Secure and Opportunistic Routing in WSN using Associative Secure Optimized Routing Algorithm

Pritesh A Patil, R. S. Deshpande, P. B. Mane

Abstract*: Under wireless communication domain optimized routing for wireless networks is the trending scenario for research. Various older schemes faces performance issues such as consistency, alongside ensuring routing security which significantly causes performance degradation. Although the current mechanisms designed for routing are low-cost and precise positioning is also not essential but security still requires emphasis to be given during design. In this paper a secure and optimized routing technique is proposed for WSN mentioned as Associative Secure Optimized Routing (ASOR) Algorithm. Optimized data progression is the prime focus of ASOR alongside ensuring security to it. ASOR operates in two phases, in first phase it identifies and club the associative nodes based on the defined indulgent constant(IC) based on explicit trust, strength of link and link_quality parameters. Explicit trust and strength of link are directly measurable however to measure quality, survival time of link and the incurred delay are taken into consideration. Secondly the selection of optimized nodes using proposed ASOR is carried out through defined aptness function(AF) which is dependent on explicit_trust(ET), strength_of_link(SOL), node_quality(NQ) and distance. Proposed associative secure optimized routing scheme's performance is evaluated based on metrics for adhoc sensor network of 100 dynamic nodes in the presence of worm_hole and black_hole attacks. Comparatively higher throughput and detection_rate whereas lower distance and delay are indicated by ASOR, which are relatively better than opposing methods. ASOR shows significantly high detection_rate and throughput as 55.7 and 44.1 respectively and comparatively less delay and distance as 13 and 168.2 which are significantly better than opposing methods. ASOR can be effectively used in WSN for real time application such as in agriculture, industries etc.

***Keywords* : Optimization in routing, ASOR, Indulgent Constant, Aptness Function, trust_level, strength of link, link_quality.**

I. INTRODUCTION

Industries, weather forest, civilian and military services are some of the key areas and scope for applications of WSN. WSN mechanism consists of battery operated nodes that indicates constraints on power usage by these nodes. Multihop path is incorporated by wireless sensor network for the effective communication over very limited radio range to handover the message initiated by node to base station[1]. Various severe attacks harm this multihop communication vulnerable which can further damage the network upto great extent. Through these affected nodes attacker can harm physically to the network, which may cause traffic collision or message drop or cause message misdirection or results in blockage of communication medium because of interference.

Coordination between nodes is required to control power and energy usage and low-cost end-to-end communication which are essential as to hold lower energy usage, minimum cost of communication which are useful in monitoring environmental conditions, various crucial parameters of military services, applications observing human health etc. But these networks suffer due to limitation of operational power, storage capacity and also due to challenges in provision of security. These limitations leads to consider and estimate the values of trust and energy for the network. Substantial saving of energy and desired outcomes can be obtained by making the security provisions in the network[3].

Dynamic and distributed feature of routing in WSN attracts it to various savior attacks, due to which both data and security are compromised[4].

There are possibilities of bad impact of these attacks in network which causes improper deployment of WSNs during movement of data in it[5].

Deviation in the configuration of routing mechanism designed for outmoded networks might not be suitable for wireless networks and creates complexities in the process of routing. Prime focus of routing is to identify best suited path to carry related information alongside selects appropriate forwarders. Automatic repeat request or suitable data link mechanism or complex error checking method is used by traditional routing schemes instead of transmission medium[6].

Significant complications increase in routing because of the continuation of identified rigid node locations on routes, as for many applications these nodes are dispersed and installed on remote area in ad-hoc fashion[7]. Opportunistic Routing(OR) is the key interest of various researchers as their prime intention over traditional routing methods, is to select the best possible route for WSNs and ad-hoc networks[8].

OR actually exploit the broadcast nature of wireless transmission medium which never binds itself to the specific route before transmission of data. More simply, several weak links are combined to form one strong link which leads to several benefits during data transfer and communication[9].

Manuscript published on January 30, 2020.
* Correspondence Author

Pritesh A Patil*, Assistant professor, Department, Information Technology of All India Shri Shivaji Memorial Society's Institute of Information Technology, Pune, India

Dr. Rajkumar S. Deshpande, Principal, JSPM's Imperial College of Engineering and Research, Wagholi, Pune, India.

