International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Novel Cross Optimization based Trusted and Opportunistic Routing Scheme in Wireless Sensor Network

Pritesh A. Patil[1,3]
[1]Research Scholar, Dept. of E&TC
Vishwakarma Institute of Information Technology, SPPU, Pune
[3]Assistant Professor, Dept of IT
AISSMS Institute of Information Technology
Pune, India
e-mail: p.patil.k@gmail.com

Tushar R. Jadhav[2]
[2] Associate Professor, Dept. of E&TC
Vishwakarma Institute of Information Technology, SPPU
Pune, India
e-mail: tushar.jadhav@viit.ac.in

R. S. Deshpande[4]
[4]Professor, Dept. of E&TC
Imperial College of Engieering and Research
Wagholi, Pune, India
e-mail: raj.deshpande@yahoo.co.in

Abstract— Opportunistic routing in wireless networks under mobile computing domain is one of the point of attraction for the research. Consistency along with routing security are the challenges faced by many old schemes which results performance to be compromised. However the existing techniques developed for effective routing are cost effective without the concern for the exact positioning of nodes in the network but while designing the scheme, security still requires attention. A novel cross optimization based trusted and opportunistic routing scheme for WSN is proposed in this paper which is referred as Unified Trusted and Optimized Routing (UTOR) scheme. The prime intention of UTOR is to realize optimized data movement along with routing and data security. UTOR functions in two stages, the first stage recognizes and unites the unified nodes depending on defined liberal constant(LC) which has definite trust, link stability, and quality components. Definite trust as well as link stability can be measured directly but time to live and the associated delay are considered for measuring the quality. Whereas in second stage optimized nodes selection takes place with the help of proposed UTOR over defined proclivity function(PF) based on definite_trust(DT), link_stability (LS), quality_of_node(QN) and distance. Proposed UTOR's performance is evaluated based on performance measures for Ad-Hoc sensor network of varying range of dynamic nodes in the presence of black_hole and DoS attacks. UTOR exposes relatively superior throughput and detection rate at the same time showcases minimal distance and delay, which are comparatively better than competing schemes. Significantly higher throughput and detection_rate as 44.1 and 55.7 respectively alongside low distance and delay as 168.2 and 13 are shown by UTOR which are comparatively better performance parameters than competing schemes. UTOR's effective use in WSN may be under real-time scenarios such as environmental monitoring, smart farming, automation industries etc.

Keywords- Definite_trust, Liberal Constant, Link stability, Proclivity Function, UTOR.

I. INTRODUCTION

Armed Services, forecasting of weather, civil line and industrial automation are few prime areas and opportunity for WSN to explore in these numerous applications. Battery operated nodes are the key components of any WSN setup which are restricted in terms of power usage. WSN incorporates multihop path to effectively communicate with base station, however the radio range is narrow[1]. This multihop routing is highly vulnerable to sever attacks and exploration of which may cause disaster to network upto a significant level.

Physical harm can be imposed on the network by these malicious nodes, which results to the congestion in network traffic or dropping of messages or diversion in message or interferences causing obstruction of network communication.

Unification and association between the nodes are essential for controlling the power, utilization of energy and lowest-cost peer-to-peer communications that is required to realize minimum utilization of energy, low-cost of communications which are helpful in environment monitoring, critical parameters monitoring in armed services, usage in medical for human physical condition observation vehicular networks[31] etc. But WSN's functioning is affected by restriction in operating power, storage space and because of the limitations incurred in providing the security. Mentioned limitation forced to believe and approximate the trust and energy values with

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

respect to the network. Considerable energy savings and expected outcomes may be realized by provisioning the security aspects in network[3].

Compromise in data and security usually realized as distributed and dynamic features of routing are prone to severe attacks[4]. There is always the possibility of influence of attacks on WSN which further results in inappropriate implementation of WSN at the time of data transfer[5].

Variations in the routing mechanisms developed for outdated networks may not be favourable for wireless ad-hoc networks and inculcate computational overheads in routing process. Routing's main focus is to choose the most appropriate path to transport relevant information alongwith choosing best suited forwarders. In place of transmission medium the traditional routing mechanisms primarily adopt ARR(Automatic repeat request) or compound methods for error checking or data link techniques[6].

Continuous identification of the location of static nodes in the route significantly increases the complexity, as for many of the applications dispersion and installation of these static nodes under isolated area is adhoc in nature[7].

The prime interest of researchers is opportunistic routing(OR) over outmoded routing schemes, to obtain most likely route in adhoc networks and WSNs[8].

Wireless transmission medium's broadcast nature is oppressed through OR that certainly not restrict itself to the precise route before data transmission. Simply stating, various weak links are combined to form a strong link that is advantageous during communication and data transfer[9].

Furthermore, based on the desired policy of routing there is a significant increase in the possibility of hit in the route selection. For generating the route the major constraint is the inclusion of nodes selected with moderately higher trust value, as trusted nodes demonstrate highest probability of forwarding desired data to sink node alongside indicate maximum possibilities for effective route selection[10].

Trust based mechanisms are adopted as the most prominent schemes of routing in the presence of malicious node causing internal attacks. Realization in recognizing the malicious node, the schemes focusing on trust management are the best suited candidates as evaluating trust values incurs less computation complexities and minimum communication load[11]. Data transfer initiated in traditional routing schemes is through identified fixed routes which then harmed by the difficulty while cloning the untrustworthy and uneven wireless medium. DSR which is Dynamic Source Routing[12], DSDV which is Sequenced Distance Vector routing[13], AODV which is Ad Hoc On-Demand Distance Vector Routing[14] etc. are termed as the conventional routing mechanisms[9]. Distributed scheme is used in ATSR that is Ambient trust sensor routing to evaluate the reliability of nodes[16], in which the process of monitoring the nature of node is initialized based upon the actual trust methods, also for its instantaneous neighbouring nodes the direct trust is calculated. Furthermore, Trust dependent link state routing protocol(TLSRP)[17] incorporates direct as well as indirect trust values into consideration excluding the computation of conflict due to nodal attack. Moreover Trust aware routing framework[2] is one of the capable multipath routing method wherein neighbouring node's trustworthiness is calculated, also it supervises the dependencies in routing on efficient energy usage and trust computation[3]. For the provisioning of routing based on opportunity, each element prepares as well as maintains information about routing in tabular fashion where optimum path between source and destination is indicated by the default route, also the list of probable candidates is comprised of next-stage candidates those potentially forwards the originated information. Through OR the chances of one or more possible routes is realized to simultaneous packet forwarding is demonstrated in ROMER[18] perhaps MORE[19] uses network coding technique for this purpose. Whereas in[20] unicast routing for multi-hop wireless ad-hoc network is performed.

Remaining organization of the paper as: 2nd section highlights the existing work. Presented Unified Secure and Optimized Routing framework is presented in 3rd section. 4th section describes the outcomes and observations alongside improvement in performance of presented framework UTOR over the existing methods. Finally 5th section presents the observable concluding remarks and further extension scope.

