International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

Optimized and Secure Routing in WSN using Collaborative Optimized Routing Algorithm

Pritesh A Patil, R. S. Deshpande

Abstract-Optimized routing in wireless network is the trending research area in ad-hoc wireless communication. Performance of outmoded schemes designed for security during the process of routing in sensor networks significantly affected by consistency and security issues. However the present routing schemes are inexpensive and need no rigorous positioning but security is still unavoidable apprehension. An optimized routing scheme is proposed for WSN in this paper which is named as Collaborative Optimized Routing Algorithm (CORA), which precisely focuses on optimized progression of data during routing along with security aspects. CORA functions in two phases, first phase is to identify and group the collaborative nodes through defined lenient constant based on direct_trust, link_strength and quality parameters. Direct_trust and link_strength are direct measures but to evaluate quality, link survival time and caused delay are considered. Whereas in second phase suit function is defined for choosing the optimized nodes using the proposed CORA, based on direct_trust, link_strength, quality and distance. Performance of proposed collaborative optimized routing scheme is assessed based on the measurement metrics with 50 dynamic nodes ad-hoc sensor network in presence of selective forwarding and denial-of-service attacks. CORA indicates the higher detection rate and throughput as 54.9 and 41.6 respectively and lower delay and distance as 15 and 158.8 respectively which are significantly better than competing schemes.

Keywords: Optimized routing, CORA, Lenient Constant, Suit Function, Direct Trust, link strength, Quality.

I. INTRODUCTION

Industry, observing the environment, military services and civilian are the area where WSN has widespread applications. Configuration of WSN involves battery powered sensor nodes indicating restricted power competencies. To realize effective communication under narrow radio range the message initiated by a sensor node in wireless network which is sent to the base station over multi-hop path[1]. But this multi_hop routing is vulnerable to various malicious attacks which can harm the network in broader sense. With temper nodes adversary physically affect the network, cause collision in the traffic with deceptive drop of messages or may tend to misdirect the message on the path or cause the blocking of communication channel due to radio interference. Assistance among the nodes of WSN is highly essential as to hold lower energy usage, minimum cost of communication which are beneficial in observing the temperature, pressure, military service parameters, health monitoring applications etc. But limited operating power, memory capacity and security issues the unavoidable facts which make these networks suffer. These limitations of WSNs leads to confirm the estimation of network based on trust and energy values. Significant energy saving and appropriate results can be realized through ensuring security in the network[3]. Because of dynamic specifications, distributed and open nature of WSN routing is prone to various attacks[4], which affects the security and data. Limited energy creates the possibility of side-effects of typical attacks in the network and results in improper WSN deployment at the time of data movement[5].

Variation in the mechanism of routing protocols associated with the traditional networks may not be applicable to wireless network, makes the routing process complex. The main focus of routing is identification of appropriate path for carrying the information related with the selection of probable forwarding nodes. Instead of transmission medium traditional routing uses, automatic repeat request or data link strategy or forward error checking mechanism[6]. The complexity increases in routing due to follow-up of fix identified points on the routes, as the nodes are deployed on the isolated area in ad-hoc manner for various applications[7]. As best route selection is the prime requirement in routing process under WSNs and ad-hoc networks so OR is one of the area of interest of the researchers over the traditional routing mechanisms[8]. Broadcast nature of wireless medium is exploited by OR which never commit any specific path earlier to the data transfer. In other words this mechanism form one stronger link by combining several weaker links which tends to many advantages during communication [9]. Additionally, enhancement of route success possibility as secure route policy is done by the preferred strategy. Prime requirement is to generate the route through identified nodes with highest trust factor as they possess greater probability in realizing the efficient routing so that the generated routes in this manner effectively forward data to base station with high probability [10]. Under the situation of malicious node attack the trust based management scheme considered to be the effective and prevalent scheme. As it is known that the trust-evaluation scheme holds less computations and minimum communication load which is the great benefit of the scheme while focusing on the internal attacks during identifying malicious node[11].

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Pritesh Patil*, E&TC Department, VIIT Pune, Affiliated to Savitribai Phule Pune University, Maharashtra, India. Email: p.patil.k@gmail.com
Dr. R. S. Deshpande, Principal, SCSMCOE, Nepti, Ahmednagar, Affiliated to Savitribai Phule Pune University, Maharashtra, India, Email: raj.deshpande@yahoo.co.in

Outmoded routing schemes transfer the traffic over determined paths and incurs difficulties during copying the undependable and unpredictable wireless medium. The existing routing schemes, such as Dynamic Source Routing (DSR) [12], Sequenced Distance Vector routing (DSDV) [13], Ad Hoc On-Demand Distance Vector Routing (AODV) [14] etc. are mentioned as traditional routing schemes[9].In Ambient Trust Sensor Routing (ATSR) [16] reliability of nodes are assessed through distributed mechanism, where monitoring of node's behaviour carried out depending on the precise trust compositions and calculates the direct trust about its neighbours. Whereas direct and indirect trust were considered in Trust dependent Link State Routing Protocol (TLSRP) algorithm[17].However confrontation of nodal attacks was not calculated. Trust-Aware Routing Framework (TARF) [2] in WSN is termed as multipath routing protocol which calculates the trustworthiness of the neighbours, defines the untrusted nodes and overlooking routing dependency on energy efficacy and calculation of trust[3].As a part of assisting OR, each node maintains routing table where default route refers to the shortest route with respect to source and destination nodes and the forward list is the composition of nodes for next_hop which are then the probable forwarder of the data. ROMER[18] is the OR that forward the multiple packets simultaneously over more than one path whereas MORE[19] incorporates network coding for the same and ExOR[20] is based on the random coding to realize multiple paths.