Pradeep B. Mane, Principal, AISSMSs Institute of Information Technology, Pune, India.

Moreover, increase in the possibility of success of route selection as policy for secure route is carried out by the desired routing policy. Major constraint is to generate a route with the inclusion of nodes identified with comparatively greater trust measure, because they indicate highest likelihood for efficient route realization so as the identified routes this way efficiently forward information to sink with highest probability[10].

In the presence of attack caused by malicious node the scheme based on trust management is realized as most prominent and efficient scheme. Due to this internal attacks can be focused as scheme evaluating trust values incurs less computational overheads and also communication load is minimum, which indicates significant advantage in recognizing malicious node[11].

In traditional schemes of routing data transfer takes place through fixed identified routes which then suffer from the difficulty at the time of copying the unreliable and irregular wireless medium. Ad Hoc On-Demand Distance Vector Routing (AODV) [14], Dynamic Source Routing (DSR) [12], Sequenced Distance Vector routing (DSDV) [13] etc. are termed as traditional routing methods [9]. Reliability of nodes are evaluated using distributed scheme in Ambient Trust Sensor Routing (ATSR) [16], wherein node's behaviour monitoring process is initiated based on the actual trust mechanisms and direct trust is calculated against its immediate neighbouring nodes. Moreover direct and indirect trust were taken into consideration in Trust Dependent Link State Routing Protocol(TLSRP) scheme[17] except the calculation of confrontation of nodal attacks. Another promising multipath routing scheme Trust-Aware Routing Framework (TARF) [2] in WSN in which trustworthiness of neighbours is calculated, overlooks the routing dependencies on efficiency of energy usage and computes trust[3]. To support Opportunistic Routing(OR), every node prepare and maintain routing information in table in which default route indicates the shortest route between source and destination, also and the list of forwarders is consisting of next_hop nodes which will be then become the potential forwarders of the initiated data. Possibility of more than one path is created to forward packets simultaneously through OR is done in ROMER[18] however network coding technique is used for the same purpose in MORE[19]. Unicast routing for multihop wireless network is performed through MAC protocols in[20]

Rest of the paper is organized as: Section 2 presents the related work. Framework of proposed Associative Secure and Optimized Routing is detailed in section 3. Discussion on obtained results along with performance comparison with opposing methods and effectiveness of ASOR are presented in section 4 and section 5 concludes the paper with key observations and scope for extension.

II. RELATED WORK

In addition to the brief review of methods presented in section I, a more detailed review of compatible methods mentioned in the literature is given here.

For researchers, provision of security to routing in WSN is still a topic of interest. Protection of WSN and routing process from attacks make the routing process complex. Getting optimum solution will be difficult besides protection of network from threats.

A trust_based routing scheme presented in[2] significantly reduces the efficiency of the routing protocol at the time of integration with the existing routing schemes having poor strength. But it failed to address the attacks injecting packets having wrong sensing information. Also this scheme does not provide significant defense from the attacks caused due to identity theft which replays the routing information. Faults can be easily explored by the attacker during routing process through identity theft.

An energy and trust based routing presented by Parma. F., [3], in which the best route is selected based on the hop_count, trust, energy and rate of flow of traffic on various routes and realized overhead on the network. However in case when WSN have more than one sink such as clustered WSN then this scheme shows inefficiency.

Qin, D. et al. [5] presented trust based secure routing method TSSRM to increase protection and undertook the common network attacks. Routing's computational complexities were improved as a result the reliability in data transmission is achieved. Distributed intrusion detection is missing in this scheme that condenses another way to find and evaluate degree of trust and prevalent routing. TSSRM rely on the specific route because it strictly dependent on degree of trust, due to which, certain limitations incurred in the process. There are several opportunistic routing schemes available and in all schemes the common requirement is maximizing the progression of the transmission while disabling the packet duplication at that time[6].

To minimize the traffic load inside the network for performance stability congestion-aware opportunistic routing is proposed in[8] however sleep scheduling which actually require to minimize the consumption of energy and delay is not focused.

For identifying and selecting the probable forwarders and incorporate the priority-based timers simple opportunistic adaptive routing protocol (SOAR)[9] is proposed. This method effectively handle multiple flow alongside realizes greater efficiency. Due to lack of reliability support by MAC layer during broadcast, broadcasted nodes easily become target and results in loss of packet and its manipulation. Also default path selection is out of the scope of this method which actually required to improve the performance of scheme.