II. EXISTING WORK

Over and above to the ephemeral survey of exiting schemes discussed in first section, some what detailed description of suitable schemes highlighted in the referencing is presented here.

Providing security to WSN routing is abstract point of attention for the research community. Significant computational overheads are experienced in the process of routing while protecting it over various sever threats. Obtaining optimal solution the difficult task inspite of protecting the networks from attacks.

In [2] a routing scheme is presented based on trust, which decreases the efficiency of the routing protocol significantly during integrating with the existing schemes indicates poor strength. However failed to report compromised packets getting injected in routing possesses false information. Moreover attacks caused due to indent theft which then unexpectedly replay the genuine routing information, is out of the scope of this framework. At the time of routing process the faults can be easily exploited through identity deception.

Parama et. al.[3] presented a trust and energy factor based routing scheme, wherein the best suited route is chosen depending in energy, trust, hop-count and rate_of_flow of route traffic which significantly increases the computational complexities over the network. In case of Clustered kind of WSN where it have more than one sink present in the network this method is inefficient.

Another trust based routing scheme presented by Qin, D. et. al. [5] named ad TSSRM with the intention to enhance protection and handle the most common attacks on the network. Reliable data transfer is achieved because of the reduction of computational overheads in routing. This method is lacking in realizing distributed intrusion detection which shortens the way to obtain and examine the trust degree and predominant routing. TSSRM is precisely depending on the trust degree

which results in limitations in routing process as it relies on the static route. Several available opportunistic routing schemes are ensuring the transmission progression to be maximized but at the same time disabling the duplication of packets[6].

Congestion aware opportunistic routing scheme is proposed in[8], to reduce the traffic load of the network however the mechanism to minimize the energy consumption and delay is out of the scope of this method.

In [9] scheme abbreviated as SOAR which is Simple-Opportunistic-Adaptive-Routing is proposed to recognize and choose the most prominent candidates while precedence based timers incorporated. The proposed method also capable to handle multiflow and realizes greater efficiency at the same time. Due to the broadcast nature of nodes and lack of MAC layer reliability support, the nodes may become easy target which then may result to packet loss or manipulation. To improve the performance of any routing scheme default path selection should be there, but it is beyond the possibility by this method.

Active-trust based mechanism proposed in[10] showcase effective energy utilization, performance scalability, efficient success rate during routing process with adequate provision of security and effective data rate between the nodes of network. However at the same time the scheme suffers unexpected energy consumption that significantly degrades the performance of the scheme and lead to the failure. The proposed scheme also consumes large amount of energy because of the procurement of trust and release may incur computational overheads which makes the process of detecting malicious node more complex and affect the lifetime of the network.

An efficient optimization scheme is proposed by Wang et.al.[11] named Ant colony optimization routing, which focuses on two facts, firstly to reduce the packet loss and secondly on ensuring security in routing. The scheme demonstrates the improvement in the lifetime of network because of the efficient harmonising of consumed energy by the nodes which then significantly reduces the entire utilization of energy in network. Still the estimation is expected by this scheme in presence of active complex attacks.

Optimized routing with focus on power efficacy and its utilization proposed in[21] offers tripling of lifetime of network. Irrespective of the size of network the scheme presents better energy usage throughout the routing process. Inspite of efficiency of the scheme, computational overheads and complex communications are the limitations of this method.

An ant colony optimization enabled and trusted scheme for peer-to-peer network is proposed in[24], which selects the genuine server effectively. Criteria for measuring the trust level of neighbours is the scent leftover by ants. Identity theft generated issues such as replay of network and routing information is beyond the possibilities by this scheme.

For evaluating trust between nodes of the network a Self-recommendation method presented in [25]. Key point of this method is the computation of trust level based on the energy level. Identity theft and erroneously replaying routing information may badly affect the network and routing, which further affects the process of optimum route selection for communication.

HTMS proposed by Karthik et. al.[26] which has strength of node and originality of data are the two main operating parameters. Ratings are allotted to the originated packet based upon parameters of node linkage and source of packet. Using these parameters, decisions related to further routing are taken. Basic network details can easily be manipulated by the adversaries stealing the identity of nodes elected as the members of routing which significantly increase the chances of compromising the reliability of data at the time of communication in the network.

Vishwas et. al.[27] proposed the scheme for handling attack causing packet drop during communication in wireless ad-hoc network based on the list of trust indicating the node's participation in routing. Nodes are separated out using trust and energy values maintained in the list depending on selfishness and unselfishness. As WSNs are resource constrained and because of involved computational overheads this method is not suitable.

Caliber of machine learning towards enhancing wireless network communication specially in case of Smart Grids is presented in [28] which is the integration of ML into Routing Protocol for Low-Power and Lossy Networks (RPL) and named as ML-RPL. ML-RPL uses CatBoost which is Gradient Boosted Decision Trees (GBDT) scheme, for optimizing routing decisions. How ever obvious classification and computations incurred in ML may affect packet delivery ratio significantly.

Darwish et. al. [29] proposed blockchain based routing to improve the efficiency and security in WSN. For authorizing the process of transmission initiated by the node they utilized PoA technique implied in blockchain technology. As the properties of each node involved in routing is manipulated, it may lead to false detection of malicious node or may incur unwanted delay due to finalization of next potential forwarder.

Bin-Yahya et. al. [30] proposed another strong flavour of efficient trust based scheme for Software-defined WSNs which is a tiered trust management scheme named as TSW to identify probable threats occurs during forwarding process of routing in SDWSNs. Moreover, separate score of trust and parameters control and traffic, accordingly were considered, to improve identification of attacks. However distributed version of attacks are out of the scope of this work.

Prime focus of work is to put forth and assess Unified Trust and Optimized Routing mechanism for WSN. Method is depending upon opportunity unification and trust which is employed in recognition of trending scenario wherein participation of each probable node in the process of routing as well as security is assured.

Our proposed technique is divided into two stages: identification and selection of legal nodes to further guarantee secure network communication is the scope of stage-I. Stage-II is intended to ensure secure routing based on trust and opportunity in recognition of reasonable solution.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

III. Development of Cross Optimization Routing(UTOR)

To determine optimum and favourable routes various routing schemes are designed for WSNs. Efficiency of routing method for WSNs can be decided based on two main factors trust and energy. Due to simultaneous evaluations existing schemes incurred more computational overheads. A technique is proposed in this work to reduce this unwanted computational complexities alongwith handling complicated threats. So, to realize security and optimization, an Unified trusted optimized routing(UTOR) is presented. Name unified is given to the proposed scheme as our earlier work[15] considers static nodes and process of routing was severely conducted only via recognized path.

Nevertheless, positions of the nodes are not static in real time application scenarios, it may be installed on the target items and as target objects moves, nodes will also roam accordingly. That's why the available methods may not be the probable solution. At the same time it is also the expectation from the routing scheme to generate the possibilities of more than one route from source to destination. Considering all these facts, proposed unified secure optimized routing technique which functions in two stages.