Organization of rest of the paper as: Related work in section 2. Proposed framework of Collaborative and Optimized routing in section 3. Results and discussion along with comparison with competing methods and effectiveness of CORA are presented in section 4 and at the end section 5 concludes the paper.

II. RELATED WORK

A brief review of the schemes is described in section 1, however a more detailed comparative schemes reported in the literature are presented in this section. Providing security in WSN is still a point of attraction of the researchers. Significant complexity incurred in protecting WSN routing against attacks. Also it is difficult to find the optimal solution besides protecting the network.

Trust-Aware Routing scheme is proposed in [2] which reduces the efficiency of routing schemes while integration with the present protocols possessing deprived strength. The method fails to address the attacks due to injection of many data packets comprising wrong sensing information. The mechanism also condenses light defense against identity theft through replaying routing information. An attacker can explore the faults in confessing several devastating attacks on the process of routing based on identity deception.

Parma, F., [3] presented an Energy-aware Trust-based Gravitational Search Approach (ETGSA) which selects the best route depending on the hop_count, trust, energy and rate at which the traffic is flowing on routes and imposed low network overhead. But if there are two or more sinks which is usually in case of clustered WSN this method is not efficient.

TSSRM which is Trust sensing based secure routing mechanism is proposed by Qin, D., *et al.* [5] to enhance the protection and undertook the popular network threats. The computational overheads of routing related with the technique was improved, due to which reliable data transmission is realized. There is a lack of distributed intrusion detection in this method which renders alternative way to re-search the trust degree and pervasive routing. This method is dependent on the precise route as it is based on the degree of trust which incurs certain limitations.

There exists many opportunistic routing protocols available and the most common challenge is to maximize the progress of transmission, by overcoming the duplication of packet at the same time[6].

Congestion-aware opportunistic routing proposed by Shelke M., *et al.* [8] which minimizes the load of traffic in the network to realize stable performance. Sleep scheduling is out of the scope of this method, which actually reduce the energy consumption and delay.

Simple Opportunistic Adaptive Routing protocol (SOAR)[9] is developed to identify and select potential forwarders and employs priority_based timers. Multiple transfer flow is effectively handled and higher efficiency achieved by this method. As MAC layer does not offer reliability support for broadcast, data packets broadcasted by the nodes becomes victims of packet losses and corruption. This method also lagging in selection of default path which improves the performance.

Active_Trust scheme presented in [10] attained successful routing probability, scalability, energy efficiency, significant degree of security and higher data rate between sink and nodes near to it. This causes unnecessary energy consumption which leads to the failure of the method. Network lifetime is degraded significantly as trust gaining and release causes higher energy consumption thereby it becomes hard to detect malevolent nodes.

An Ant colony optimization algorithm for secured routing (ACOSR) scheme proposed by wang et. al.[11]which reduces loss of packets and maintains secured routing. Alongside, amount of used energy by the nodes is efficiently balanced and network energy consumption is reduced significantly so as to increase the network lifetime. However this scheme required the estimation of the nodes in the complex state of the attacks.

Two optimization techniques i.e. power efficiency and power utilization optimization techniques are proposed in[21] that achieved three times network lifetime. Irrespective of size of the network this technique shows improved energy usage. Higher computation and communication overheads are the main drawbacks of this scheme.

Another trust based model for P2P Networks based on ant colony system is developed[24], which is efficient enough to select trusted server upto a great percentage. Leftover essences by ant are the base criteria for determining the level of trust of the neighbours by the source. But, identity deception through replaying routing information is not successfully defended by this scheme.

In [25] a self_recommendation technique is presented to evaluate trust value between the nodes of WSN. The main focus of this approach is to maintain the level of energy and based on that level calculation of trust carried out. Routing and network will be severely affected by the devastating attacks causing identity theft and false advertisement that they have high energy values, will results in inability to identify and select optimal route for transmission.

Another trust management scheme presented by Karthik et al. [26] is Hybrid Trust management scheme (HTMS) that functions on two factors, first is strength of node and second is data originality. Marks are assigned to the data originated based on the metrics node linkage and source of data. Depending on these assigned marks further routing decisions were made. Adversaries can easily manipulate the basic details due to which reliability of data based on source cannot be realized.

Packet drop attack identification and avoidance scheme proposed by vishwas et al. [27] for ad-hoc networks. Trust list is maintained in this approach which indicate how many time nodes participated in routing process. Selfish and Un-selfish nodes are distinguished through trust and energy values. But this method is not suitable for the resource constrained WSNs as it incurs significant amount of computation overheads.