The scheme proposed in [10] is based on active-trust which realized efficient energy usage, scalable performance, higher success rate in routing probability sufficient security provision and high data rate among the nodes. But this incurs unwanted consumption of energy which reduces the performance of the method and may lead to the failure. Lifetime of network is drastically degraded because of the consumption of great amount of energy due to acquisition of trust and its release may consume significant amount of energy due to which malicious node detection become harder.

Wang et.al.[11] proposed Ant colony optimization algorithm for secured routing (ACOSR) scheme in which packet loss is significantly reduced and provided secure routing. Along with that effective balancing of energy consumed by nodes also the overall energy usage by network is significantly reduced which improves the lifetime of network. But estimation is required by this scheme in the presence of attacks which are in its intricate state.

Power efficiency and utilization optimization scheme proposed in[21] realized triple network lifetime. Better usage of energy is demonstrated by this method which is irrespective of the network size. However greater overheads due to complex computation and communication are the flaws of this method.

A model based on trust for peer-to-peer network using ant colony optimization is proposed in[24], where the legitimate server is efficiently selected. Basic criteria to measure the trust level of neighbouring nodes by the source node is the essence left by ants. However replay of routing and network information caused due to identity theft is out of the scope of this method.

Another self-recommendation scheme is proposed in[25] which evaluates trust among the nodes of the network. Maintaining the energy level and based on that calculation of level of trust is the key point of this scheme. Attacks stealing identity and falsely replying routing information will affect network and routing badly, may result in failure to recognize and choose optimum route for communication.

Karthik et.al.[26] proposed HTMS, that operates on two parameters strength of node and originality of data. Depending on node linking metrics and data source, ratings are assigned to originated data. Based on these ratings further routing related decisions are taken. There are greater chances of easy manipulation of basic details by attacker which is big challenge in realization of reliability of data during communication in the network.

Moreover the scheme for identifying and avoiding packet drop attack is proposed by Vishwas et.al.[27] for wireless ad-hoc network in which trust is maintained in list that indicates the number of time participation of node in routing. With the help of trust and energy values nodes are separated based on selfishness and un-selfishness. Usually WSNs are highly resource constrained so this method is not suitable due to unavoidable computational overheads.

Main emphasis of the work is to propose and evaluate an Associative secure optimized routing scheme in WSN. Scheme based on the association of opportunity and security is implemented in realization of novel architecture such that along with the participation of nodes in routing process but security is also guaranteed.

Proposed work is divided in two phases: phase I is intended to identify and select legitimate nodes which further guarantee secure group communication in the network. Secure routing is carried out in phase II of work depending on opportunity and trust in realization of fine solution.

III. DESIGN OF ASSOCIATIVE SECURE OPTIMIZED ROUTING FRAMEWORK

Routing techniques for WSNs are designed to discover the best suited and optimized routes. Trust and energy are two factors based on which effectiveness of routing scheme for WSN can be decided. There are greater computation complexities incurred in existing routing schemes. To reduce this unintended computational overhead alongside treating complex threats, a technique is proposed. Therefore to experience security alongwith optimization, an Associative Secure Optimized Routing (ASOR) is proposed. Associative name given to proposed method because in our previous work[15] nodes were rigid and routing was strictly carried out through identified route only.

However in the real time scenario the location of nodes are not rigid to single location, they may be mounted on objects and with the movement of objects nodes will also move. So existing schemes are not the correct alternative always. It is also expected that the scheme should produce more than one possibilities for routing for the source. Taking into account all these aspects proposed associative secure optimized routing scheme operates in two stages. In the first stage associative nodes among all the initiated nodes are identified and selected. Also in this stage the method commits greater degree of defence against worm hole attack and black hole attack, by ensuring that the scheme possess trusted and adaptive structure. Associative nodes are selected through the defined indulgent constant(IC) based on explicit trust, strength of link and link_quality parameters. Sub section 3.1 describe these parameters. WSN is simulated with N nodes initially and based on IC associative nodes are selected to be handed over to the second stage of the proposed scheme. Second stage focuses on making packets greedy, also optimizing the utilization of critical network resources such as memory, effective end-to-end communication. Through ASOR optimum routing is then performed and identification and selection of route carried out based on Aptness Function (AF) consists of four parameters trust_level, strength_of_link(SOL), link_quality(LQ) and distance. In this way optimum routing by ensuring explicit trust is performed in WSN. Block schematic of the proposed routing technique is shown in fig 1.

