

Multi level trust calculation with improved ant colony optimization for improving quality of service in wireless sensor network

Ahmed Jamal Ahmed¹, Ali Hashim Abbas², Sami Abduljabbar Rashid¹

¹Department of Computer Engineering Technology, Al-Maarif University College, Ramadi, Iraq

²Department of Computer Technical engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Samawah, Iraq

Article Info

Article history:

Received Jan 28, 2022

Revised Nov 3, 2022

Accepted Dec 1, 2022

Keywords

Ant colony optimization

Clone attack

Multi level trust

Network security

Sybil attack

ABSTRACT

Wireless sensor network (WSN) is the most integral parts of current technology which are used for the real time applications. The major drawbacks in current technologies are threads due to the creation of false trust values and data congestion. Maximum of the concept of WSNs primarily needs security and optimization. So, we are in the desire to develop a new model which is highly secured and localized. In this paper, we introduced a novel approach namely multi level trust calculation with improved ant colony optimization (MLT-IACO). This approach mainly sub-divided into two sections they are multi level trust calculation which is the combination three levels of trust such as direct trust, indirect trust and random repeat trust. Secondly, improved ant colony optimization technique is used to find the optimal path in the network. By transmitting the data in the optimal path, the congestion and delay of the network is reduced which leads to increase the efficiency. The outcome values are comparatively analyzed based the parameters such as packet delivery ratio, network throughput and average latency. While compared with the earlier research our MLT-IACO approach produce high packet delivery ratio and throughput as well as lower latency and routing overhead.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ahmed Jamal Ahmed

Department of Computer Engineering Technology, Al-Maarif University College

Ramadi, Al-Anbar, Iraq

Email: ahmed.jamal@uoa.edu.iq

1. INTRODUCTION

In recent times, wireless sensor networks (WSNs) have sparked increased interest in both general theory and behavior modeling. A WSN is comprised of a more sensor nodes that are often effectively deployed in a specific geographical area in gathering data of interest, which is collected from the source nodes and sent to a base station (BS) via multi-hop communication. The sensor nodes are cost effective, low powered, limited irreplaceable source of energy as well as randomly localized. In general, the communication capability of the sensors is low so a highly effective highly stable routing becomes essential [1]. Due to its other properties of huge, self-organization, frequent topology, and finite resources, wireless sensor network is extremely prone to a range of assaults. WSN threats can result in system abnormalities, which can be seen in the information recorded from the infrastructure. The information gathered is significant which can be used to spot malicious activity. This information is organized as protection info, because they can assist us through detecting abnormalities and determining cyber threats, invasions. Various types of sensor network applications such as smart city, home automation, and smart medical can create security data [2]. Energy efficiency conservation

(or prolonged lifespan of the network), accessibility, and connection, are all essential quality of service (QoS) requirements. In commodity sensor networks, meeting those criteria is difficult. Additionally, various kinds of faults are detected for the sender node failure. One such kind is active DoS attacks such as wormhole attack, vampire attack, jamming attack, Sybil attack and clone attack [3].

As seen above, sensor nodes collect a lot of information from the sensing area. In such commodity networks, transmitting quite a high quantity of data through the network ends up with variety of issues, including low QoS, i.e., delay, bottleneck, speed, and privacy. They have poor memory, computation, and network control, as well as an irreversible form of energy [4]. Several studies concentrate on providing an answer with efficient routing efficacy and network connectivity due to poor connectivity and restrictive limits of edge devices. However, due to the introduction of huge dynamic and varying changes in the network architecture in most of the cases the packet delivery ratio and the throughput of the network is reduced. Similarly, reliable data transmission needs to pay more attention to secure the network [5].

Furthermore, existing trust based on topology control and time synchronization protocols suffer large control overheads in trust estimation and propagation, resulting in a high number of dead nodes and high route instability due to the topology control route discovery mechanism [6]. In some cases, flooding takes place which becomes an ordinary issue in network security. In WSN several intrusion detection techniques are available to secure the network from attacks but fail to improve the overall performance of the WSNs. Even in those trust-based intrusion detections process few drawbacks are addressed. In order to find the false trust values and dishonest node recommendations few processes are needed. At the initial stage, each node consists of trust values which variable in nature and uncertain. Few nodes will maintain low trust score because of poor connectivity it may not be a malicious node. During the process of communication, the attackers also will send false messages. So, it is very essential to build a network with high security [7], [8]. So, a highly defensive modern network with new security requirements is essential to overcome the network from such attacks [9], [10].

The main objectives of our research work presented in this paper is:

- a) The paper proposes an efficient routing model to overcome the network from attacks, congestion and delay.
- b) The major attacks which are taken into account are sybil attack and clone attack.
- c) To provide better accuracy than the earlier works multi level trust calculation is concentrated.
- d) As so to reduce the network delay optimal path finding is done by using improved ant colony optimization (IACO).

The organization of the paper is listed as follows. In section 2, we study about the earlier work in the area of trust based WSN networks and optimization based WSN networks. In section 3, the localization of the nodes in the network, and the concept of sybil as well as clone attacks are discussed. In section 4, energy calculations, attack models and the concepts of multi level trust as well as ant colony optimization algorithm are elaborated. In section 5, the proposed multi level trust with improved ACO model summarized. In section 6, the simulation for our model is performed and the results are compared with the earlier methods.

2. COMPREHENSIVE SURVEY

2.1. Trust oriented wireless sensor networks

Khan *et al.* [11] suggested a well-organized integrity assessment-based routing algorithm for networks that includes a multi-trust method to mitigate malicious activities such as slandering, Active attacks, preferential relaying, sinkhole, and gray-hole threats. It uses a trust formula based on the stochastic process since the restoration of trust levels under assault is quicker in the Gaussian and other distributions. Liu *et al.* [12] WSN based medical and environmental based vulnerabilities are taken into consideration. This method provides good results in terms of efficiency and security. However, the throughput achieved by this method is moderate.

Srividya and Devi [13] the author introduced a strategy named ECPSO-PCM which concentrates on PSO optimization, clustering and trust management. The residual energy and spatial correlation-based clustering is used then trust based CH selection is introduced. However, the throughput achieved by this method is moderate. Yang *et al.* [14], as so to improve the security and data collection capacity the light weight security protocols are introduced. This method produces more security and efficiency. However, throughput and bandwidth utility are low.