The main intent of this work is to propose and implement a collaborative optimized routing scheme in WSN. Collaboration of trust and opportunity based schemes is carried out to realize a new framework in such a fashion that nodes of network participate in the process of routing and guarantee security. The first phase of the proposed scheme focuses on the identification and selection of secure nodes which ensure security in the group communication in network depending on fitting criteria. Then in second phase, routing is performed based on trust and opportunity to realize the best optimal solution.

III. DESIGN OF COLLABORATIVE OPTIMIZED ROUTING FRAMEWORK

Engagement of routing schemes is to determine the suitable and optimal route to experience routing in WSN and there are numerous protocols assuring this optimal route detection and selection. Though the noteworthy constraints trust and energy empower effective routing with trust in WSN. Existing schemes functions with high computational complexities, to significantly reduce this extra overhead along with the capability to handle multifaceted threats, a scheme is proposed. So to realize security alongside optimization also in the network, the Collaborative and Optimized Routing Algorithm (CORA) is proposed. The name given as collaborative because in our earlier work[15] we considered nodes are static in nature and routing is restricted to identified path. But in real time application scenarios the position of nodes is not fixed at one location, they may move along with the object on which they are mounted. Due to this reason the existing routing schemes are not the suitable alternative. Also it is essential for the scheme to generate more than one routing opportunities for source nodes in this scenario. By considering these aspects, proposed collaborative routing framework functions on two phases. The first phase focuses on identification and selection of collaborative nodes out of all initialized nodes. In this phase the scheme acquires trusted and adaptive structure of routing to effectively tackle threats and ensures higher degree of defense against selective forwarding and Denial of Service (DoS) attacks. Process of selecting collaborative nodes is performed through the Lenient Constant (LC) defined using parameters trust, link and quality. Description of these parameters are detailed in 3.1 next sub_section.

Simulation of WSN for N total nodes carried out at start and collaborative nodes are selected based on the LC which are to be passed to second phase of proposed framework. Focus of second phase is to make packets greedy and additionally optimization of utilization of crucial network resources viz. memory and successful end-to-end transfer in any routing communication is carried out. Optimal routing is performed using CORA and route identification and selection process is depending on the Suit Function (SF) which has four parameters, trust, link, quality and distance. Thus optimal routing alongside ensuring trust is performed in WSN scenario. Figure 1 represents the architectural block diagram of proposed routing scheme.

3.1 IDENTIFICATION OF COLLABORATIVE NODES:

To ensure security in the network, collaborative nodes are identified using formulated Lenient Constant (LC). Computation of lenient constant is based on three parameter, trust, link and quality, which should be high and strong. The lenient constant LC is computed as,

$$LC = [DT_i + LS_i + Q_i]/3 \qquad (1)$$

where, DT_i refers to the direct trust of i^{th} node, LS_i indicates the link strength of i. M collaborative nodes are identified and selected from initiated N nodes such that $(M < N)$. The node which acquires highest trust value, link strength, and maximum quality is chosen as collaborative node whereas isolated nodes are simply rejected in taking part in communication. Quality parameter Q_i strictly depends on the highest Link_Survival_Time (LST) and lowest delay, of nodes in network.

3.1.1 Direct Trust (DT): Local trust is also termed as Direct Trust [22] that depends upon the approval and degree of approval during interaction between nodes. D T_i among i and j nodes depends on degree of approval between them. On the moment when j senses comfortable with i, the degree of approval is high and indicating the local trust. Computation of degree of approval app_{ij} among j and i is depending on the completed transactions C_{ij} and number of nodes in network as follows:

$$app_{ij} = \frac{C_{ij}}{N} \qquad (2)$$

Here completed transactions happened between the i and j is denoted as, C_{ij} and N indicates total nodes.

3.1.2 Link Strength (LS): The link strength defines the connectivity present between the nodes and the link bi-directional links joining the nodes. The Link Strength (LS_j) of the nodes is computed as,

$$LS_j = \frac{1}{N}\left[\sum_{i=1}^{N} \frac{LS_i}{c} \cdot\right] \qquad (3)$$

where LS_i denotes link strength of i^{th} node, and c is total connections.

3.1.3 Quality: Link_Survival_Time (LST) and delay are the base for computation of quality. There is association of LST with survival_time of the network. LST of nodes depends on the existing connections among the nodes [23]. The dominant link during data transfer is determined and is involved in communication process to activate the link and to realize transfer without any data loss or