A. Associative Nodes Identification

Associative nodes are identified to realize security in the network using defined Indulgent Constant(IC). Based on explicit_trust(ET), strength_of_link(SL) and link_quality(LQ) parameters, IC is computed. The indulgent constant IC is computed as,

$$IC = \left[ET_i + SL_i + LQ_i\right]/3 \qquad (1)$$

here, ET_i referred as explicit trust of i^{th} node, SL_i shows the strength of link of i. M associative nodes are recognized and chosen from initialized N nodes such that $(M < N)$. The node indicating higher trust, strength of link and quality is elected as associative node, while other nodes are just rejected from involvement in routing process. Quality of link parameter LQ_i is purely depending on the greater survival time of link(STL) and lower delay experienced by nodes of network

a. Explicit Trust (ET)

Explicit trust also mentioned as local trust[22] depend on the degree_of_approval at the time of communication among nodes. ET_i between nodes i and j depending upon degree_of_approval d_app_{ij} between them. When node j is contented with node, d_app_{ij} is higher and denoting local trust. Based on successful communication SC_{ij} between nodes j and i and total nodes present in the network, d_app_{ij} is computed as:

$$d\_app_{ij} = \frac{SC_{ij}}{N} \qquad (2)$$

Where successful communication carried between nodes i and j is expressed as, SC_{ij} and N indicates total nodes.

b. Strength of Link (SL)

Strength of the link expresses the connections exist among the nodes and connect bi-directional links connecting nodes. The Strength of Link (SL_j) of the nodes is computed as,

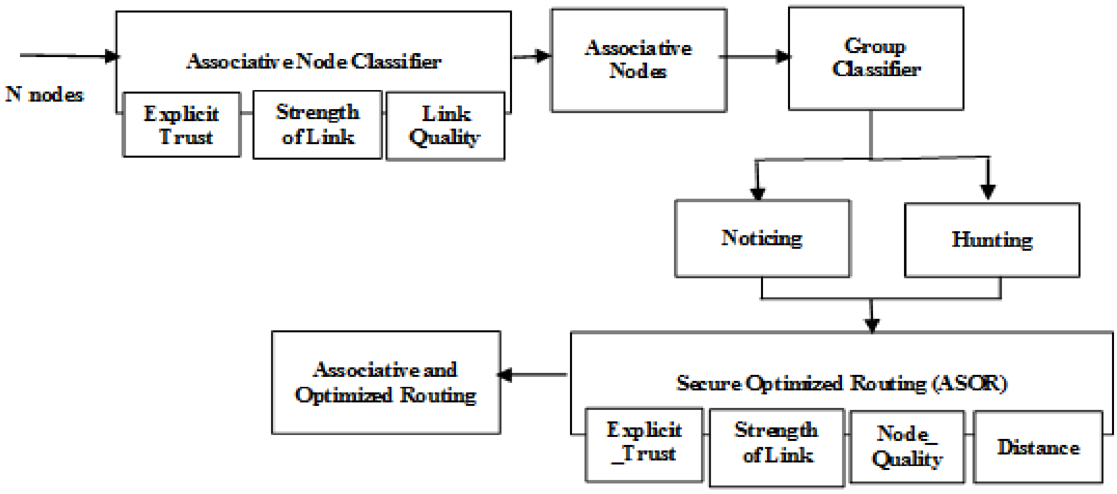


Figure 1: Associative Optimal Routing Scheme Architecture

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

where SL_i expresses strength of link of i^{th} node, and c is total number of connections.

c. Link_Quality(LQ)