Shahid *et al.* [15] the author presented a multi objective model which is cellular automata with trust based malicious activity measurements in WSN. The proposed trust based cellular automata achieves higher efficiency comparatively. Anyhow this method creates more delay and overhead. Fang *et al.* [16] hierarchical routing protocol is used in WSN. The trust management is introduced to protect the network from the internal attacks. With the help of this method the energy consumption and packet loss during the process of communication is reduced. Rouissi *et al.* [17] author proposed a LEACH based trust management to improve the efficiency and security of the WSN network by protecting the network from the misbehavior caused by the

internal attacks. High efficiency is achieved but the number of nodes used in the network is low. This method is not suitable for the network with huge number of nodes in it.

2.2. Optimization in WSN

Mohamed *et al.* [18] innovated coyote optimization based on a fuzzy logic (COFL) algorithm is used to introduce a different clustering method for heterogeneous WSNs. It employs the conjunction with the fuzzy logic (FL) system to optimize the clustering method in order to extend the lifetime. Kaur and Kumar [19] suggested a multi-objective ant-colony-optimization based QoS-aware cross-layer routing (MACO-QCR) protocol to overcome the transportation problem. This method reduces the delay and network congestion. However, it consumes more energy.

Han *et al.* [20] hybridization of PSO-ABC finite volume approach was used to progressively improve the surface performance of a bike's disc rotor, and the parameter estimation model was confirmed using WSN. To test the optimum impacts of a suggested PSO-ABC hybrid algorithm within a week of simulation analysis, the method was applied with the classic PSO and ABC frameworks.

Sabella *et al.* [21] krill herd (KH) meta-heuristic method was used and hence option was chosen to locate non-anchor nodes utilizing mobile cluster centers. To discover the locations of semi nodes, mobile anchor nodes have GPS systems and communicate the exact position at fixed time intervals. This method reduces the energy consumption but it produces more networks overhead. Qasim *et al.* [22] enhanced ant colony optimization is developed. The experimental results demonstrated that the proposed algorithm outperforms the traditional ACO in terms of complexity. The Dij-Huff Approach is proposed in this study as a secure and energy efficient method of optimization (DHM) which leads to improve the accuracy and efficiency of the network.

Habelalmateen *et al.* [23] introduces heat deteriorated techniques using clusters, with encryption private protection. Cluster formation techniques, is from the other hand, cause traffic, and problematic owing to the self-organized topology. As a result, the broadcaster's performance will suffer. The Dij-Huff approach is adopted in this research as a reliable and energy effective approach of refinement. Xin *et al.* [24] suggested improved DV-Hop technique based on hybrid anchor node meant to enhance positioning accuracy. To begin, the nodes choosing are generalized into an optimization problem. The dynamic anchor node set (DANS) is then constructed using the binary particle swarm optimization (BPSO) algorithm, and the placement is performed on the DANS. It creates more overhead during the process of communication.

Al-Kaseem *et al.* [25] the emphasis of this research for data access control and multimodal processing and transmission. An irreconcilable optimal solution is initially defined based on numerical models of the two risk controls, with several concerns such as data usefulness, energy usage, response time, and information leakage rate. Rashid *et al.* [26] and Abbas *et al.* [27], the authors proposed firefly optimization and multi-objective optimization algorithms. The performance is good. The only drawback is it produces more routing overhead. From the earlier study it is understood that in the earlier researches in main demerits of the WSNs are congestion, packet loss due to lack of security. The proposed MLT-IACO protocol is designed in the way to overcome these drawbacks.

3. PRELIMINARIES

3.1. Exploitation of node in network

Initially, a set up is made as multi-hop sensor network in a two-lateral space, assuming that perhaps the local sensor node placements are stable or fluctuating slowly. Every sensor network seems to have the same communication range G and transmits at the same energy 'E'. The network packets will be finally obtained if the detected signal's intensity is higher than that of the input power criterion.

Initially, the network is created by utilizing the graph 'K' where $K(D, F, G, y(x, y) \in D)$, the notations can be explained as follows, D represents the edges, F represents the number of nodes in graph K, G_x, y represents the description link (x, y) with the delay and bandwidth ranges. $F \in V$ indicates the source available in base station and $R = \{r1, r2, r3 \dots rn\}$ indicates the multicasting process. So, it is significant to construct the graphs $K = (F, D)$ with the representation of 'F' number of nodes and 'D' communication links. This construction is made for the sensor nodes namely $n1$ and $n2$ and hence the transmission range can be chosen between $n1$ and $n2$ for undirected graph.

Presumption is made that $(K, G - ID)$ is an existing multichannel broadcast demand notation, wherein G denotes the source node and $G - ID$ denotes a set of multiplex reception networks 'N', namely, all multichannel recipients share the very same $G - ID$. Initially, all the available nodes send out a "HEL-meg" on such a regular basis to communicate properly among the multicast team members, by using $G - ID$. If the operations to achieve to record the data of its multicast group mates, it will also have sent out such message "HEL-meg". Following the startup stage, the node receives the data of all available members of its present

distributed network of neighbor nodes. Every node keeps a table of neighbor records and times stamp of each entry in the table. It will scan the neighbor table according with ID of every node by using "HEL-meg". If it's a new neighbor, the list will be updated with fresh content. If the neighbor is known, the entry times stamp will indeed be amended. To prevent from the feting the data, the sensor node sets a timeout; were, the outstanding data entries along with neighbor table within short time. It can also be used to dynamically build connectivity and manage the participants of a distributed network, lowering the absolute complexity of the routes and increasing flexibility. The multichannel base station will transmit a multicast query ($K, G - ID$) when it wants to deliver a warning. The multichannel base station will disseminate the packet whenever it has data to broadcast. Whether a node is a multicast receiver or not, when it gets the signal join reply, it checks to see if it is the next node designated by the signal join reply. If it is, it determines that being on the way to the intermediate host and, at the same time, declares itself as something transceiver of the present broadcast event. The packet joins reply travels thru the allocating resources until it finds the source node via the reverse path of the comparable packet join query.

3.2. Sybil attack

The sybil attack involves altering network equipment in order to disrupt data transmission. A sybil node, specifically the sybil node, falsely claims many credentials and adopts assault to get different benefits, such as access to unauthorized supplies, hurting user confidentiality, broadcasting misleading control messages, and publicizing the private information. A sybil node can engage in information systems in the very same manner as a quasi node since it possesses genuine information. As a result, sybil nodes may execute a range of assaults, making them more and more dangerous.

3.3. Clone attack

The sensor module is susceptible to the clone attack, which really is a serious threat. This strategy aids in the detection of cloning assaults that occur in networks. There are a variety of logically centralized detection methods clones in sensor nodes using pseudorandom pre allocation, sensing node replicas; real-time sensing of clone attacks, centralized node replication attacks detection, compressed sensing-based clone recognition, and fast detection of replica node attack in mobile sensor networks using sequence analysis.