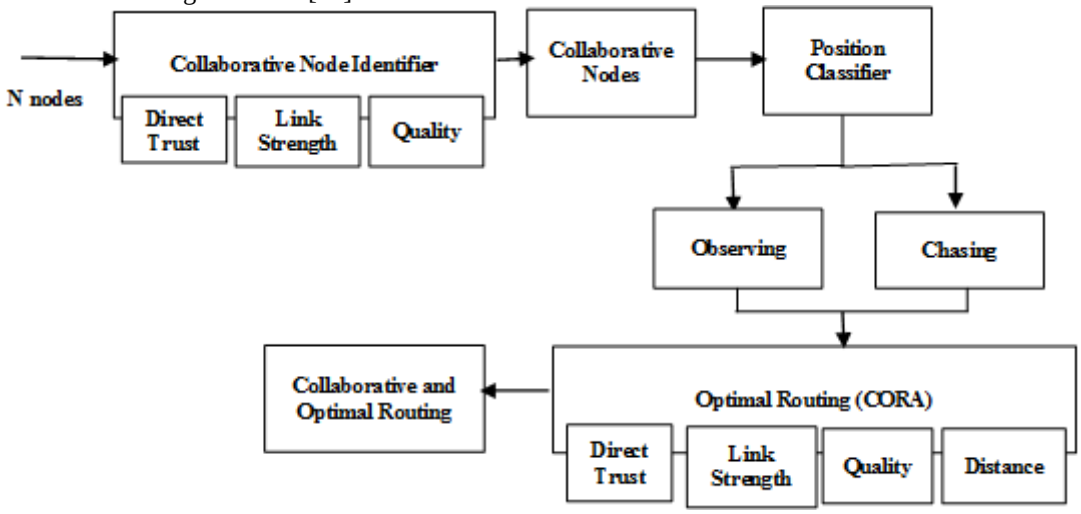


Figure 1: Architecture of Collaborative Optimal Routing Scheme

delay. Evaluation of LST becomes essential as WSNs suffer from link loss issues due to dynamic nature of network. There is a need to reduce the possibility of link breakages to effectively choose the path for communication. Movement of nodes, direction of movement and their locational coordinates under the area are the basis for computation of LST. The ratio of number of nodes alive on the current route to the total number of nodes of the network, is used to evaluate delay d_j of node j. Hence the quality of j^{th} node is expressed as

$$Q_j = LST_j + d_j \qquad (4)$$

Finally the lenient constant can be expressed as

$$LC = \left[\frac{C_{ij}}{N} + \frac{1}{N} \left[\sum_{i=1}^{N} \frac{LS_i}{c} \cdot \right] + (LST_j + d_j) \right] / 3 \qquad (5)$$

3.2 COLLABORATIVE OPTIMIZED ROUTING ALGORITHM(CORA)

The collaborative nodes are identified and classified through the lenient constant (LC)and these nodes take part in the routing, which is progressing depending on the optimized routing algorithm. By setting the source, destination and collaborative nodes to generate routing paths through optimization. The source and sink nodes are decided and v is the number of nodes involved in secure routing and v number of collaborative nodes are selected based on optimized routing algorithm CORA depending on Suit Function (SF).

3.2.1 Encoding Vector

The encoding vector is the demonstration of probable solution to be evaluated using CORA algorithm. Composition of encoding vector is the nodes in-between involved in the process of routing and the number of in-between nodes are represented as, v . Here v varies between 1 to M , where M is the total number of the collaborative nodes in the session. Encoding vector is shown in figure 2,

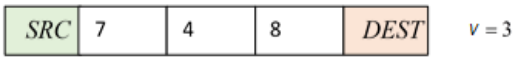


Figure 2. Encoding Vector

Here 7, 4 and 8 are the collaborative nodes through which the data transmission will take place to reach destination in case when $v = 3$.To identify and select the optimal collaborative nodes is done through CORA which based on Suit Function. Encoding vector operates among source and destination, with the similar format used by other paths originated for routing purpose.

3.2.2 Suit Function (SF)

Suitability measure ensures, selection of optimal collaborative nodes to perform the collaborative routing in WSN and suitability should have maximum value. Simply stating, for the solution to the problem of maximization, suitability needs to be effectively calculated. Suit function is formed based on the direct trust, link strength between adjacent nodes, Quality of the nodes, and distance among these nodes. The Suitability is formulated as,

$$SF = \frac{1}{4} \left[\sum_{i=1}^{v} DT_j + LS_j + Q_j + \left(1 - D_{i,i+1}\right) \right] \qquad (6)$$

Here the distance among the two adjacent collaborative nodes i and $i+1$ is denoted by, $D_{i,i+1}$ .For maximization of the suitability, solution should possess the maximal values of Direct Trust (DT), Link Strength (LS) and Quality of node (Q), however distance should be minimum. The distance factor in SF formulation should have the minimum value so, it is defined in the function by subtracting $D_{i,i+1}$ from 1 realize the maximum value of SF.

3.2.3 CORA Algorithm

Acquisition of comprehensive optimized solution and complex_free computation are the major capabilities of the proposed Collaborative Optimized Routing Algorithm.