Quality is computed based on the existence time of link(ETL) and caused delay. ETL and network's existence duration are associated. ETL of nodes of network depends directly on the live connections present between nodes[23]. Strong link while transfer of data is evaluated and is taken in that transfer process to initialize the connection and realize lossless data transfer. Due to unavoidable issue of link failure as nodes are assumed to be dynamic in nature, it becomes essential to computation of ETL. So it raises the need to avoid these link losses to efficiently decide the communication path. To compute ETL the basic parameters such as node's movement, its direction and coordinates of its location are considered. Here delay d_j of node j is evaluated as the ratio of live nodes to total nodes present in the network. So the link_quality through j^{th} node is stated as:

$$LQ_j = ETL_j + d_j \qquad (4)$$

Indulgent constant can be finally given as

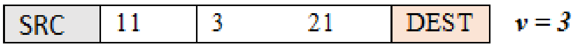
$$IC = \left[\frac{SC_{ij}}{N} + \frac{1}{N}\left[\sum_{i=1}^{N} \frac{SL_i}{c} \cdot\right] + (ETL_j + d_j)\right] / 3 \qquad (5)$$

B. Associative Secure Optimized routing (ASOR) Algorithm

Through indulgent constant(IC) the associative nodes are recognized and separated, which only participate in the routing process. Progression of routing depends on optimized and secure routing algorithm. Source, destination and associative nodes are initialized such that optimized routing path is generated. After the decision on source and sink nodes, there are v number of associative nodes are obtained depending on secure optimized routing algorithm ASOR based on Apt Function (AF).

a. Vector Frame/ Encoding Vector

The vector frame is the representation of possible solution to be appraised by using ASOR algorithm. Configuration of vector frame is intermediate nodes intricate in routing process, number of associative intermediate nodes are denoted by v, where v varies from 1 to M and M is the number of associative nodes in the initiated session. Fig 2 show vector frame having 3 associative nodes,



SRC	11	3	21	DEST

$v = 3$

Figure 2. Vector Frame

So nodes 11, 3 and 21 are the associative nodes and data transmission carried out through these nodes to approach destination when $v = 3$. Identification and selection of optimum associative nodes is carried out using ASOR based on Apt Function. Between source and destination the encoding vector is operating with unique formats followed by paths generated for routing.

b. Aptness Function (AF)

Aptness measure confirms the selection of optimum associative nodes for performing associative routing in WSN with aptness should have max value. To obtain the solution for the maximization problem aptness calculation needs to be effective. Apt function is defined based on four parameters explicit trust, strength of link, node's quality and distance between these adjacent associative nodes. So the Aptness is framed as,

$$AF = \frac{1}{4}\left[\sum_{i=1}^{v} ET_j + SL_j + NQ_j + \left(1 - D_{i,i+1}\right)\right] \quad (6)$$

Where $D_{i,i+1}$ denotes the distance among adjacent associative nodes i and $i+1$. To realize maximum solution of aptness it is essential for the mechanism to have maximum values of Explicit_Trust(ET), Strength_of_Link(SL) and Node's Quality(NQ) but at the same time Distance(D) should be minimum. The parameter distance in AF construction, should be minimum, due to this it is declared in function by subtracting it from 1.

c.ASOR Algorithm

Main highlight of the proposed Associative Secure Optimized Routing Algorithm is to obtain significant optimized results with less complexities in computation. In most of the real time applications of WSN the nodes are dynamic in nature and also these networks are constrained for the utilization of resources, ASOR efficiently handle this. Associative nodes are arranged in two segments, first is noticing and other is hunting with respect to the realization of optimization of the utilization of resources of network effectively.

This separation indicates the nature of cats, as they rest most of the time noticing their pray and in case of favourable opportunity they immediately react to the situation to hunt it and get success most of the time. Capability of energy restoration is noticeable characteristic of them because they usually require less for hunt and get success. In technical terms the exploration and operation sections of ASOR abbreviate optimal result with greater join rates. In simple terms the associative nodes are categorized into two parts. First part holding the nodes which are in noticing segment whereas the other segment is hunting. In hunting part the associative nodes reach the intended next hop or destination or sink node in less time, so the population of nodes in this part is lesser as compare to other section. Latest location and aptness are calculated to get the modified solution and saved. To reach to the best optimal solution these steps are repeated and iterated.