4. PROPOSED METHODS

4.1. Energy representation

All the nodes in multi-hop wireless sensor network are battery energizes and hence calibrating the consumption of energy is significant. It consists of two phases such as generation part and absorption part as indicated in (1). In (2) the notation $E(h, k)$ indicates the average energy consumed to transfer the data for the distance 'x', the notations h, k represents the energy consumption rate of 'l' data bits. By chosen the source and destination node properly the model can be fixed. In (3), the notations $E(k)$ represents the energy consumed during transmission of data, $Et(h)$ represents the total energy required for transferring a data with the time 'n'.

$$E(h, k) = Ener_{cons}(h) + Ener_{trans}(h, k) \quad (1)$$

$$E(k) = Et(h) = k \times Trans_n \quad (2)$$

$$Rem_{ener} = Avail_{ener} - Consum_{ener} \quad (3)$$

4.2. Attack model

A hacker can interrupt the algorithm's functionality by launching assaults at several phases of the study, which including acquiring location data, estimating distance between nodes, and verifying the predicted area. These threats can be carried out by either internally or externally. They are constructed with the ability to sum up both the sensor and tampering nodes. The purpose of the adversary is to achieve the location of node and forge the actual uniqueness of the nodes. An attacker can perform the following behavior to benign nodes:

- a) The consolidated amount of hacker nodes can be representing as 'malic' where ($k = 1, 2, 3 \dots \dots l \ll m$) numbers are representing as 'malic'
- b) Significant beacon nodes have the chance to ping the irregular position report deliberately to its intermediate node as indicated below

$$pack_{false} = \{iden, loc(c), timelapse(t), res_{ener}\}$$

- c) There is possibility of ‘malic’ nodes n particular area to contact with adversary nodes
- d) ‘malic’ nodes can specifically tamper the incoming packets in the network
- e) Selfish adversary nodes can distribute wrong information regarding energy
- f) ‘malic’ node knowledge fully replicates the false reputation score about intermediate nodes.

4.3. Proposed multi level trust in routing:

The suggested method can be divided into three parts: (1) threshold-based trust evaluation and (2) beacons based indirect trust calculation and (3) random repeat trust evaluation. The trust value of anchor node is measured in the first segment using both of the direct trust and indirect trust. The trust values are checked in section 4.1 to minimize malicious activity by attacks.

4.3.1. Evaluation of trust value

The trust value (trust_v) of every node can be set as 0.5, where the trustworthiness start forms this range threshold. The value of trust_v can be calibrated by using the parameters such as integrity, reputation state, residual energy and trust provider unit. By calibrating these parameters, the average trust (avg_trust) can be find out. It is significant that, every node should maintain two counts such as X_count and Y_cout under positive and negative cases correspondingly. The initially count for these cases in zero and hence the illustration is shown in Figure 1.

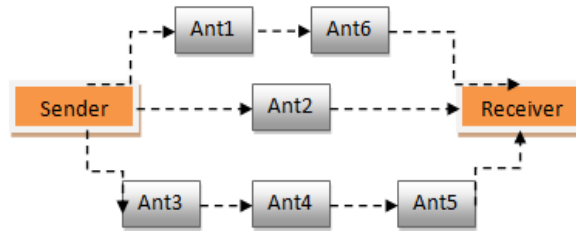


Figure 1. Structure of ants

4.3.2. Direct trust value evaluation

All the beacon nodes forward the data, say (data_i) to all its intermediate nodes by calibrating the distance Dis_i with the speed spe_i by coordinated nodes correspondingly. For communicating properly, the free space renovation model is utilized and hence the receiver model can be calculated mathematically in (4).

$$prop_R = Prop_{tran} \times Gain_{tran} \times Gain_{recei} \times \frac{\nabla}{4 \times \pi * D} \quad (4)$$

The above notations ‘prop_R’ indicates the total power transmitted and received by all beacon nodes, Prop_{tran} represents the transmission power, Gain_{tran} represents the gain of the transmitter, Gain_{recei} represents the gain of the receiver, ∇ represents the wavelength range with the distance D. Where, the notation ‘r’ is a constant parameter, ‘D’ represents the distance among sensor nodes. The reputation scores can be calibrated for all the beacon nodes and it is mathematically expressed in (6):

$$D = r / prop_R \quad (5)$$

$$R(s + 1) = \Omega \times R(s) + (1 - \Omega) \quad (6)$$

Where, the notations R (s+1), R(s) indicates the reputation score for the beacon node with the time interval ‘s’. It is mandatory to fix the threshold range of 0.5 to all the nodes in the network for calibrating the weight. Initially, all the residual energy are same for the nodes hence the counts such as Pcount and Ncount initiate to record the process for broadcasting and then the increment process will begin with the assistance of tampering. Once reaching the threshold value the tampering process can be stopped with the finalization of residual energy in (8).

$$\Omega = \frac{H(i,j) - J(i,j)}{G(i,j)} \quad (7)$$

$$Ener_resi \geq Ener_thres \quad (8)$$

From the above equation $Ener_thres$ indicates the threshold energy range. By checking the above equation; we can decide whether the Pcount or Ncount can be incremented. Finally, the energy parameter is finalized for all the malicious nodes with the consideration of beacon node energy parameter. As a result, y considering Pcount and Ncount the beacon nodes are deciding with the calibration of trusted weight (wei_{trust}) and weighted expectation (wei_{exp}). The values for wei_{exp} and wei_{trust} indicates the importance of specific trust parameter which is calibrated and it is mathematically expressed in (9):

$$wei_{trust} = \frac{Pcount(wei)}{\sum_{i=0}^4 Pcount(wei)} \quad (9)$$

wei_{exp} Finalizes the importance of beacon by elaborating the trust parameter (Pi) and hence the calibration is.

$$wei_{exp} = \frac{Pcount+1}{Pcount+Ncount+2} \quad (10)$$

Here, the wei_{exp} and wei_{trust} should have the range between [0,1] due to elaborated trust and hence the equation is given as follows,

$$Dir_{trust} = \sum_{i=0}^4 wei_{trust} * wei_{exp} \quad (11)$$

The consolidated value for the Dir_{trust} ensures the trust value for all the beacons and hence it must be higher than 0.5, that indicates the begin node or else, it is malicious node. These nodes can continuously monitor and set to the counts between the range 0 and 1.