As, in the network of resource constrained WSN, nodes are dynamic in nature in most of the real time applications, CORA effectively handles this situation. Optimization of effective utilization of network resources is realized through arranging the collaborative nodes in two sections, first is observing and the other is chasing. This classification inherits the behaviour of cats, as most of the time they are observing and when they find favourable opportunity they instantaneously react to trace the object and get success maximum time. Restoration of energy is the incredible capability of them as time of hunt is significantly less, is their precise characteristic. Technically stating that the investigation and manipulation phases of algorithm condense optimum solution having high coupling rates. Simply stating, the collaborative nodes are divided into two sets. First set consisting of the nodes in observing mode and the other is in chasing mode. In chasing subset the collaborative nodes take less time to reach to the expected hop or destination so the number of nodes in this set is less. Current position and suitability are computed for getting the updated solution, which is saved. These steps are repeated for maximum number of time till the best optimum solution. Location of the collaborative nodes when they are in chasing mode in CORA are fixed using the following rule:

$$L_{i,q}^{t+1} = \frac{1}{\left[R_1 * \gamma_1\right]}\left\{\left[-\beta \times \left(S_q - 0.5\right)\right]\left[1 - R_1 * \gamma_1\right] + v_{i,q}^{t} + R_1 * \gamma_1 * L_q^{*}\right\} \qquad (7)$$

here, $L_{i,q}^{t+1}$ is the location of the collaborative node at instant $(t+1)$, $L_{i,q}^{t}$ specifies the location of the collaborative node. $L_{i,q}^{t+1}$ and $L_{i,q}^{t}$ are the solutions at instants $(t+1)$ and t, $v_{i,q}^{t+1}$ is the velocity of these nodes at instant $(t+1)$, S_q is the convergence speed of the nodes and R_1, β are the random number varying between 0 and 1. Velocity of i^{th} node in q^{th} dimension, $v_{i,q}^{t+1}$ is expressed as,

$$v_{i,q}^{t+1} = v_{i,q}^{t} + R_1 * \gamma_1 \left(L_q^{*} - L_{i,q}^{t}\right) \qquad (8)$$

where γ_1 is a proportionality constant. To realize optimization, initially the total nodes (N) are initiated, expressed as,

$$N_{iq}; \left(1 \le i \le CN\right) \qquad (9)$$

where, CN refers to the total collaborative nodes and search area dimension is given by q .Optimization starts by randomly describing the location and migration velocity of collaborative nodes which is then followed by observing and chasing modes. Firstly, the location and velocity of nodes are initialized randomly, then arranging the nodes in observing and chasing groups. Swapping among these modes is based on Self-Location Attention (SLA) which has boolean value 1 for observing mode and 0 for chasing. SLA is defined for all the instances of the nodes and is generated randomly for given instances t .Depending on the situation of condition collaborative nodes perform traversal, otherwise they remain idle but alert in observing mode. In the seeking mode, the cats remain quite for some time and in this phase, the cat traverses slowly according to the environment. At the start of rounds the copies of i^{th} node is formed and instructed to analyse their Acquisition Memory Buffer (AMB). The copies are continued to acquire fresh copies of the node, their modified locations are updated on the basis of present location of node, the selected dimensional area (SD) and random number.

The location of node is indicated as $L_{i,q}^{t+1}$ and is expressed as follows,

$$L_{i,q}^{t+1} = \left(1 \pm SD \times \beta\right) \times L_{i,q}^{t} \qquad (10)$$

The suitability associated with the locations of collaborative node is evaluated and confirmed to 1 which indicates the discrete solution. But when it is not 1, in that case probability of finding discrete solution is expressed as,

$$P_i = \frac{|SF_i - SF_\omega|}{|SF_{max} - SF_{min}|} \qquad (11)$$

where, P_i is the probability of i^{th} collaborative node, SF_i is the suit function of i^{th} node, SF_{max} is the maximal value of SF, and SF_{min} is the minimum value of SF. SF_ω has the maximum value of the suitability for the problem of minimization and has minimum value for the problem of maximization. Furthermore based on the value of SLA parameter decision on the modes is taken. When SLA is not 1 then, collaborative node is initiated in chasing mode to hunt for the fittest forwarder. After the successful identification, based on proposed CORA, the location and velocity of that chasing collaborative node are updated accordingly.

Moreover, after fixing the locations of the nodes in either observing mode or chasing mode, calculation of best suitability measure P_{best} of the updated solution is done. The suite function should have maximum value as far as selection of optimal and effective solution is concern, which means the optimal collaborative nodes engaged in the process of routing.

Lastly, the end of the optimized routing process is verified through the stopping criteria which is defined to obtain improved effect of algorithm comprises of exhaustive iterations, percent of improvement and execution time.

For the continuation of routing process between source and destination through collaborative nodes is realized on the basis of proposed collaborative optimized routing algorithm (CORA). The algorithmic steps of CORA are shown in algorithm 1.

Algorithm 1 : *Collaborative Optimized Routing*
Input : *Group of Nodes*, L_{iq} *,with M Collaborative Nodes*
Output : *Best Suitability Measure*, P_{best}
Begin
  Initiate Nodes
While $(t < t_{end})$
  Suitability Evaluation
Evaluate best suitability Measure, P_{best}
for $(t < t_{end})$
If $(SLA = 1)$
Collaborative nodes update their location in observing mode using eq 10
Else
Collaborative nodes update their location in chasing mode using eq 7
End If
End For
End While

IV. RESULTS AND DISCUSSION

Experimental observations and effectiveness of CORA is presented in this section alongside the comparison with competing methods. The proposed CORA is implemented in NS2 platform and the performance is computed based on the performance metrics distance, delay, detection_rate and throughput. In addition to the comparative analysis with existing techniques, network analysis is carried out for network in existence of selective forwarding and Denial-of-Service attacks.