First stage's focus is on recognition and choice of unified nodes from the initiated nodes. Moreover this stage also ensures highest capabilities of protection from black hole and DoS attacks by guarantying that the method acquires trusted and unified structure. Unified nodes are selected using devised liberal constant(LC) based on definite trust, link stability, and quality component. Section 3.1 illustrates these components. Simulation of WSN initially for N nodes and depending on LC unified nodes get identified to be submitted to the next phase of the proposed method. Next to that the second phase intended on incorporating greediness in packets, additionally optimization of utilization of memory, efficient end to end communication etc. which are the critical network resources. Based on UTOR routing process is performed optimally to select and identify the route, on the basis of Proclivity Function(PF) comprising with four components definite_trust(DT), link_stability(LS), distance and quality_of_node(QN). Optimized routing by assuring definite trust is carried in WSN in this way. Structural schematic of the proposed UTOR routing scheme is depicted in figure 1.

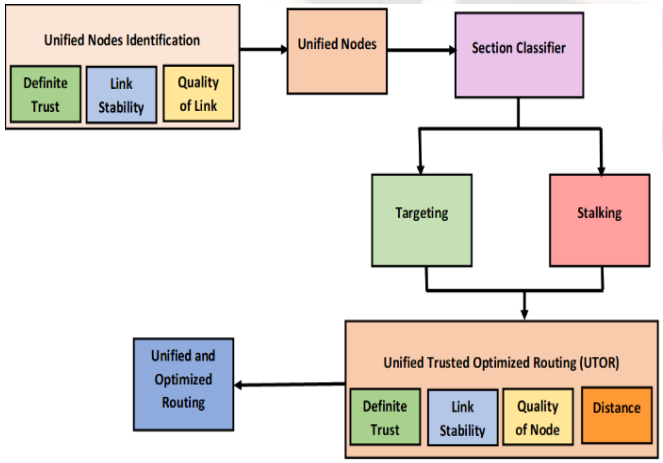


Figure.1 Unified Trusted and Optimized Routing Framework

A. Recognition of Unified Nodes

Unified nodes are recognized to experience secure network using defined Liberal Constant(LC). LC is computed based on definite_trust(DT), link_stability (LS), and quality_of_link(QL) component. The liberal constant LC is computed as

$$LC = [\mathrm{DT_i} + \mathrm{LS}_i + \mathrm{QL}_i]/3 \qquad (1)$$

here, $\mathrm{DT_i}$ termed as definite_trust of i[th] node, LS_i indicates stability of link of i[th] node. Recognition of M unified nodes among the N initialized nodes such that $(M < N)$. The election of unified node is based on the criteria where the node shows greater trust, higher link stability and quality, meanwhile the all the other nodes are simply denied from their involvement during routing. QL_i is solely depends upon the higher persistence time of link(PTL) and comparatively low delay faced by the nodes.

a. Definite Trust (DT)

Definite trust as mentioned as local trust in[22] based on $scale\_of\_consent$ during the interaction between the nodes. $\mathrm{DT_i}$ among the nodes i and j rely on $scale\_of\_consent$ s_con_{ij} among them. Whenever node j is comfortable with the node, s_con_{ij} is high and indicate local trust. Upon profitable interaction PI_{ij} among the nodes i and j by the entire nodes of the network s_con_{ij} is computed as follows:

$$s\_con_{ij} = \frac{PI_{ij}}{m} \qquad (2)$$

here profitable interaction took place between nodes i and j is mentioned as PI_{ij} and m denotes the entire nodes present in the network.

b. Link Stability (LS)

Link stability indicates the connections present between nodes and join communication links. The Link stability (LS_i) of the node is evaluated as,

$$LS_j = \frac{1}{m}\left(\sum_{i=1}^{m} \frac{LS_i}{c}\right) \qquad (3)$$

here, LS_i denotes the link stability of i^{th} node and c is the total number of possible and existing connections in the network.

c. Quality of Link (QL)

Quality of link is calculated depending upon the link's survival time(STL) alongside incurred delay. STL and survival interval of network are correlated. STL of candidates in the area precisely depending upon the active connectivity exist among elements[23]. During active data transfer the strong link is evaluated and involved in the process of data transfer to initiate the communication to experience lossless transfer of data. Because of the dynamic nature of nodes there are high chances of link failure and that's why its mandatory to compute STL.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Therefore, it's the need to prevent these link failures so that the effective communicating path can be decided. For the calculation of STL the factors like movement of node, direction of movement and locational coordinates are considered. Delay d_j of j^{th} node is considered as the ratio denoting active vs entire nodes exists in the prescribed area. Hence the quality_of_link via j^{th} node is expressed as:

$$QL_j = STL_j + d_j \quad (4)$$

Finally the liberal constant (LC) is presented as:

$$LC = \left[\frac{PI_{ij}}{m} + \frac{1}{m}\left(\sum_{i=1}^{m}\frac{LS_i}{c}\right) + \left(STL_j + d_j\right)\right] \quad (5)$$

B. Unified Trusted Optimized Routing (UTOR) Scheme

Based on Liberal Constant (LC) unified nodes are identified as well as splitted, and only those are allowed to take part in the process of routing. Advancement of routing rely on the secure and optimized routing mechanism. Source, sink and unified nodes are activated to generate routing path optimally. Once the source and destination nodes are decided, there are n unified nodes acquired based on opportunistic and secure routing algorithm UTOR using Proclivity Function (PF).

a. Route Vector

Route vector is nothing but the interpretation of all possible solutions to be obtained by the use of UTOR algorithm. Formation of route vector is intermediary nodes engaged during routing, total unified intermediary nodes is expresses as n, here n differs between 1 to U and U is the total unified nodes in the active session. Route vector with three unified nodes is shown in figure 2,

Src	51	23	71	Dest	n=3

Figure. 2 Route vector

Here nodes 51, 23 and 71 are the unified nodes and transmission of data took place through these nodes to reach sink for $n = 3$. Using UTOR the identification and election of optimal unified nodes is done through Proclivity Function. Among the source and sink nodes the route vector operates with exclusive formats trailed by paths identified for routing process.

b. Proclivity Function (PF)

Responsibility of Proclivity Function is to confirm the election of optimal unified nodes to perform unified routing in WSN by ensuring maximum value of proclivity. For obtaining solution to the problem of maximization, effective calculation of proclivity is needed. Proclivity function is expressed based upon four factors definite_trust(DT), link_stability (LS), quality_of_node(QN) and covered distance(D). Hence the Proclivity is expressed as,

$$PF = \frac{1}{4}\left[\sum_{1i=1}^{n} DT_j + LS_j + QN_j + \left(1 - D_{i,i+1}\right)\right] \quad (6)$$

Here $D_{i,i+1}$ indicates the distance between head-to-head unified nodes i and $i+1$. To experience max value for proclivity the mechanism should have max values of DT, LS and QN but D shall have min value at the same time. During the construction of PF the parameter distance should posses min value, hence it is termed by subtracting it from 1 in the function.

c. UTOR Algorithm

Prime focus of the presented Unified Trusted Optimized Routing scheme is to acquire substantial optimal solutions alongside ensuring low computational overheads. Usually nodes of WSN are dynamic in most of the real time applications. Moreover WSNs are restricted in terms of network resource utilization, UTOR handle this situation effectively. Unified nodes are classified in two sections, first is targeting and the other is stalking section in terms of realizing optimized and effective network resource utilization.