4.3.3. Validation of indirect trust value:

The $indir_{trust}$ can be calibrated in the case of proper relation between the beacon nodes; this is due to the improvidence to find the trust of participant nodes. This direct trust can be calibrated by presenting the information's deliberately in second hand manner. Consider the beacon node 'beac_node' has the direct contact waiting beacon node 'a', which also have the second-hand details regarding the node 'b'. The positive and negative experiments of P'count and N'count can be given as follows,

$$indir_{trust} = \sum_{i=0}^4 \frac{P'count(i)}{P'count+N'count} \quad (12)$$

Where, the notations, $indir_{trust}$ = indicate the indirect trust value of the final beacon node. Pcount (i) can be increments with respect to the trust value k which must be higher than 0.5. As a result, boot the direct and indirect trusts can be combined to find the final value as given below and, in the (13) both of the wei_{dir} and wei_{indir} should be equal to 1. The reason for introducing the trust factors is to reduce the impact of wrong trust value. The role of random repeat trust calculation begins at the end of evaluating trust values.

$$trust = wei_{dir} \times Dir_{trust} + wei_{indir} \times indir_{trust} \quad (13)$$

4.4. Random repeat trust

The determination of a reliable neighbor node enabled the technique to be completed from start to finish. The hop-based delay and the payloads used to transmit files were both affected. The time will vary depending on the distance between both the sender and recipient. The journey duration is equivalent to the latency at the packet's endpoint. The end-to-end transmission latency would rise as the network frequency increase. The route duration and network congestion are finished if there is a significant coupling among either. The grading length is obtained together with the reactive routing assessment from the generator of every node in the proposed approach. The most reliable nearby node is a compact, genuine component with a short range. Messages will be sent instantly to the destination point after node details have been received. As a result of the time savings, electricity is produced. This one-of-a-kind node sends the message to the network on a regular basis. As the data arrive, each node broadcasts its internal records. The target node modifies its immediate neighbor's table based on the messages it receives from its neighbors. The existence of the association and the predicted bandwidth of the adjacent nodes were determined using similar data. After determining the shortest least traffic path, the data will be sent directly from the source node to the destination node.

Algorithm: Authentic node detection using random repeat trust for efficient categorization and detection process.

Input: set of channels and nodes

Output: Detected malicious nodes and trust range of each neighbor node

Step-1: calibrating the trust value

$$Tr_{neigh} = Ener_{node} + Tr_{neigh} \quad (14)$$

$$\text{Where, the notation } Ener_{node} = \frac{\text{summation of Pack}_{rx} + \text{summation of packet tx}}{\text{set of nodes}} \quad (15)$$

Step-2: Find the distance (D) between each node for calibrating the trusted categorized value

$$D(a, b) = \sqrt{wei(a, 1) - wei(b, 1)} \quad (16)$$

By utilizing (16), the features of all the parameters can be calibrate for both the authentic and malicious nodes. Step-3 Calibrate the abnormal rate of the malicious node. The abnormal rate of the malicious node is calculated using the mobile state and it is mathematically expressed in (17).

$$Abno = (Wei_{fea(D)}) \quad (17)$$

Where, the notation 'Abno' indicates the abnormality of the malicious node in mobile state. By using the trust value, the mode of authentic nodes can be signified. Step-4 finding the overall trust value for neighbors and it is mathematically expressed in (18) using this calculation the trust score obtained for all the nodes in the network.

$$Neigh = Wei1_{con} + Wei2_{dp} + Wei3_{resEner} + Wei4_{cha} \quad (18)$$

4.5. Improved ant colony optimization

Activity of ant is basically a meta-heuristic that deals with most general problems. To begin with, ants leaving their colonies in looking for food are a circumstance locally. When selecting a static endpoint, the hormonal aroma of certain other ants would lead them down the same way, accessing them to release a chemical substance called fragrance. Sometimes ant's subgroup can place in route static position chosen way, where all the links are coated with pheromone, makes to transfer the nest in attractive manner. When the pheromone in the hyperlink disappears after one certain amount of time, some more ants can be finding. The pheromone concentration and discrete time pheromone fragrance starts to evaporating at a specific moment. As we connect all the ants to work together, there seem to be network alignments of autonomous systems that can continue to operate. Each ant in the system can take either static or dynamic shape. Whereas, the nodes in the nest wish to associate ant's place. This comparison is much more durable and applies to all ad hoc networks that are linked from a viewpoint. Between the investigation and utilization of any shared data, a probabilistic data transfer network is extremely important. However, above mentioned difficulties are critical to the opposing meta-heuristic methods. Quest attractive untapped regions of space exploration are options while extending exploitation and effectively in the search for good solutions. The ants found an excellent answer by reinforcing the synthetic pheromone in previous operations. Nevertheless, to make it easier to strengthen the focal point, by maintaining the search space diverse, the relevant strategies were proposed. The structure of ant communication is shown in the Figure 1.

- a) All ants have its own trail pheromone mode in exponential manner
- b) Creating random way with processors

The amount of pheromone is stable sanction and it actually coincides with the pheromone path by the entire way is observed in the incremental manner. Finally, the quantity of pheromone is signified as (n, m).

$$\Omega(n, m) = \beta \cdot \Omega(n, m) + \mu \cdot \Omega(n, m) \quad (19)$$

Where the notations, β represents the evaporated pheromone unit with the range of 1. This range is fixed with the probabilistic way (n, m) and it is mathematically expressed in (20):

$$Prob(n, m) = \frac{\beta(n, m) \cdot \epsilon(n, m)}{\sum(n, m) \beta(n, m)} \quad (20)$$

Initially, set the exact points for ant's travel form source to destination using pheromone level and the set of possible routs can be given ad 'J'. As a result, the characteristics of routing optimization can be given as

follows: (i) Multicast route for data transfer can be adaptive nature; (ii) Active mode of data is significant; (iii) All the nodes are computed with behavioral components.

5. MULTI LEVEL TRUSTS WITH IACO OPTIMIZATION (MLT-IACO)

The proposed MLT-IACO is the combination of trust and optimization method which is developed to improve the effectiveness of the WSN communication. The architecture of multi level trusts with Improved ACO is shown in the Figure 2. The energy-efficient base station randomized trust-based networking is built in a safe and randomized routing mode that displays all outputs and provides useful load distribution. The effectiveness of the IACO algorithm employing this improved route selection is included with multi level trust details.