Simulation setup with 50 nodes is shown in figure 3 in which source, destination and the attacker nodes are highlighted. Interactions and communication happens in this network through the collaborative nodes.

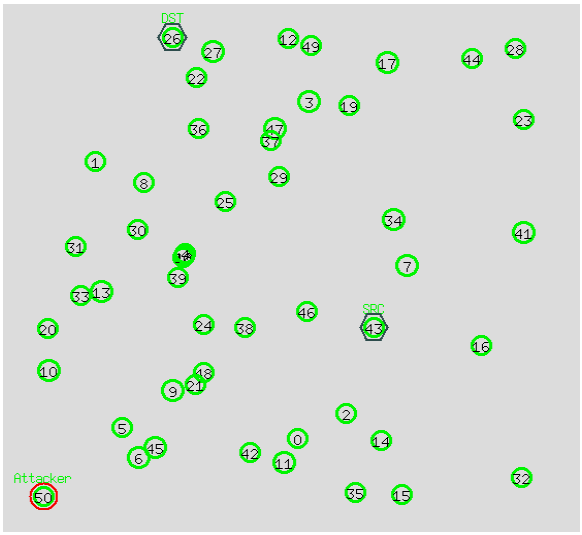


Figure 3.Simulation Setup with 50 nodes

4.1 PERFORMANCE MEASUREMENT METRICS

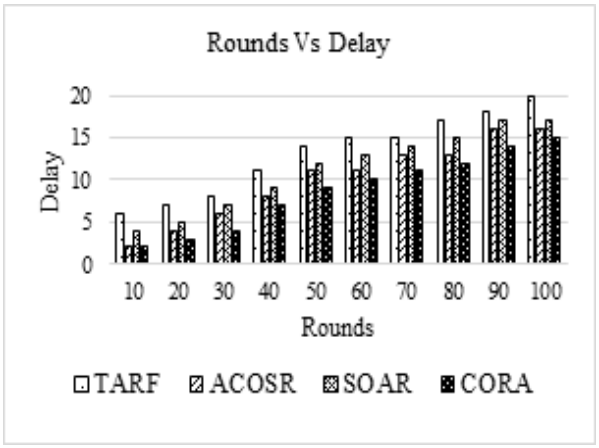
Delay, distance, detection rate and throughput are the parameters considered for the evaluation of performance of the proposed method. Data rates within a particular time frame over the network is the measured as throughput. Delay is the time consumption during the data transfer with or without the presence of attack in the network. Detection rate here is considered as the accurate and precise attack detection. Efficient scheme exhibits the performance with higher throughput, energy and detection rate and lowest delay. Distance between the collaborative nodes for data transmission should be less to realize high performance of the scheme. The proposed scheme is analysed for the effective performance under the presence of selective forwarding and DoS attacks.

4.2 PERFORMANCE INVESTIGATION AND ANALYSIS

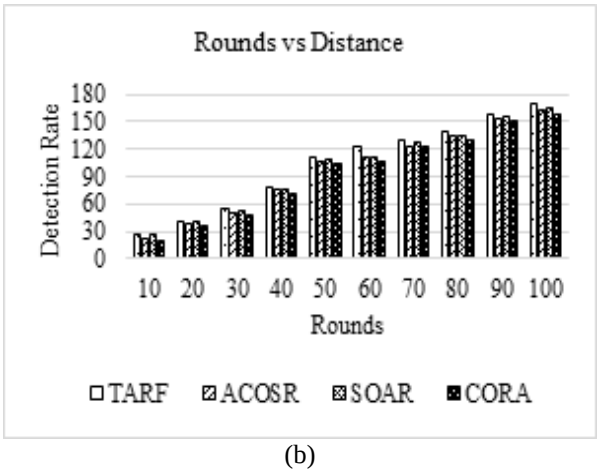
The performance of proposed CORA is investigated in the presence of two attacks, based on the performance parameters mentioned earlier and then it is compared with Trust Aware Routing Framework (TARF) [2], Simple Opportunistic Adaptive Routing protocol (SOAR) [9], and Ant colony Optimization for secured routing protocol (ACOSR) [11]. Comparison results indicate the significant performance improvement as compared to these competing schemes. Network of 50 nodes are formed where nodes are dynamic in nature to proceed to the analysis phase in NS-2.