Above mentioned segmentation implies the actions performed by wild cats, because maximum time they are targeting their pray, when they get best possibility they suddenly respond to the situation and down the pray with high rate of success in most of the cases. Perceptible feature of them here to point is their energy restoration and saving capabilities as they normally need less energy for stalking with assured success. Technically stating, the discovery and processing segments of UTOR indicate optimized solution with higher connect rate. More clearly mentioning the unified nodes are classified into two sections. The first mode is keeping the nodes which are in targeting stage however second mode is stalking. Under targeting side the unified nodes approach potential next stage node i.e. sink in less amount of time, that's why the quantity of nodes in this section is less as opposed to the other segment. Recent location and proclivity are computed to realize the updated result and stored. Iteration and repetition of above stated steps are carried out to realize the finest optimized result.

Unified node's modified locations are fixed by the following rule when the nodes are in stalking mode in UTOR:

$$ML_{i,r}^{t+1} = \frac{1}{[X_1 * \varphi_1]}\left[\{-\omega * (JS_r - 0.5)\{1 - X_1 * \varphi_1\} + v_{i,r}^{t} + X_1 * \varphi_1 * PL_r^{t}\}\right] \quad (7)$$

here, $ML_{i,r}^{t+1}$ is the modified location of unified node at time $(t+1)$, PL_r^t indicates the present location of unified node. $ML_{i,r}^{t+1}$ and PL_r^t are the positions at time $(t+1)$ and (t), $v_{i,r}^t$ is the movement speed of unified nodes at (t) time, JS_r is the linking speed or rate of unified nodes and X_1, φ are the arbitrary numbers have values precisely in 0 and 1. i^{th} node's moving speed in r^{th} domain is given as

$$v_{i,r}^{t+1} = v_{i,r}^{t} + R_1 * \varphi_1\left(ML_{i,r}^{t+1} - PL_r^{t}\right) \quad (8)$$

where φ_1 is the constant. For realizing the optimal result, at the beginning Overall_Nodes N_{ir} are initialized, represented as,

$$N_{ir};\ (1 \le i \le UN) \quad (9)$$

where, UN is the entire unified nodes whereas r is the parametric search area.

Position as well as speed of integrating UNs are described arbitrarily to initialize the process of optimization thereafter

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

they are positioned in targeting and stalking sections consequently. Initiation of position and speed or velocity of every unified node is done randomly in the first section, thereafter positioning of these initiated nodes in targeting and stalking modes appropriately.

Switching among these modes is based on UNLP Unified Node-Location-Parameter which indicates targeting section if its value is 1 and stalking section if its 0.

Towards different states UNLP is defined for nodes states s it is generated at random. Traversing is carried out by unified nodes depending upon current situation or that is inactive however attentive in targeting section. The terminology is similar to the behaviour of the wild cats as when they are targeting or observing its target it remains inactive but attentive for some time and then based on the condition it perform certain action such as traversal and that too slowly. At the starting point the i^{th} node's copies are been formed and then it is instructed to observe their Ownership Memory Buffer (OMB). This copying process continues for obtaining the current copies of nodes, and based upon its current position its locations are modified, their selected dimensions (SD) by including a random number. The modified location of unified node is expressed as $ML_{i,r}^{t+1}$ and is given as:

$$ML_{i,r}^{t+1} = (1 \pm SD * \theta) * PL_{i,r}^{t} \qquad (10)$$

The proclivity is computed and guaranteed to 1, that is associated to the position of unified node, is representing distinct result. But if proclivity is not 1 then for calculating the distinct result the probability is expressed as

$$P_r = \frac{|PF_r - PF_{\emptyset}|}{|PF_{max} - PF_{min}|} \qquad (11)$$

here P_r, is the possibility of the r^{th} unified element, PF_r is proclivity of the r^{th} element, PF_{max} and PF_{min} are the max and minimum values of PF. $PF_{\emptyset}$ represents proclivity's maximum value in case of minimization problem and minimum value in case maximization problem.

In addition, determination of nodes placements in appropriate sections is done through UNLP parametric value. In case UNLP is not equals 1, UN is categorized in stalking stage to strive towards optimal forwarding node. After the successful recognition, using presented UTOR, unified node's position and velocity or speed is modified.

Moreover, most precise proclivity measure P_{opt} for the modified result is carried out after fixing the position of unified nodes either in targeting or stalking section. To realize fine optimum and effective result the proclivity function must hold max value, which represent that the optimum unified nodes can only be the part of the process of routing.

Lastly, confirmation of the termination of process is ensured using specified terminating standards. This terminating standard is specified in experiencing favourable impact of the applied algorithm and comprises of exhaustive recursions, progression percentage and time of execution. Figure 3 depicts the above mentioned steps in pictorial representation.

Perseverance of the process of routing with unified nodes is realized through the proposed UTOR. Below given pseudo code are the steps of UTOR algorithm:

$Algorithm$: $Unified\ Secure\ Optimized\ Routing$
$Input$: $Section\ of\ nodes, L_{i,r}, with\ U\ unified\ nodes$
$Output$: $Precise\ Proclivity\ Measure, P_{opt}$
$Begin$
  $Initialization\ of\ Nodes$
$While\ (t < t_{finish})$
  $Calculate\ Proclivity$
    $Compute\ Precise\ Proclivity\ Measure, P_{opt}$
$For\ (t < t_{finish})$
$If\ (UNLP = 1)$ /
/$nodes\ are\ selected\ for\ targeting\ section$
  $Unified\ nodes\ modify\ their\ position\ in$
  $targeting\ section\ using\ eq.10$
$Else$ /
/$nodes\ are\ selected\ for\ Stalking\ section$
  $Unified\ nodes\ modify\ their\ position\ in$
  $stalking\ section\ using\ eq.7$
$End\ If$
$End\ For$
$End\ While$