Following rule fix the updated location of the associative nodes when they are in hunting segment in ASOR:

$$UL_{i,q}^{t+1} = \frac{1}{\left[R_1 * \mu_1\right]}\left\{\left[-\phi \times \left(S_q - 0.5\right)\right]\left[1 - R_1 * \mu_1\right] + v_{i,q}^{t} + R_1 * \mu_1 * CL_q^{*}\right\} \quad (7)$$

where, $UL_{i,q}^{t+1}$ is the updated location of the associative node at time $(t+1)$, $CL_{i,q}^{t}$ specifies the current location of the associative node. $UL_{i,q}^{t+1}$ and $CL_{i,q}^{t}$ are the locations at times $(t+1)$ and t, $v_{i,q}^{t+1}$ is termed as the velocity of these nodes at time $(t+1)$, S_q is the joining speed of the nodes and R_1, ϕ are random numbers having values only between 0 and 1. i^{th} node's velocity in q^{th} dimension, is expressed as,

$$v_{i,q}^{t+1} = v_{i,q}^{t} + R_1 * \mu_1\left(UL_q^{*} - UL_{i,q}^{t}\right) \quad (8)$$

where μ_1 is a constant. In respect to realize optimized solution, at the start total_nodes (N_{iq}) are initiated, expressed as,

$$N_{iq};\left(1 \le i \le AN\right) \quad (9)$$

where, AN refers to the total associative nodes and q is the dimensional search area.

Location and velocity of migrating associative nodes are randomly described to start the optimization then these nodes are arranged in notice and hunting segments accordingly. In the first phase random initialization of location and velocity each node is done, then arrangement of these initialized nodes in noticing and hunting groups accordingly is done.

Exchanging between these groups is depending on Node-Position-Parameter(NPP) having boolean value 1 for noticing group and 0 for hunting. For various instances of nodes NPP is defined and for instances t it is randomly generated. Traversal is performed by the associative nodes based on the present condition or they will be idle but attentive in noticing group. This analogy is same as the behaviour of the cats as when it is observing or noticing its pray it remain idle for few moment of time and then perform traversal slowly depending on the situation. Initially the formation of copies of i^{th} is done and is trained to analyse their Possession Memory Buffer(PMB). The process of copying is continued for acquiring the latest copies of nodes, their updated locations are modified based on its current location, its chosen dimensional area(CD) along with a random number.

The updated location of node is represented as $UL_{i,q}^{t+1}$ and is formulated as,

$$UL_{i,q}^{t+1} = \left(1 \pm CD \times \beta\right) \times CL_{i,q}^{t} \quad (10)$$

The aptness is evaluated and assured to 1, which is related with the location of associative node, is indicating discrete solution. However, if it is not 1 then probability of evaluating discrete solution is given as,

$$P_i = \frac{|AF_i - AF_{\omega}|}{|AF_{max} - AF_{min}|} \quad (11)$$

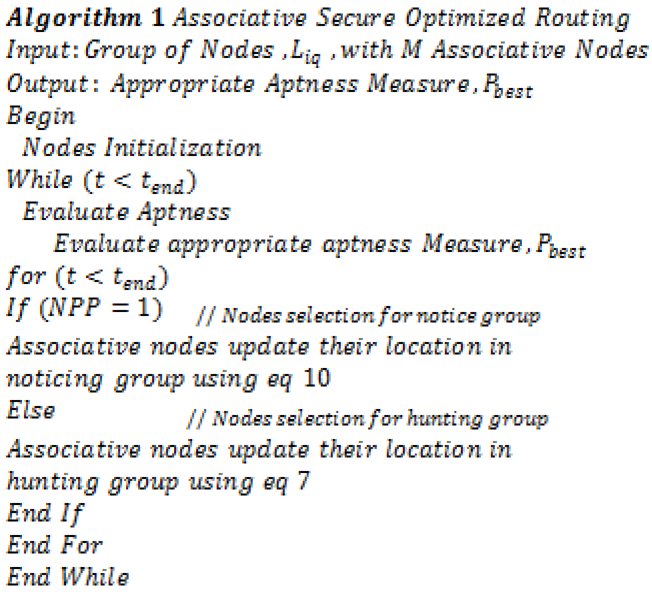
here, P_i is the probability of i^{th} associative node, AF_i is the apt function of i^{th} node, AF_{max} is the maximum value of AF, and AF_{min} is the minimum value of AF. AF_{ω} indicates aptness's max value in case of minimization problem and minimum value in case of maximization problem. Additionally, decision on placing nodes in groups is made based on the NPP parameter value.

For NPP having value not as 1, associative node is initialized in hunting mode to search for the finest forwarder. Once the identification is successful, through proposed ASOR, associative node's location and velocity are updated.