In presence of Selective Forwarding attack: Analysis based on performance evaluation measures mentioned above, in presence of selective forwarding attack is shown in figure 4. Figure 4a) indicates the delay based analysis, which should be minimum to realize effective scheme. After the 100 rounds the delay observed of the methods TARF, ACOSR, SOAR and CORA are 20, 16, 17 and 15 secs respectively. For efficient performance the distance should me minimum and

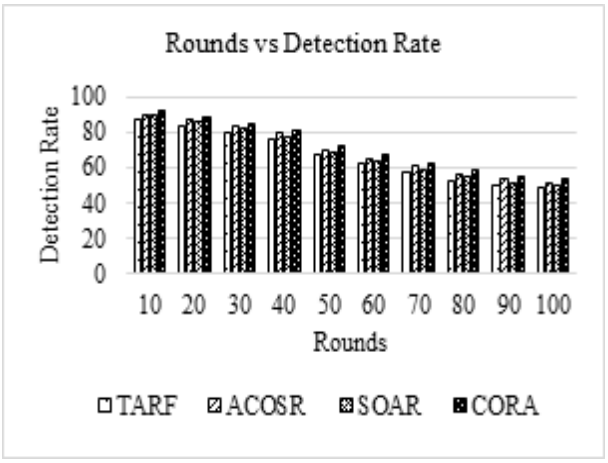
figure 4(b) indicates that after all prescribed rounds the distance of these methods TARF, ACOSR, SOAR and CORA respectively are 168.9, 163.4, 163.7 and 158.9. Detection rate should be significantly higher for the effectiveness of the method and after considered rounds for evaluation the detection rate observed for methods TARF, ACOSR, SOAR and CORA are 48.24, 51.01, 49.55 and 53.25 respectively as shown in figure 4c). Moreover for the effectiveness of routing scheme the throughput should be higher. Figure 4d) indicates 38.39, 40.21, 39.4 and 41.38 as throughput of methods TARF, ACOSR, SOAR and CORA respectively after final round. With the help of obtained results it is clear that the proposed method CORA indicates minimum delay and distance where as it indicates higher detection rate and throughput as compare to the existing methods.



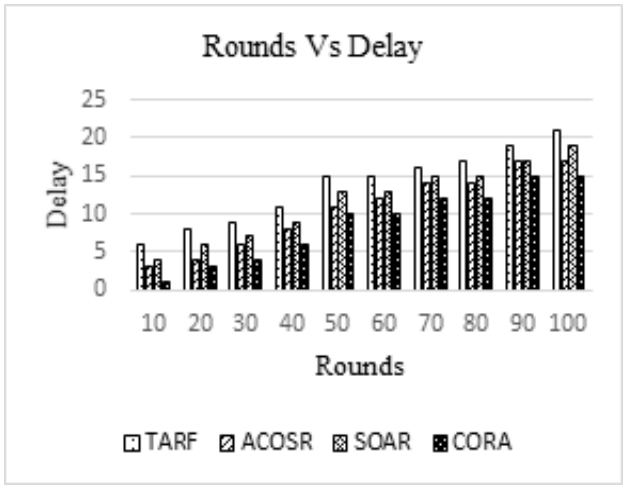
(a)



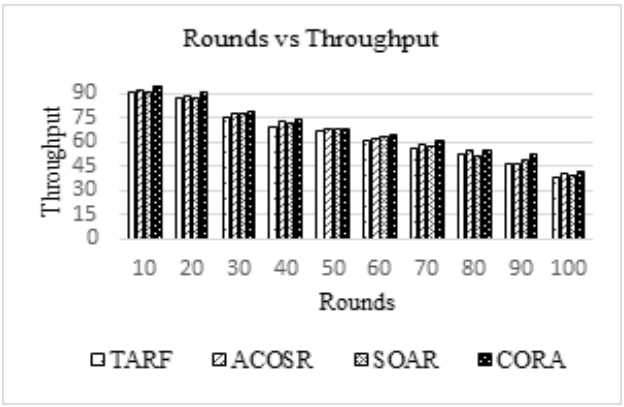
(b)



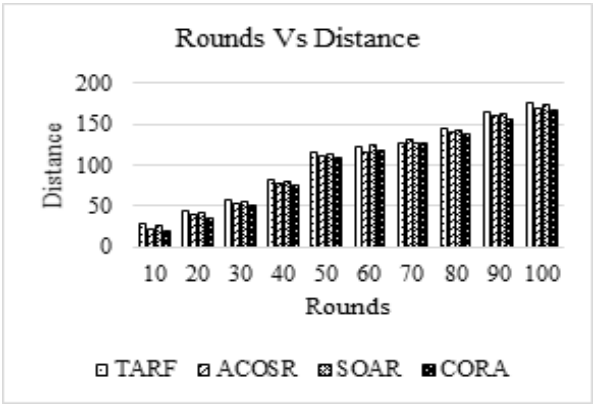
(c)



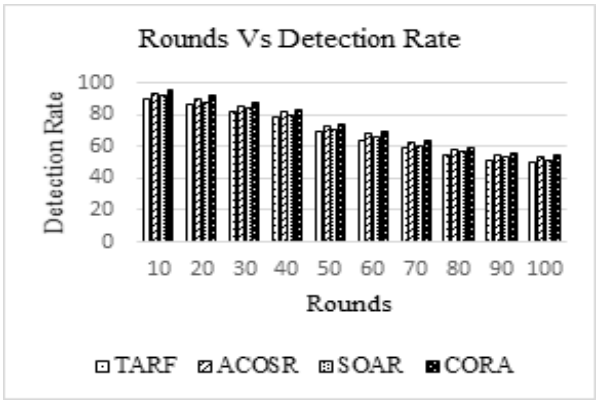
(a)