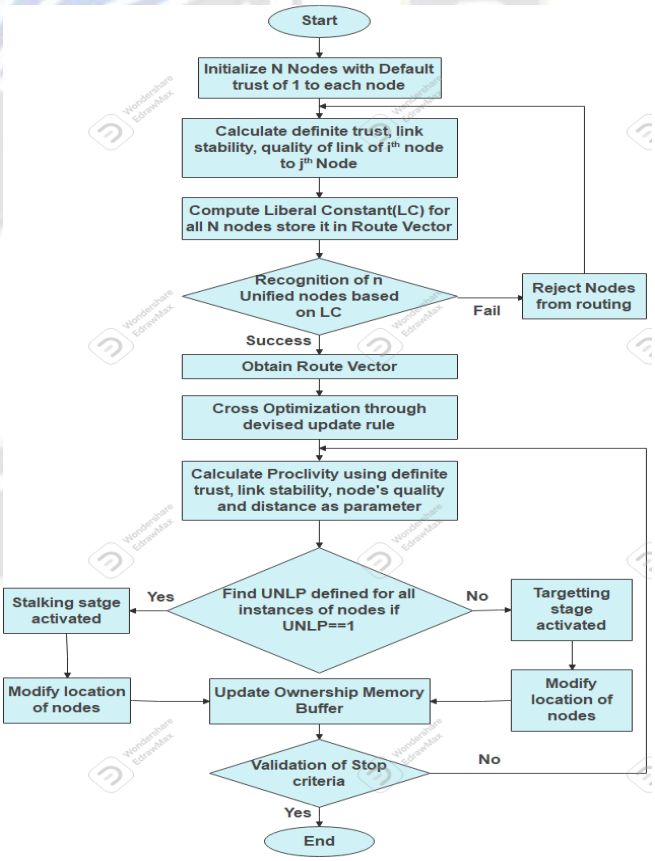


Figure 3. Flowchart of entire stages of UTOR scheme.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

IV. Outcomes and Observations

This section elaborates the experimental results and efficiency of UTOR as compared to the nearby opposing techniques. Simulation of proposed UTOR scheme is done in NS2 platform and based on detection_rate, distance, delay and throughput the performance is evaluated. Alongside the comparison, in the incidence of Black_hole and DoS attacks. Sample screen of WSN simulation with 100 node elements is presented in figure 4 that indicates the source, sink and adversary. Network interaction and message passing are done using unified nodes in this network.

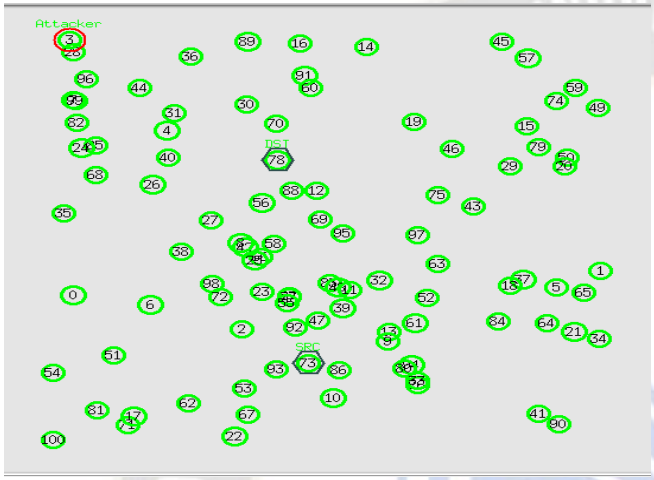


Figure. 4. Simulation setup with density 100.

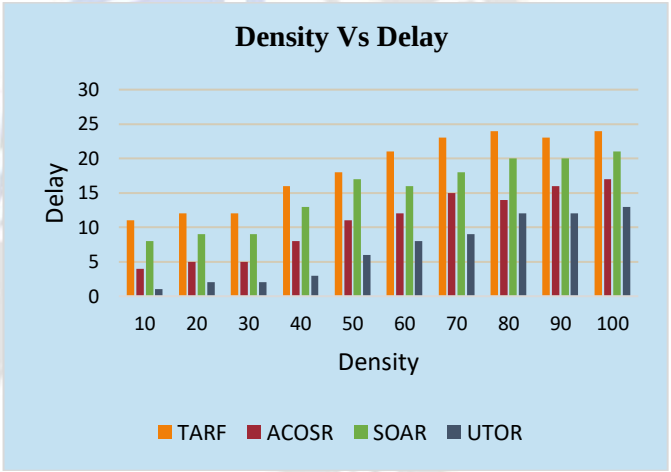
A. *Parameters of Performance Measure*

Effectiveness of the method proposed in this paper is measured on the basis of delay, distance, rate_of_detection(rod) and throughput. Throughput is measured as the rate of the data transacted in the specified timeslot in the network. Delay is measured as the consumed time while transfer of packet in the presence and/or absence of attack occurred in the network. rod is the precision of attack detection in the network. Effective method's performance is decided with high rod, energy and throughput but low delay in the network. At the same time the distance between unified nodes should be minimum to realize the performance improvement of the method. Effectiveness of performance of UTOR is examined in the existence of blackhole and DoS attacks.

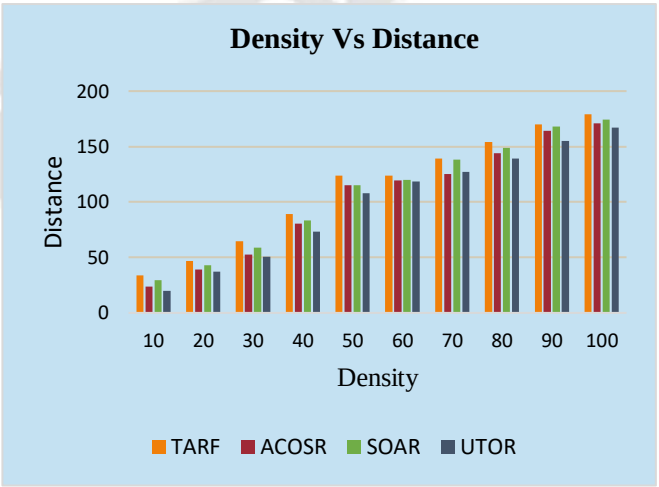
B. *Comparison of Performance*

Performance of the presented UTOR method is evaluated under the impact of black hole and DoS attacks on the network. The evaluation is based on the earlier stated metrics. Further the comparison of the performance of UTOR is done with TARF[2], SOAR [9], and ACOSR[11]. Observable enhancement in performance is presented by the comparative analysis against the mentioned opposing scheme. NS2 platform is used to establish the network of dynamic nodes of various range to test scalability in performance.

In presence of Blackhole threat: Based on the previously stated measures of the examination of the operation in existence of blackhole attack is presented in figure 5. Figure 5(a) shows delay based analysis which should be minimum for the effectiveness of the method. To present the sample quantitative improvements of proposed scheme as compare to competing methods stated above and proposed scheme(TARF, ACOSR, SOAR and UTOR) while the density of network is 100 for the measure of delay are 24, 17, 21 and 13 seconds. Distance metric should be minimum for the effectiveness of the routing method figure 5(b) reflects the distance by TARF, ACOSR, SOAR and UTOR in same case are 179.3, 171, 174.2 and 167.3 respectively. Detection_rate metric values should be significantly high to realize the high performance and accuracy of the scheme and with the density of 100, the detection_rate reflected byTARF, ACOSR, SOAR and UTOR are 49.7, 52.3, 50.4 and 57.6 respectively, as shown in figure 5(c). Moreover the scheme's performance significantly depends on the throughput parameter and that should be high. For the density 100, the schemes TARF, ACOSR, SOAR and UTOR indicates the throughput as 38.5, 40.7, 41.6 and 45.4 respectively shown in figure 5(d). Depending on the obtained results in different phases of the operating mechanism of proposed scheme, UTOR indicates considerably higher detection_rate and throughput where as significantly lower delay and distance.