Furthermore, most appropriate aptness measure P_{best} for the latest solution is done once the location of associative nodes are fixed, either in noticing or hunting group. For realizing best optimal and efficient solution the aptness function should possess maximum value, which indicates that the optimal associative nodes only take part in the routing process.

Finally, verification of the end of routing process is done through the defined ending criteria. This ending criteria is defined to realize the better effect of imposed algorithm and consists of extensive iterations, improvement percentage and execution time.

Persistence of routing process through associative nodes is experienced through the proposed associative secure optimized routing(ASOR). The steps of ASOR algorithm are given below:



```
Algorithm 1 Associative Secure Optimized Routing
Input: Group of Nodes ,$L_{iq}$ ,with M Associative Nodes
Output: Appropriate Aptness Measure, $P_{best}$
Begin
  Nodes Initialization
While ($t < t_{end}$)
  Evaluate Aptness
      Evaluate appropriate aptness Measure, $P_{best}$
for ($t < t_{end}$)
If ($NPP = 1$)     // Nodes selection for notice group
Associative nodes update their location in
noticing group using eq 10
Else               // Nodes selection for hunting group
Associative nodes update their location in
hunting group using eq 7
End If
End For
End While
```

IV. RESULTS AND DISCUSSION

Experimental observations and efficacy of ASOR is given in this section along with the comparison with near competing schemes. Proposed ASOR is simulated in NS2 and the evaluation of performance is based on metrics distance, delay, detection_rate and throughput. Along with the comparative analysis, network analysis is performed in presence of worm hole and black hole attacks. 100 nodes WSN simulation setup is shown in fig 3 where source, sink and adversary are indicated. Communication and message passing carried out in this network through associative nodes.

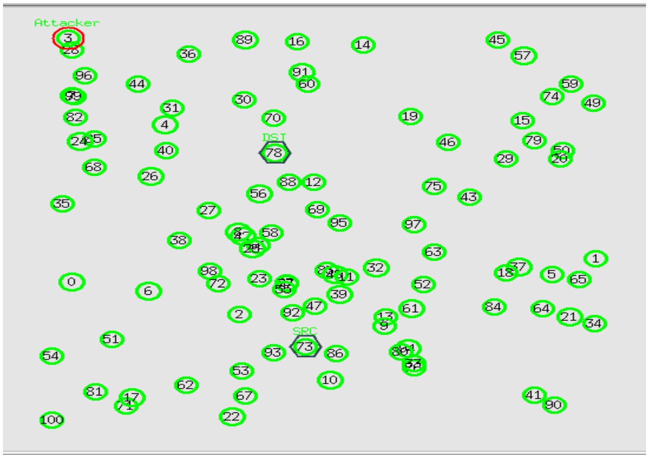


Figure 3. 100 nodes Simulation Setup

A. Performance Metrics

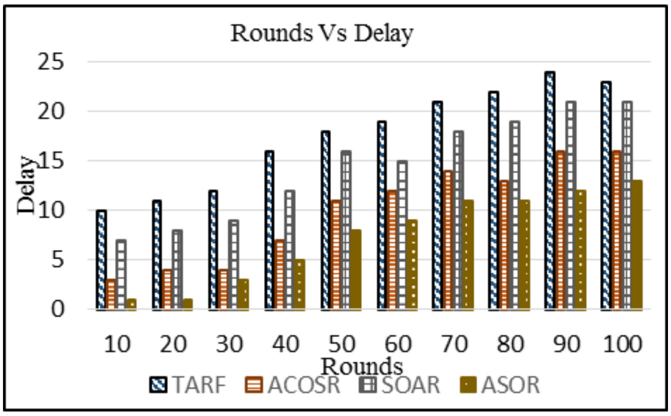
Performance of the proposed scheme is evaluated based on the parameters distance, delay, detection_rate and throughput. Throughput is measured as the rate of data under a specific timeslot in the network. Time consumption at the time of data transfer with or without attack in the network is the measured delay. Here detection_rate is termed as the accuracy in detection of attack. Performance of the efficient scheme is with greater detection_rate higher energy and throughput but with lower delay. Also the distance among associative nodes should be less for the realization of improved performance of the scheme. Performance effectiveness of the proposed scheme ASOR is analysed in the presence of attacks worm hole and black hole.