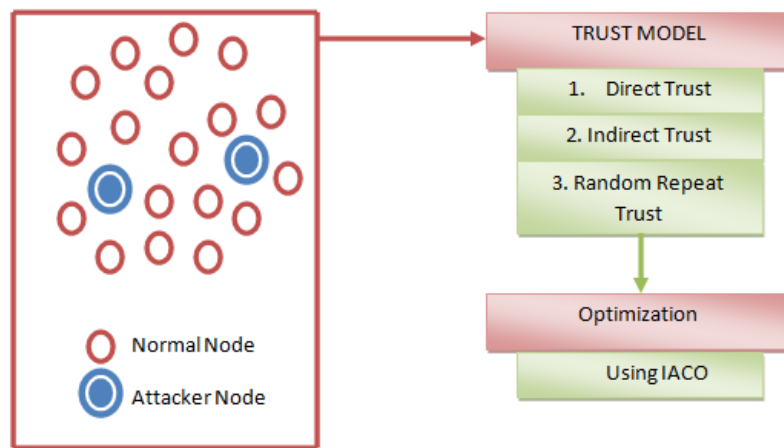


Figure 2. Architecture of the MLT-IACO approach

The developed scheme IACO high ranking range depending on resilient approach is the major use of this technique quickly while evaluating networking rates for various results. IACO begins at the central ends nodes if a broadcast request is not initiated. This approach uses the ant density method, which is a variation ant system. Whenever the base networks are chosen, the next node is chosen depending on the distance and pheromone concentration stochastically. The fitness calculated in the parameter for combining the energy levels is routed to identify the node using the IACO approach. The IACO on-demand routing method was started with route transmission. The network's first nodes are sized based on the projected size. The uniform distribution function is based on ants that are dispersed throughout the nodes. Each ant has a tabu list to keep track of its node moving network point. Tabu list search node size for fixed space. The Ant that is now on the primary node is added to Tabu's list. The ant movement is encouraging the fitness to the best competition by identifying the exercise values of all unused terminals on the network.

By considering the set of ants (A) in the network 'n' with the probability 'p' the equation is given as follows:

$$P(n, m) = \frac{\beta(n, m)(t) \cdot \Omega(n, m) \cdot \epsilon m}{\sum_{j=1}^n \beta(n, m)(t) \cdot \Omega(n, m) \cdot \epsilon m} \tag{21}$$

Where the notations, $\beta(n, m)$ represents the quantity of the pheromone, (n, m) represents the charging of node, $\Omega(n, m)$ indicates the adaptability of the node for the threshold values The fitness function can be calibrated in the equation (22) and the notations such as represents the end to end delay for the opted route, represents the average delay of all calibrated routes, represents the standard deviation parameter with the N number of hops to reach the destination. Here, a new parameter ψ interprets the distance between the nodes and repute delay is expressed in the equation (23) and the notations indicates the average trust value distance between the source and destination and the represents the power parameter between source and destination.

$$Fitness_x = \frac{end(i) - \delta}{\phi} \cdot N \tag{22}$$

$$\psi = \frac{PDR}{tr(sor-des)*pow(sor-des)} \quad (23)$$

6. SIMULATION SCENARIO AND PARAMETERS

In the section, the WSN network performance is analyzed using our simulation scenario as well as the predefined parameter details are shared in the Table 1. In order to calculate the impact of the proposed methodology, several experiments are taken on behalf of number of nodes in the network and transmitted data rates. The simulation is done using the number of nodes in the range of 100 as well as the fixed transmitted data rates are 1 sec to 5 sec. As so to perform numerical calculations, in this research we used network simulator NS2 software in the version 2.34. The final trust value of the network nodes helps to measure the successful and failed transmissions. The trust value of the node varies from 0 to 1. The value 0 represents the untrusted node and the highly trusted node which maintains the value of 1. To validate the network performance of the proposed methodology we used some metrics and are compared with the earlier works such as FTM-ABC [28], TDB-MDP [29] and MTE-TEAM [30] protocols and those parameters are packet delivery ratio, network throughput and end to end delay of the network.

Table 1. The simulation parameter details for MLT-IACO

Parameters	Values
Simulator	NS-2.34
Simulation period	500 ms
Coverage area	1000*1000 m ²
Transmission range	300 m
No of nodes	100
Network interface type	WirelessPhy
Standard	IEEE 802.11
Propagation model	Two ray propagation model
Antenna	Omni-directional antenna
Node's transmission range	15m to 20m
Traffic type	CBR
Control messages	30 bits
Initial power	1000 Joules
Transmission power	0.05 Joules
Reception power	0.02 Joules
Payload size	512 bytes
Agent type	TCP

The performance analysis is divided into two scenarios and the results are calculated. The scenarios are parameter analysis based on number of nodes and Parameter calculation with and without the attack. The scenarios are explained in detail in the section 6.1.

6.1. Parameter analysis based on number of nodes

6.1.1. Packet delivery ratio (PDR)

This parameter is one among the primary prerequisite parameter to measure the performance of the network. It is defined as that of the ratio of packets which gets transmitted at first to the destination node to the number of packets anticipated to get received by the destination node. The parameters show the clear-cut view of the data transmission most significantly. Figure 3 shows the outcome comparison of PDR. Here the proposed model MLT-IACO protocol is evaluated and compared with the earlier approaches like FTM-ABC, TDB-MDP and MTE-TEAM protocols. From the graph it is understood that our proposed method reached high PDR ratio while compared with the other earlier models such as the PDR achieved by the FTM-ABC, TDB-MDP and MTE-TEAM protocols are 76.165%, 84.278% and 89.421% where the MLT-IACO protocol achieved upto 97.242%.

6.1.2. Average latency

The parameter is termed as that the transmission length process, which the time taken to transmit the information from the sender node to the receiver node for the overall network. This calculation is performed at the end of the simulation. Figure 4 shows the result comparison of AL of our work with the earlier works such as FTM-ABC, TDB-MDP and MTE-TEAM protocols. From the graph it's clearly shown that our proposed MLT-IACO protocol process very less latency when compared with the other earlier works. The latency produced by the FTM-ABC, TDB-MDP and MTE-TEAM protocols are 321.18ms, 288.13ms and 253.44ms where the MLT-IACO protocol produces 112.46ms.

6.1.3. Network throughput

It is the calculation of average number of packets transmitted from source to the destination during the process of data transmission to the overall simulation. The unit of throughput is Joules. Figure 5 shows the throughput calculation of the proposed work compared with some earlier works. When compared with earlier approaches like FTM-ABC, TDB-MDP and MTE-TEAM protocols our MLT-IACO protocol produced high throughput during the process of communication in the network such as the throughput achieved by the FTM-ABC, TDB-MDP and MTE-TEAM protocols are 235.89Kbps, 285.79Kbps and 321.89Kbps where the MLT-IACO protocol achieved upto 424.68Kbps. By calculating all these results, we came to know that MLT-IACO protocol is very stable which leads to improve the QoS of the network.