(d)



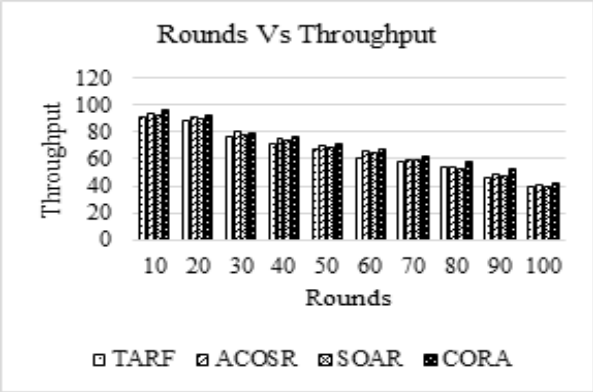
(b)



(c)

Figure 4: Performance of CORA with Selective Forwarding attack.

In presence of Denial-of-Service attack: Analysis based on performance evaluation measures mentioned above, in presence of Denial-of-Service attack is shown in figure 5. Figure 5a) indicates the delay based analysis, which should be minimum to realize effective scheme. After the 100 rounds the delay observed of the methods TARF, ACOSR, SOAR and CORA are 21, 17, 19 and 15 secs respectively. For efficient performance the distance should me minimum and figure 5(b) indicates that after all prescribed rounds the distance of these methods TARF, ACOSR, SOAR and CORA respectively are 175.1, 168.9, 173.6 and 165.6. Detection rate should be significantly higher for the effectiveness of the method and after considered rounds for evaluation the detection rate observed for methods TARF, ACOSR, SOAR and CORA are 49.69, 52.97, 51.62 and 54.87 respectively as shown in figure 5c). Moreover for the effectiveness of routing scheme the throughput should be higher. Figure 5d) indicates 39.12, 40.92, 39.69 and 41.61 as throughput of methods TARF, ACOSR, SOAR and CORA respectively after final round. With the help of obtained results it is clear that the proposed method CORA indicates minimum delay and distance where as it indicates higher detection rate and throughput as compare to the existing methods.



(d)

Figure 5: Performance of CORA with Denial-of-Service attack.

V. CONCLUSION

Collaborative routing is performed in WSN through optimization and opportunities, which is implemented in two phases, collaborative node selection and optimization. In the first phase, the Lenient Constant (LC) is defined and calculated which separates the probable collaborative nodes from the initialized nodes, based on parameters direct_trust, link strength and quality. These identified collaborative nodes are only allowed to get involved in the process of routing whereas the other non-suited nodes are simply restricted to take part in routing. In the second phase, optimization is incurred based on the proposed Collaborative Optimized Routing Algorithm (CORA). CORA operates on the defined Suit Function (SF) which is modelled based on the parameters direct_trust, link strength, quality and the distance. Initially the identified collaborative nodes are kept in two modes accordingly i.e. observing and chasing. Encoding vector then help the network to select the probable collaborative nodes between the source and destination communication. CORA is implemented through the simulation setup with 50 dynamic nodes for WSN. Performance analysis is carried out based on metrics delay, distance detection rate and throughput in the presence of selective forwarding and DoS attacks. Effectiveness of the method is revealed through the results of simulation, compared with the considered existing methods as it indicates distance and delay of 158.9 and 15 respectively, which are minimum and the detection rate and throughput of 53.5 and 41.6 respectively, which are higher.

Reducing computational overheads is always a prime focused challenge in design of robust routing algorithm. Further this method can be explored to develop more specific optimized and robust routing mechanism to reduce this factor based on the requirements of specific applications.

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.

AUTHORS PROFILE

Pritesh A Patil is working as assistant professor in Information Technology Department of All India Shri Shivaji Memorial Society's Institute of Information Technology, Pune, MS, India since 2009. His research interest are Mobile Computing, Wireless Sensor Networks and Applications, Database Optimization and Internet of Things. He has several publications in UGC approved and SCOPUS index Journals. He is PhD research scholar at E&TC Department, VIIT,, Pune, MS, India (Savitribai Phule Pune University, Pune).

Dr. Rajkumar S. Deshpande is currently working as Principal and Professor at Shri Chatrapati SMCOE, Ahmednagar, MS, India. He has completed his Ph.D. at Rajiv Gandhi Prodyogiki Vishvidyala, Bhopal (Research at Gunma University, Japan) in 2009. He is having more than 30 years of academic and research experience. He ha published more than 45 research papers in reputed journals such as IEEE Sensors, Ad Hoc sensor and Wireless Networks. He has also authored a book entitled "ATM Congestion Control Mechanism in Wired and Wireless Network" with Himalaya Publishing House. He has professional membership of IEEE, IEICE Japan and Senior Fellowship of the Institute of Engineers, India. He is a recipient of National Merit Scholarship, India in 1981. He is also a registered Ph.D. guide with E&TC Department, VIIT, Pune, MS, India (Savitribai Phule Pune University).