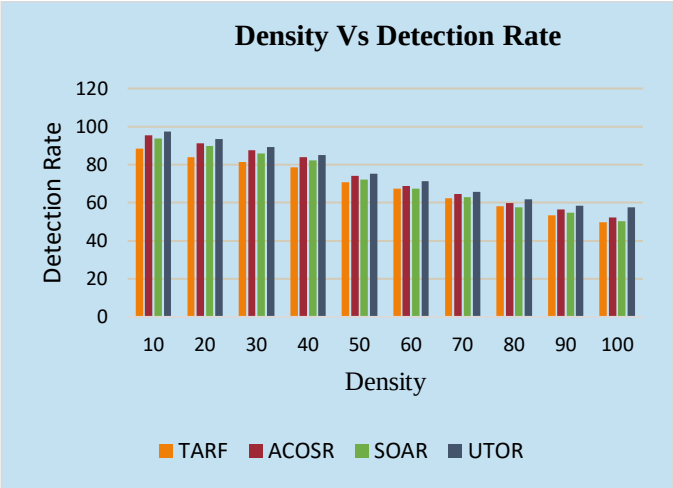


(a)

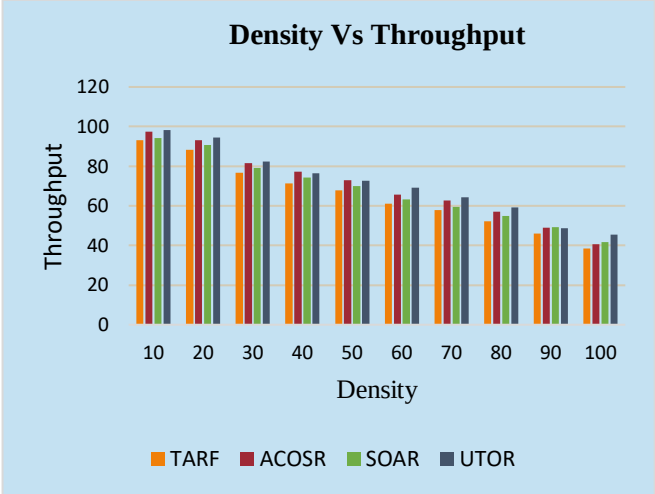


(b)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*



(c)



(d)

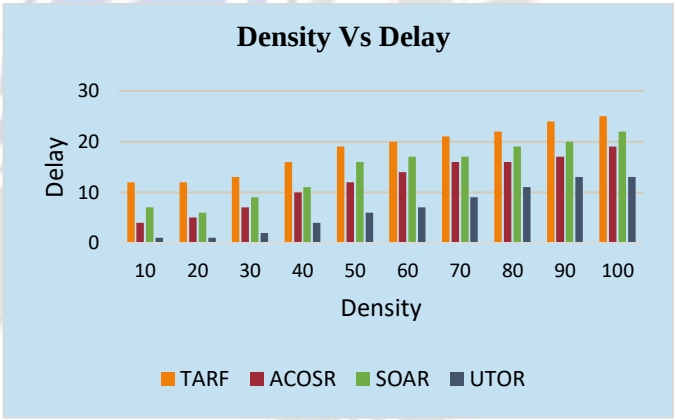
Figure. 5. Performance of Proposed UTOR Scheme in presence of blackhole

Besides that more comprehensive values are presented in table 1, where high performance of proposed UTOR over competing methods is clearly indicated in varying density of WSN from 10 to 100 in the existence of blackhole threat on the basis of performance metrics considered.

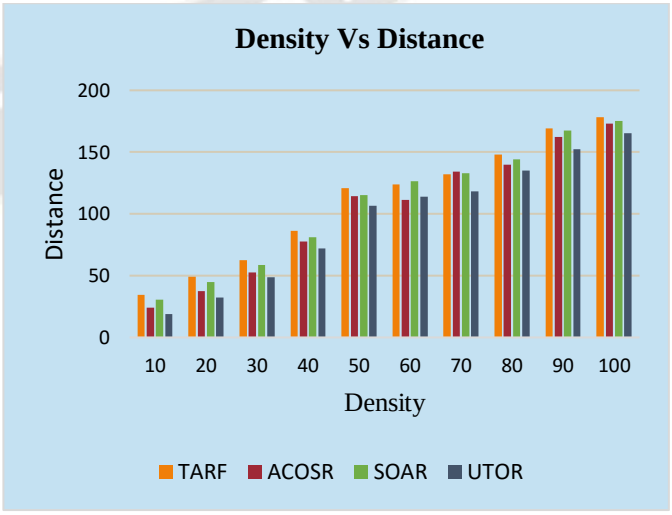
Density	Delay: D				Distance: DT				Detection_rate: DR				Throughput: T			
	TARF				ACOSR				SOAR				UTOR			
	D	DT	DR	T	D	DT	DR	T	D	DT	DR	T	D	DT	DR	T
10	11	34	88.3	93.2	4	23.7	95.4	97.4	8	29.3	93.8	94.1	**1**	**20**	**97.4**	**98.3**
20	12	47	84	88.4	5	39.2	91.3	93.2	9	42.9	89.8	90.7	**2**	**37.4**	**93.4**	**94.5**
30	12	64.5	81.3	76.8	5	52.7	87.5	81.5	9	58.7	86	79.1	**2**	**50.6**	**89.2**	**82.3**
40	16	89.3	78.6	71.3	8	80.5	83.8	77.3	13	83.3	82.1	74.4	**3**	**73.3**	**85.1**	**76.4**
50	18	124	70.7	67.7	11	115.2	74.2	72.9	17	115	72.2	70.1	**6**	**107.7**	**75.2**	**72.8**
60	21	124	67.3	61	12	119.4	68.8	65.6	16	120	67.4	63.2	**8**	**118.5**	**71.2**	**69.1**
70	23	139	62.4	57.8	15	125	64.6	62.8	18	138	62.8	59.4	**9**	**127**	**65.8**	**64.3**
80	24	154	58.2	52.1	14	144	59.9	57.1	20	149	57.6	54.9	**12**	**139.4**	**61.7**	**59.2**
90	23	170	53.4	46.1	16	164	56.4	48.9	20	168	54.8	49.3	**12**	**155.2**	**58.3**	**48.8**
100	24	179.3	49.7	38.5	17	171	52.3	40.7	21	174.2	50.4	41.6	**13**	**167.3**	**57.6**	**45.4**