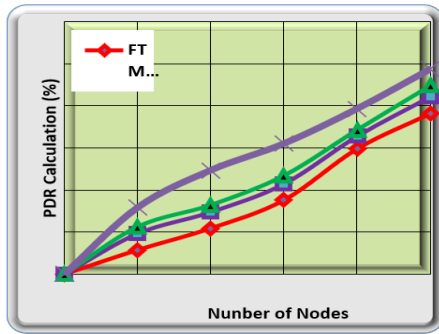


Figure 3. Packet delivery ratio calculation

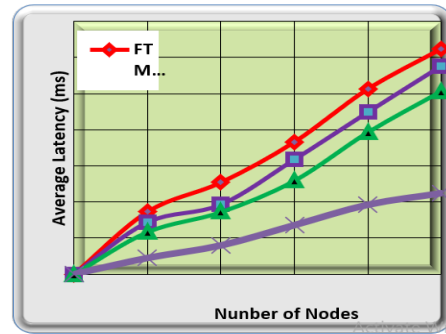


Figure 4. Average latency comparison

6.1.4. Energy efficiency

Calculation of energy efficiency is the most important part to improve the overall performance of the network. Figure 6 show the energy efficiency calculation of the proposed MLT-IACO and it is compared with the earlier approaches like FTM-ABC, TDB-MDP and MTE-TEAM protocols. In the proposed method, multilevel trust with improved ACO optimization is used. Improved ACO is employed here to find the optimal path in the network that reflects in the reduction of the energy consumption that leads to improve the efficiency of the network. The efficiency achieved by the earlier works like FTM-ABC, TDB-MDP and MTE-TEAM are 63.44%, 75.18% and 81.26% respectively whereas the proposed MLT-IACO achieved 93.14% which greatly helps to improve the overall performance of the network.

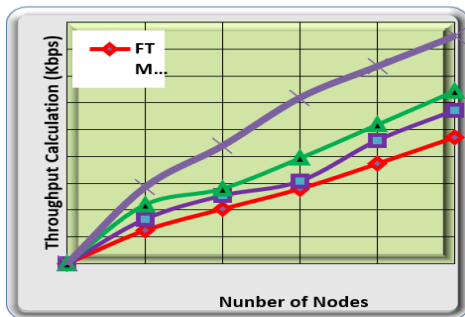


Figure 5. Network throughput calculation

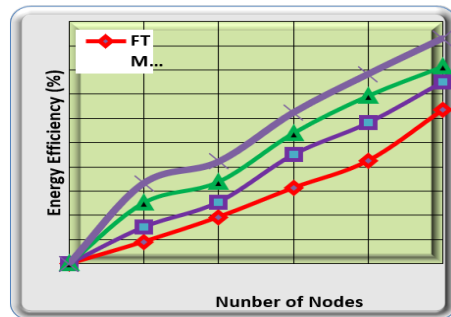


Figure 6. Network efficiency calculation

6.1.5. Network overhead

During the process of communication in maximum of the cases retransmission occur due to congestion. To overcome that in the proposed MLT-IACO method Improved ACO is used. Figure 7 show the overhead calculation of the proposed MLT-IACO and it is compared with the earlier approaches like FTM-ABC, TDB-MDP and MTE-TEAM protocols. Through optimization congestion is reduced in the proposed network that reflects in the reduction of overhead in the network. Hence the overhead produced by the earlier works like FTM-ABC, TDB-MDP and MTE-TEAM is 5468 packets, 4289 packets and 2967 packets

respectively whereas for the proposed MLT-IACO it is 1867 packets only which is around 1000-3500 packets lower than the earlier works.

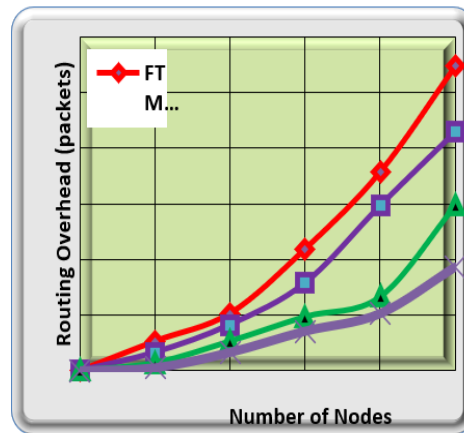


Figure 7. Network overhead calculation

6.2. Performance analysis of with and without attacks of the MLT-IACO method

To calculate the performance with and without attacks the parameters which are considered are packet delivery ratio, network latency and packet loss. The calculation and discussion of these parameters are given below from Figures 8 to 10. The performance variation of the parameters according to the activities of the malicious nodes are calculated in the elaborated manner.

6.2.1. Packet delivery ratio calculation

The performance of proposed MLT-IACO method's packet delivery ratio is analyzed with and without the presence of attacks and it is described in the Figure 8. The performance is 99.99 percent achieved by the proposed MLT-IACO method without attacks and in average it reached up to 97.5% with the presence of attacks. The accuracy that the proposed MLT-IACO method reached high when compared with the other methods. Due to the process of multi level trust in the proposed method the security is very high that reduce the message loss due to attacks during the process of communication that reflects in the increase of packet delivery ratio.

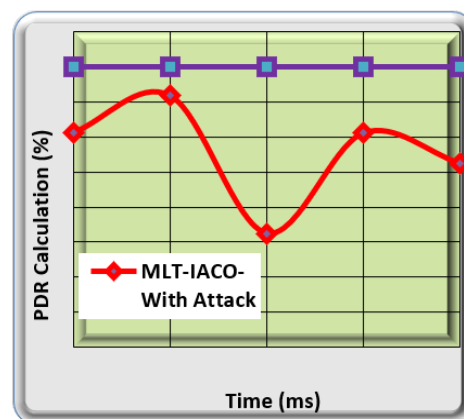


Figure 8. Packet delivery ratio calculation

6.2.2. Network latency calculation

The performance of proposed MLT-IACO method's latency is analyzed in terms of (ms) for with and without the presence of attacks and it is described in the Figure 9. The average latency is minimum 100ms

during the presence of attacks for the entire data communication in the network. This is mainly achieved by using the IACO concept in it. The latency created by the attacks is easily monitored at managed by the proposed methods. The average latency produced by the network with attacks is 36ms and without attack is 14ms which are very close values.

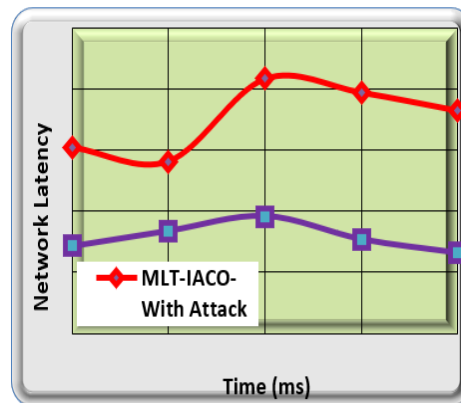


Figure 9. Network latency calculation

6.2.3. Packet loss calculation

The packet loss produced in the network with attack is very much close to the network without attack which is shown in the Figure 10. In it completely achieved by using the multi-level trust method which consist of direct trust, indirect trust and random repeat trust. Trust in again in these three levels that results in the reduction of packet loss in the network. The calculated packet drop of the network without attacks is 85 packets and with attacks are 102 packets which are very close and no bigger difference.

