 5. DOI: 10.1109/WOCN.2006.1666600
- [9] Camilo T, Carreto C, Silva JS, Boavida F. An energy-efficient ant-based routing algorithm for wireless sensor networks. In: Dorigo M, Gambardella LM, Birattari M, Martinoli A, Poli R, Stützle T, editors. *Ant Colony Optimization and Swarm Intelligence*. ANTS 2006. *Lecture Notes in Computer Science*. Vol. 4150. Berlin, Heidelberg: Springer; 2006. pp. 49-59. DOI: 10.1007/11839088_5
- [10] Maarouf I, Baroudi U, Naseer AR. Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks. In: *IET Communications*. Vol. 3, Issue. 5. IET. May 2009. pp. 846-858. DOI: 10.1049/iet-com.2008.0324
- [11] Naseer AR. Reputation system based trust-enabled routing for wireless sensor networks. In: *Handbook of Research on Wireless Sensor Networks*. USA: INTECH Open Access Publisher; 2012
- [12] Ganeriwal S, Srivastava MB. Reputation-based framework for high integrity sensor networks SASN '04. In: *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, October 2004. pp. 66-77. DOI: 10.1145 /1029102.1029115
- [13] Josang A, Ismail R. The beta reputation system. In: *15th Bled Electronic Commerce Conference e-Reality: Constructing the e-Economy*, June 17–19. Bled, Slovenia; 2002. pp. 1-14
- [14] Wenliang D, Jing D, Jonathan K, Yunghsiang SH, Pramod KV, Aram K. A pair wise key pre-distribution scheme for wireless sensor networks. *ACM Transactions on Information and System*

Security. 2005;8(2). DOI: 10.1145/1065545.1065548

[15] Sultana J, Ahmed T. Securing AOMDV protocol in mobile adhoc network with elliptic curve cryptography. In: 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, 16-18 Feb. 2017; 2017. pp. 539-543. DOI: 10.1109/ECACE.2017.7912964

[16] Sharma B, Madaan V. Enhancing security of MANETs by implementing elliptical curve based threshold cryptography. International Journal of Engineering and Computer Science. 2015;4(7):13346-13350. ISSN: 2319-7242

[17] Zhu L, Yang Z, Li M, Liu D. An efficient data aggregation protocol concentrated on data integrity in wireless sensor networks. International Journal of Distributed Sensor Networks. Vol. 2013. Hindawi Publishing Corporation. 2013. p. 1-9. Article ID 256852. DOI: 10.1155/2013/256852

[18] Elhoseny M, Elminir H, Riad A, Yuan X. A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. Journal of King Saud University – Computer and Information Sciences. 2016;28:262-275

[19] Temirlan I, Li Y. ECC-based user authentication scheme for wireless sensor networks. International Journal of Engineering Research & Science. 2017;3(6):21-28. ISSN: 2395-6992

[20] Udaykumar K, Thirugnanam T. Analysis of various clustering algorithms in wireless sensor network. International Journal of Computer Science and Information Technologies. 2015;6(2):1685-1691

[21] Thi PT, Mai BH, Tuan NT, Hung TC. Improving distributed energy efficient clustering algorithm to save

lifetime for heterogeneous WSN. International Journal of Computer Networks & Communications. 2017;9(4). DOI: 10.5121/ijcnc.2017.9407,81-96

[22] Kaur S, Mahajan R. Hybrid meta-heuristic optimization based energy efficient protocol for wireless sensor networks. Egyptian Informatics Journal. 2018;19:145-150, Science Direct Elsevier Publisher. DOI: 10.1016/j.eij.2018.01.002

[23] Zhang Y, Kuhn LD, Fromherz MPJ. Improvements on ant routing for sensor networks. In: Dorigo M et al., editors. ANTS. Vol. 3172. LNCS; 2004. pp. 289-313

[24] Neelima V, Naseer AR. SIBERXLP: Swarm intelligence based efficient routing protocol for wireless sensor networks with improved pheromone update model and optimal forwarder selection function. International Journal of Advanced Research. 2016;4(7):769-789. ISSN: 2320-5407

[25] Ducrocq T, Hauspie M, Nathalie N. Balancing energy consumption in clustered wireless sensor networks. International Scholarly Research Notices (ISRN) Sensor Networks. 2013;2013:314732. 14 p. DOI: 10.1155/2013/314732

[26] Xu Z, Chen L, Liu T, Cao L, Chen C. Balancing energy consumption with hybrid clustering and routing strategy in wireless sensor networks. Sensors. 2015;15(10):26583-26605. DOI: 10.3390/67s151026583

[27] Neelima V, Naseer AR. Impact of threshold energy control on energy conservation and balancing in Swarm intelligence based efficient routing for wireless sensor networks Proceedings of the World Congress on Engineering and Computer Science 2016 Vol I WCECS 2016, October 19-21, 2016, San Francisco, USA, ISBN: 978-988-14047-1-8 ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

- [28] Neelima V, Naseer AR. Energy conservation and balancing in swarm intelligence based efficient routing for wireless sensor networks. In: IAENG Transactions on Engineering Sciences. Vol. II. Publisher World Scientific; 2018. pp. 416-433. DOI: 10.1142/9789813230774_00 30
- [29] Neelima V, Naseer AR. SIBER-DELTA: Swarm intelligence based efficient routing with distance, energy, link quality and trust awareness for wireless sensor networks. International Journal of Scientific & Engineering Research. 2016;7(7):1598-1622. ISSN: 2229-5518, IJSER © 2016. Available from: <http://www.ijser.org>
- [30] Neelima V, Naseer AR, SIBER-DELTAKE NG. An improved ACO-KM-ECC based trust aware routing technique in WSN with optimal data resolution. Journal of Theoretical and Applied Information Technology. 2018; 96(20):6903-6925. ISSN: 1992-8645, www.jatit.org
- [31] Toy N, Senthilnathan T. Light weight authentication protocol for WSN using ECC and hexagonal numbers Ind onesian Journal of Electrical Engineering and Computer Science Vol. 15, Issue 1. pp. 443-450. July 2019. DOI: 10.11591/ijeecs. ISSN: 2502-4752
- [32] Park H-S, Lee J-S, Jun C-H. A K-Means-Like Algorithm for K-Medoids Clustering and its Performance. South Korea: Department of Industrial and Management Engineering, POSTECH; 2006
- [33] Miller VS. Use of elliptic curves in cryptography. In: Williams HC, editor. Advances in Cryptology - CRYPTO '85, LNCS 218. Berlin Heidelberg: Springer-Verlag; 1986. pp. 417-426
- [34] Moinet A, Darties B, Baril JL. Blockchain Based Trust & Authentication for Decentralized Sensor Networks. arXiv:1706.01730. 6, June 2017. arxiv.org
- [35] She W, Liu Q, Tian Z, Chen J-S, Wang B, Liu W. Blockchain trust model for malicious node detection in wireless sensor networks. Special section on mobile service computing with internet of things. IEEE Access Journal. 2019;7: 38947-38956