Table 1. Comprehensive result in presence of blackhole

In presence of DoS threat: Based on the previously stated measures of the examination of the operation in existence of DoS attack is presented in figure 6. Figure 6(a) shows delay based analysis which should be minimum for the effectiveness of the method. To present the sample quantitative improvements of proposed scheme as compare to competing methods stated above and proposed scheme(TARF, ACOSR, SOAR and UTOR) while the density of network is 100 for the measure of delay are 25, 19, 22 and 13 seconds. Distance metric should be minimum for the effectiveness of the routing method figure 6(b) reflects the distance by TARF, ACOSR, SOAR and UTOR in same case are 178.4, 173.2, 175.3 and 165.3 respectively. Detection_rate metric values should be significantly high to realize the high performance and accuracy of the scheme and with the density of 100, the detection_rate reflected by TARF, ACOSR, SOAR and UTOR are 48.3, 51.4, 50.5 and 58.2 respectively, as shown in figure 6(c). Moreover the scheme's performance significantly depends on the throughput parameter and that should be high. For the density 100, the schemes TARF, ACOSR, SOAR and UTOR indicates the throughput as 37.7, 39.8, 40.2 and 45.2 respectively, shown in fig 6(d). Depending on the obtained results in different phases of the operating mechanism of proposed scheme, UTOR indicates considerably higher detection_rate and throughput where as significantly lower delay and distance.

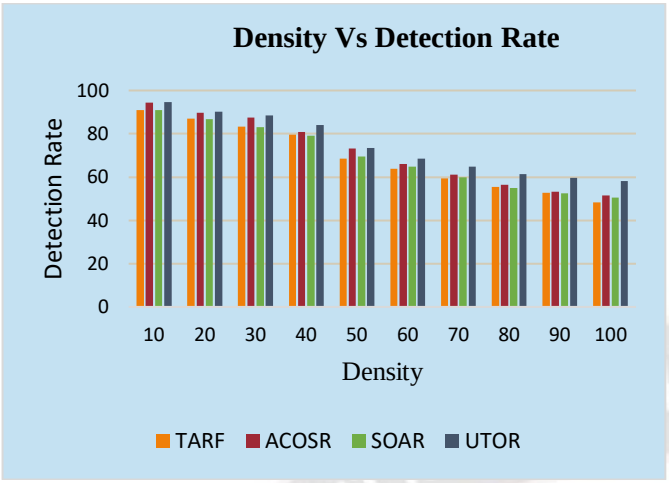


(a)

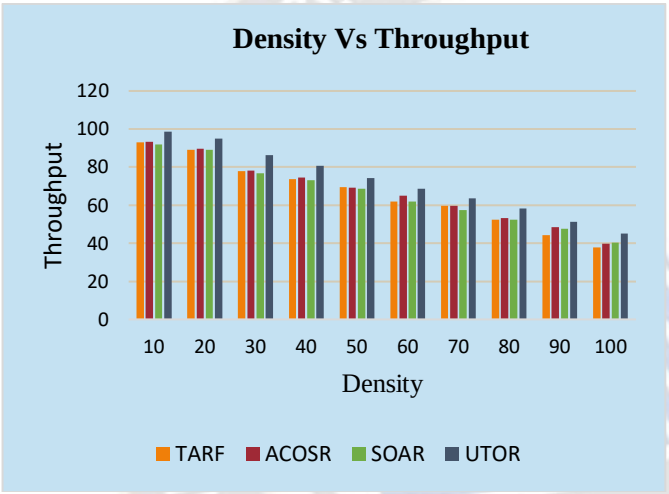


(b)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*



(c)



(d)

Figure. 6. Performance of Proposed UTOR Scheme in presence of DoS

Besides that more comprehensive values are presented in table 2, where high performance of proposed UTOR over competing methods is clearly indicated in varying density of WSN from 10 to 100 in the existence of DoS attacks on the basis of performance metrics considered.

Density	Delay: D				Distance: DT				Detection_rate: DR				Throughput: T			
	TARF				ACOSR				SOAR				UTOR			
	D	DT	DR	T	D	DT	DR	T	D	DT	DR	T	D	DT	DR	T
10	12	34.6	91	93.1	4	24.2	94.3	93.4	7	30.7	90.9	91.8	1	18.9	94.6	98.6
20	12	49.1	87.1	89.1	5	37.3	89.6	89.6	6	44.7	86.8	89.1	1	32.2	90.3	95.1
30	13	62.7	83.4	77.8	7	52.8	87.4	78.2	9	58.8	83	76.7	2	48.8	88.5	86.2
40	16	86.2	79.5	73.6	10	77.5	80.9	74.5	11	81.2	79.2	73	4	71.9	84	80.8
50	19	121	68.4	69.4	12	114.2	73.2	69.2	16	115.1	69.5	68.5	6	106.7	73.4	74.2
60	20	124	63.7	61.9	14	111.1	66.1	65.1	17	126.3	64.8	62	7	113.8	68.5	68.5
70	21	132	59.3	59.7	16	134	61.2	59.6	17	133	59.9	57.5	9	118.2	64.9	63.7
80	22	148	55.5	52.4	16	140	56.5	53.3	19	144	55	52.4	11	135	61.4	58.4
90	24	169	52.7	44.3	17	162.4	53.1	48.4	20	167.5	52.5	47.6	13	152.4	59.7	51.2
100	25	178.4	48.3	37.7	19	173.2	51.4	39.8	22	175.3	50.5	40.2	13	165.3	58.2	45.2

Table 2. Comprehensive result in presence of DoS

V. CONCLUSION

Routing based on unified and trust is accomplished for WSN alongside opportunity and optimization performed under two stages, recognition and fixation of unified nodes. Liberal constant(LC) is devised in first phase, that categorizes unified nodes among all initiated nodes. LC's function is based on definite_trust, link_stability and quality of link measures. Only unified nodes are permitted to participate in routing and other than those are simply rejected. For realizing the optimized routing an Unified Trusted Optimized routing (UTOR) framework is proposed in the second phase. UTOR performs based upon devised Proclivity Function(PF) which is expressed using definite_trust(DT), link_stability (LS), quality_of_node(QN) and distance measures. Recognition of unified nodes are grouped in two categories viz targeting and stalking modes. Then after the assistance for the network is done through route vector to pick the respective unified nodes to perform the communication between source and destination. UTOR is implemented using simulation in NS-2 with 10 to 100 dynamic nodes in WSN. Assessment of the performance and comparison is carried out using delay, detection_rate, distance, and throughput as measures in existence of black hole and DoS threats. Results of simulation expresses the efficacy of the proposed UTOR scheme vs the existing methods taken into account in the phase of evaluation. Prosed scheme shows minimum delay and distance of 13 and 165.3 respectively whereas greater throughput and detection_rate of 45.2 and 58.2 respectively. While the design of routing framework, major challenge is to minimize the computation overhead. As per the demand of application, the proposed method can be explored further to significantly decrease this complexity and design even better optimized routing method.