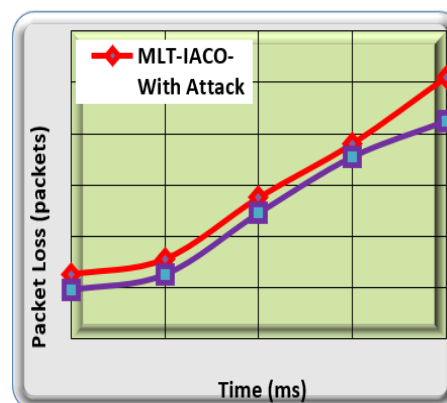


Figure 10. Packet loss calculation

7. CONCLUSIONS

In major drawbacks in the WSNs are congestion due to huge usage of sensor and security. In this research work, we introduced a multi level trust model with improved ACO to protect the network from malfunctions as well to improve the overall QoS of the network. By using various parameters in multi levels the trust values are calculated for the nodes in the network. So, the results calculated by our trust model are more accurate when compared with the other earlier works. In other side by providing the optimal path using improved ACO the overall performance of the network is improved. The simulation is done and the test results are compared with the earlier works FTM-ABC, TDB-MDP and MTE-TEAM protocols. The results indicate that our MLT-IACO achieves superior results when compared with this earlier works. Our protocol MLT-IACO provides more than 95% accuracy in data transmission with large throughput utility and low latency. In

the future work, we are interested to utilize our technique cluster-based environment and to add some validation methods to it.

ACKNOWLEDGEMENTS

This work was supported and funded by Al-Maarif University College under Grant (DCT-03).




REFERENCES

- [1] A. Salim, W. Osamy, A. Aziz, and A. M. Khedr, "SEEDGT: Secure and energy efficient data gathering technique for IoT applications based WSNs," *Journal of Network and Computer Applications*, vol. 202, p. 103353, Jun. 2022, doi: 10.1016/j.jnca.2022.103353.
- [2] F. Alcaraz Velasco, J. M. Palomares, and J. Olivares, "Lightweight method of shuffling overlapped data-blocks for data integrity and security in WSNs," *Computer Networks*, vol. 199, p. 108470, Nov. 2021, doi: 10.1016/j.comnet.2021.108470.
- [3] R. Bhatt, P. Maheshwary, P. Shukla, P. Shukla, M. Shrivastava, and S. Changlani, "Implementation of fruit fly optimization algorithm (FFOA) to escalate the attacking efficiency of node capture attack in wireless sensor networks (WSN)," *Computer Communications*, vol. 149, pp. 134–145, Jan. 2020, doi: 10.1016/j.comcom.2019.09.007.
- [4] R. Alturki *et al.*, "Sensor-cloud architecture: A taxonomy of security issues in cloud-assisted sensor networks," *IEEE Access*, vol. 9, pp. 89344–89359, 2021, doi: 10.1109/ACCESS.2021.3088225.
- [5] L. Zhiqiang, G. Mohiuddin, Z. Jiangbin, M. Asim, and W. Sifei, "Intrusion detection in wireless sensor network using enhanced empirical based component analysis," *Future Generation Computer Systems*, vol. 135, pp. 181–193, Oct. 2022, doi: 10.1016/j.future.2022.04.024.
- [6] S. K. Sahu, D. P. Mohapatra, J. K. Rout, K. S. Sahoo, Q.-V. Pham, and N.-N. Dao, "A LSTM-FCNN based multi-class intrusion detection using scalable framework," *Computers and Electrical Engineering*, vol. 99, p. 107720, Apr. 2022, doi: 10.1016/j.compeleceng.2022.107720.
- [7] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion protocols in wireless sensor networks integrated to internet of things deployment: survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020, doi: 10.1109/ACCESS.2019.2962829.
- [8] E. E. Abdallah, W. Eleisah, and A. F. Otoom, "Intrusion detection system using supervised machine learning technique: A survey," *Procedia Computer Science*, vol. 201, pp. 205–212, 2022, doi: 10.1016/j.procs.2022.03.029.
- [9] P. B. M., N. G. M., and M. S. Hema, "Towards an effective deep learning-based intrusion detection system in the internet of things," *Telematics and Informatics Reports*, vol. 7, p. 100009, Sep. 2022, doi: 10.1016/j.teler.2022.100009.
- [10] M. Ragab and M. Farouk S. Sabir, "Outlier detection with optimal hybrid deep learning enabled intrusion detection system for ubiquitous and smart environment," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102311, Aug. 2022, doi: 10.1016/j.seta.2022.102311.
- [11] T. Khan *et al.*, "ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs," *Future Generation Computer Systems*, vol. 125, pp. 921–943, Dec. 2021, doi: 10.1016/j.future.2021.06.049.
- [12] J. Liu, L. Liu, Z. Liu, Y. Lai, H. Qin, and S. Luo, "WSN node access authentication protocol based on trusted computing," *Simulation Modelling Practice and Theory*, vol. 117, p. 102522, May 2022, doi: 10.1016/j.simpat.2022.102522.
- [13] P. Srividya and L. N. Devi, "An optimal cluster & map; trusted path for routing formation and classification of intrusion using the machine learning classification approach in WSN," *Global Transitions Proceedings*, vol. 3, no. 1, pp. 317–325, Jun. 2022, doi: 10.1016/j.glt.2022.03.018.
- [14] T. Yang, F. Zhai, H. Xu, and W. Li, "Design of a secure and efficient authentication protocol for real-time accesses of multiple users in PloT-oriented multi-gateway WSNs," *Energy Reports*, vol. 8, pp. 1200–1211, Jul. 2022, doi: 10.1016/j.egy.2022.02.061.
- [15] J. Shahid, Z. Muhammad, Z. Iqbal, A. S. Almadhor, and A. R. Javed, "Cellular automata trust-based energy drainage attack detection and prevention in Wireless Sensor Networks," *Computer Communications*, vol. 191, pp. 360–367, Jul. 2022, doi: 10.1016/j.comcom.2022.05.011.
- [16] W. Fang, W. Zhang, W. Yang, Z. Li, W. Gao, and Y. Yang, "Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks," *Digital Communications and Networks*, vol. 7, no. 4, pp. 470–478, Nov. 2021, doi: 10.1016/j.dcan.2021.03.005.
- [17] N. Rouissi, H. Gharsellaoui, and S. Bouamama, "Improvement of watermarking-LEACH algorithm based on trust for wireless sensor networks," *Procedia Computer Science*, vol. 159, pp. 803–813, 2019, doi: 10.1016/j.procs.2019.09.239.
- [18] A. Mohamed, W. Saber, I. Elnahry, and A. E. Hassanien, "Coyote optimization based on a fuzzy logic algorithm for energy-efficiency in wireless sensor networks," *IEEE Access*, vol. 8, pp. 185816–185829, 2020, doi: 10.1109/ACCESS.2020.3029683.
- [19] T. Kaur and D. Kumar, "MACO-QCR: multi-objective ACO based QoS-aware cross-layer routing protocols in WSN," *IEEE Sensors Journal*, vol. 21, no. 5, pp. 6775–6783, Mar. 2021, doi: 10.1109/JSEN.2020.3038241.
- [20] Z. Han, Y. Li, and J. Liang, "Numerical improvement for the mechanical performance of bikes based on an intelligent PSO-ABC algorithm and WSN technology," *IEEE Access*, vol. 6, pp. 32890–32898, 2018, doi: 10.1109/ACCESS.2018.2845366.
- [21] V. R. Sabbella, D. R. Edla, A. Lipare, and S. R. Parne, "An efficient localization approach in wireless sensor networks using krill herd optimization algorithm," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2432–2442, Jun. 2021, doi: 10.1109/JSYST.2020.3004527.
- [22] T. Qasim *et al.*, "An ant colony optimization based approach for minimum cost coverage on 3-D grid in wireless sensor networks," *IEEE Communications Letters*, vol. 22, no. 6, pp. 1140–1143, Jun. 2018, doi: 10.1109/LCOMM.2018.2819643.
- [23] M. I. Habelalmateen, A. H. Abbas, L. Audah, and N. A. M. Alduais, "Dynamic multiagent method to avoid duplicated information at intersections in VANETs," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 2, p. 613, Apr. 2020, doi: 10.12928/telkomnika.v18i2.13947.
- [24] W. Xin, Z. Jiang, G. Lin, and D. Yu, "Stochastic optimization of data access and hybrid transmission in wireless sensor network," *IEEE Access*, vol. 8, pp. 62273–62285, 2020, doi: 10.1109/ACCESS.2020.2982868.
- [25] B. R. Al-Kaseem, Z. K. Taha, S. W. Abdulmajeed, and H. S. Al-Rawashidy, "Optimized energy efficient path planning strategy in WSN with multiple mobile sinks," *IEEE Access*, vol. 9, pp. 82833–82847, 2021, doi: 10.1109/ACCESS.2021.3087086.




- [26] S. A. Rashid, M. Alhartomi, L. Audah, and M. M. Hamdi, "Reliability-aware multi-objective optimization based routing protocol for VANETs using enhanced gaussian mutation harmony searching," *IEEE Access*, vol. 10, pp. 26613–26627, 2022, doi: 10.1109/ACCESS.2022.3155632.
- [27] A. H. Abbas, A. J. Ahmed, and S. A. Rashid, "A cross-layer approach MAC/NET with updated-GA (MNUG-CLA)-based routing protocol for VANET network," *World Electric Vehicle Journal*, vol. 13, no. 5, p. 87, May 2022, doi: 10.3390/wevj13050087.
- [28] B. Pang, Z. Teng, H. Sun, C. Du, M. Li, and W. Zhu, "A malicious node detection strategy based on fuzzy trust model and the ABC algorithm in wireless sensor network," *IEEE Wireless Communications Letters*, vol. 10, no. 8, pp. 1613–1617, Aug. 2021, doi: 10.1109/LWC.2021.3070630.
- [29] I. A. A. E.-M. And and S. M. Darwish, "Towards designing a trusted routing scheme in wireless sensor networks: a new deep blockchain approach," *IEEE Access*, vol. 9, pp. 103822–103834, 2021, doi: 10.1109/ACCESS.2021.3098933.
- [30] P. Srividya and L. Devi, "Multi-strategic trust evaluation for intrusion detection in wireless sensor networks," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 2, pp. 106–120, Apr. 2021, doi: 10.22266/ijes2021.0430.10.

BIOGRAPHIES OF AUTHORS






Ahmed Jamal Ahmed    received the B.Eng. degree in computer engineering and information Technology from SIUST (Syrian International University for Science and Technology, Syria, in 2010 and the M.S. and Ph.D. degrees in Communication engineering (WSN) Wireless Sensor Network from UTHM University Tun Hussein Onn Malaysia, Johor, Malaysia, in 2015 and 2018, respectively. Currently, he is a Senior Lecture at the Department of Computer Engineering Technique, Almaarif University college, Alramadi, Iraq. His research interests include WSN, WSN application, prolong lifetime of WSN, Compression Data, use compression data by WSN, power consumption of WSN, extend network of WSN, Optimization WSN, AD HOC ROUTING PROTOCOLS, select best routing path and Distribute data throw WSN. He can be contacted at email: ahmed.jamal@uoa.edu.iq.



Ali Hashim Abbas (A.H.Abbas)    received the B.S. degree in communication engineering from Al-Furat Al-Awsat Technical University/ Engineering Technical College of Al-Najaf, in 2010 and the M.S. degree in digital system and computer electronics (DSCE) from Jawaharlal Nehru Technological University Hyderabad (JNTU), Hyderabad, India, in 2014, and Ph.D. degrees in Communication engineering, Clustering of Vehicular Ad-Hoc Networks (VANETs) from UTHM University Tun Hussein Onn Malaysia, Johor, Malaysia, in 2019. Where he is currently working Head of Department of Scientific Affairs and Promotions at the Department of Computer Technical engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Al-Muthanna 66002, Iraq. His research interests are cluster stability for intervehicle communication and distributed algorithms, for vehicular ad hoc networks. In addition, He is a reviewer for leading communication, and computer networks engineering journals such as vehicular ad hoc networks, vehicular communications, wireless communication, IEEE Wireless Communications Letters, Journal of Sensors, and IEEE Access Journal. He can be contacted at email: alsalamy1987@mail.com.



Sami Abduljabbar Rashid    Sami Abduljabbar Rashid was born in Al-Anbar, Iraq. He received the B.Eng. degree in computer engineering technology from Al-Maarif University College, Iraq. and the M.Sc. degree in communication and compute engineering from University Kebangsaan Malaysia (UKM), Malaysia. He is currently pursuing the Ph.D. degree in the department of communication engineering, University Tun Hussein Onn Malaysia (UTHM), Malaysia. His research interests include wireless and mobile communications and VANET. He can be contacted at email: Sami25.6.1989@gmail.com.