REFERENCES

[1] Townsend, C. and Arms, S., "Wireless sensor networks," MicroStrain, Inc, vol.20, no.9, pp.15-21, 2005.

[2] Zhan, G., Shi, W. and Deng, J., "Design and implementation of TARF: A trust-aware routing framework for WSNs," IEEE Transactions on dependable and secure computing, vol.9, no.2, pp.184-197, 2012.

[3] Zahedi, A. and Parma, F., "An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks," Peer-to-Peer Networking and Applications, pp.1-10, 2018.

[4] J. G. Choi, S. Bahk, "Cell-throughput analysis of the proportional fair scheduler in the single-cell environment," IEEE Transactions on Vehicular Technology, vol. 56, no. 2, pp. 766-778, 2007.

[5] Qin, D., Yang, S., Jia, S., Zhang, Y., Ma, J. and Ding, Q., "Research on trust sensing based secure routing mechanism for wireless sensor network," IEEE Access, vol.5, pp.9599-9609, 2017.

[6] Saidi, H., Gretete, D. and Adnane, A., "Opportunistic routing in wireless sensors networks," In Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems, pp.69, November 2017.

[7] Liu, D., et al. ,"Duplicate detectable opportunistic forwarding in duty-cycled wireless sensor networks," IEEE/ACM Trans. Netw, vol.24, no.2,pp.662–673, 2016.

[8] Shelke, M., Malhotra, A. and Mahalle, P.N., "Congestion-Aware Opportunistic Routing Protocol in Wireless Sensor Networks," In Smart Computing and Informatics, Springer, pp. 63-72, 2018.

[9] Rozner, E., Seshadri, J., Mehta, Y.A. and Qiu, L., "SOAR: Simple opportunistic adaptive routing protocol for wireless mesh

networks," IEEE transactions on Mobile computing, vol.8, no.12, pp.1622, 2009.

[10] Liu, Y., Dong, M., Ota, K. and Liu, A., "ActiveTrust: secure and trustable routing in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol.11, no.9, pp.2013-2027, 2016.

[11] Wang, Y., Zhang, M. and Shu, W., "An emerging intelligent optimization algorithm based on trust sensing model for wireless sensor networks," EURASIP Journal on Wireless Communications and Networking, vol.1, pp.145, 2018.

[12] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multihop wireless ad hoc networks," In Ad Hoc Networking, 2001.

[13] C. E. Perkins and P. Bhagwat, "Highly dynamic destination sequenced distance-vector routing (dsdv) for mobile computers," In Proceedings of ACM SIGCOMM, Aug.-Sept. 1994.

[14] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing," In Proceedings of the Workshop on Mobile Computing Systems and Applications, Feb. 1999.

[15] Pritesh Patil and R. S. Deshpande, " Trustworthy Routing in Wireless Sensor Networks Using Hop Count Filter", Int. Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-5, PP 303-313, March, 2019.

[16] Zahariadis T, Leligou H, Karkazis P, Trakadas P, Papaefstathiou I, Vangelatos C, Besson L ,"Design and implementation of a trust-aware routing protocol for Large wsns," International Journal of Network Security & Its Applications, vol.2, no.3, 2011.

[17] Babu SS, Raha A, Naskar MK, "Trustworthy route formation algorithm for WSNs," Int J Comput Appl, vol.27, no.5, pp.0975–8887, 2011.

[18] Y. Yuan, H. Yuan, S. H. Wong, S. Lu, and W. Arbaugh, "ROMER: resilient opportunistic mesh routing for wireless mesh networks," In Proc. of IEEE WiMESH, Sept. 2005.

[19] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," In Proc. of ACM SIGCOMM, Aug. 2007.

[20] S. Biswas and R. Morris, "ExOR: opportunistic multi-hop routing for wireless networks," In Proc. of ACM SIGCOMM, Aug. 2005.

[21] Yu, C.M. and Ku, M.L., "Joint Hybrid Transmission and Adaptive Routing for Lifetime Extension of WSNs," IEEE Access, vol.6, pp.21658-21667, 2018.

[22] Anupam Das and Mohammad Mahfuzul Islam, "SecuredTrust: A Dynamic Trust Computation Model for Secured Communicationin Multiagent Systems, " IEEE transactions on dependable and secure computing, VOL. 9, NO. 2, pp.261 - 274, March/April 2012.

[23] Ram Mohan Chintalapalli and Venugopal Reddy Ananthula, "M-LionWhale: multi-objective optimisation model for secure routing in mobile ad-hocnetwork", IET Communications, vol.12, no.12, pp.1406 – 1415, 31 July 2018.

[24] Félix G, M Gregorio, M Pérez, Antonio F. "TACS, a Trust Model for P2P Networks", Wireless Personal Communications, Volume 51, Issue 1, pp 153–164, Oct 2009.

[25] Xiang Gu, Jin Wang, Jianlin, Qiu, Zhengzheng Jiang, "Self-Recommendation Mechanism in Trust Calculation Among Nodes in WSN", Wireless Personal Communications, Volume 97, Issue 3, pp 3705–3723, Dec 2017.

[26] N. Karthik, V. S. Ananthanarayana "A Hybrid Trust Management Scheme for Wireless Sensor Networks", Wireless Personal Communications, Volume 97, Issue 4, pp 5137–5170, Dec 2017.

[27] Vishvas Kshirsagar, Ashok M. Kanthe, Dina Simunic "Trust Based Detection and Elimination of Packet Drop Attack in the Mobile Ad-Hoc Networks" Wireless Personal Communications, Volume 100, Issue 2, pp 311–320, May 2018.

[28] CARLOS SANTOS, AHMAD MEZHER, JUAN LEÓN, JULIAN BARRERA, EDUARDO GUERRA and JULIAN MENG, "ML-RPL: Machine Learning-Based Routing Protocol for Wireless Smart Grid Networks" IEEE Access, VOLUME 11, PP 57401 – 57414, 2023.

[29] IBRAHIM A. ABD EL-MOGHITH AND SAAD M. DARWISH, "Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach" IEEE Access, Volume 9, PP 103822 – 103834, 2021.

[30] Manaf Bin-Yahya , Omar Alhussein, and Xuemin Shen, " Securing Software-Defined WSNs Communication via Trust Management" IEEE INTERNET OF THINGS JOURNAL, VOL. 9, NO. 22, PP 22230- 22245, 2022.

[31] Zhenguo Bi, Guiying Meng, Ammar Hawbani , Sotirios K. Goudos, Shaohua Wan and Liang Zhao, "TRUE: A Correlation Analysis Approach for Conducting Optimal Routing Metrics in VANETs", IEEE NETWORKING LETTERS, VOL. 5, NO. 1, PP 55-58, 2023.