B. *Performance Comparison*

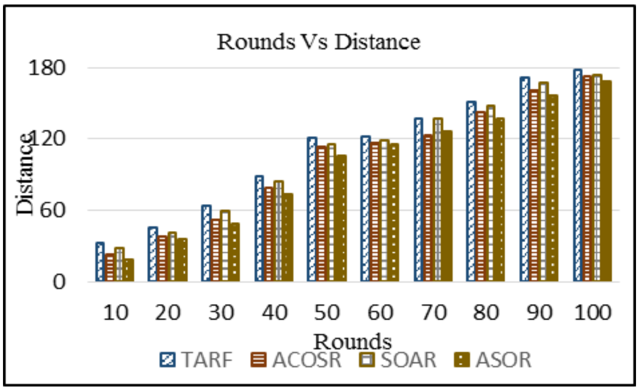
Proposed scheme ASOR's performance is examined for the network with impacted by two attacks. The examination is carried out based on the metrics as mentioned earlier. Then performance comparison is done of proposed ASOR with Trust Aware Routing Framework (TARF) [2], Simple Opportunistic Adaptive Routing protocol (SOAR) [9], and Ant colony Optimization for secured routing protocol (ACOSR) [11]. Comparative analysis show the noteworthy improvement in performance against these competing methods. Network with 100 dynamic nodes proceeding towards the analysis phase is established in NS2.

In presence of wormhole attack: On the basis of above mentioned measures of evaluation of performance in presence of wormhole attack is represented in fig 4. Analysis based on delay is shown in fig 4(a) and for effectiveness of the scheme this measure should be minimum. Methods TARF, ACOSR, SOAR and ASOR indicate delay at the end of 100 rounds as 23, 16, 21 and 13sec. For the effectiveness of routing scheme distance measure should be minimum which is indicated in fig 4(b) where the distance reflected by the methods TARF, ACOSR, SOAR and ASOR are 178.2, 172, 173.7 and 168.2 respectively. Similarly for high performance and accuracy the detection_rate parameter should have significantly high value and after all the prescribed rounds the detection rate of TARF, ACOSR, SOAR and ASOR are 50.1, 53.2, 51.9 and 55.6 accordingly which is represented in detail in fig 4(c).

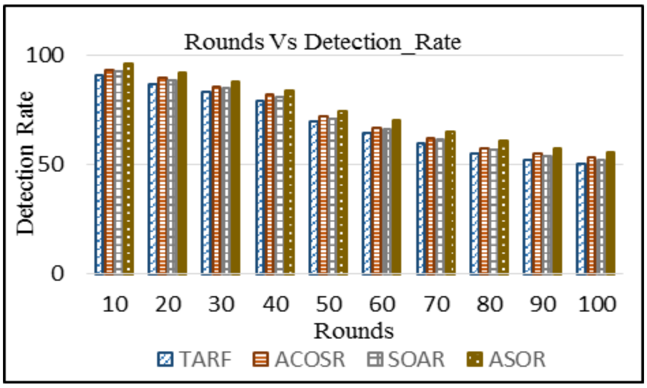
Nevertheless the effective performance of scheme also depend on the throughput which must be high. Throughput after all 100 rounds of the methods TARF, ACOSR, SOAR and ASOR are 39.6, 40.7, 40.7 and 44.1 respectively. Based on the results obtained on various phases of working of proposed routing mechanism, ASOR shows comparatively less delay and distance however at the same time it shows high detection_rate and throughput.



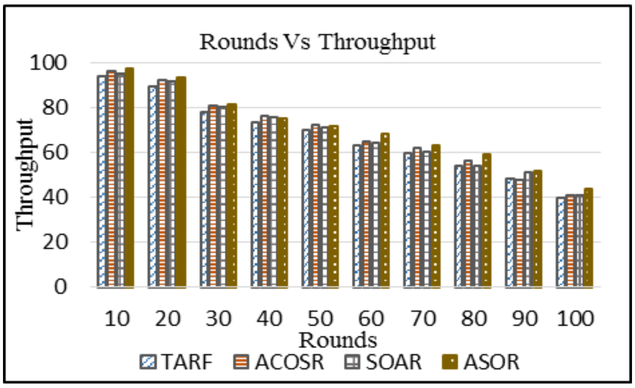
(a)



(b)



(c)



(d)

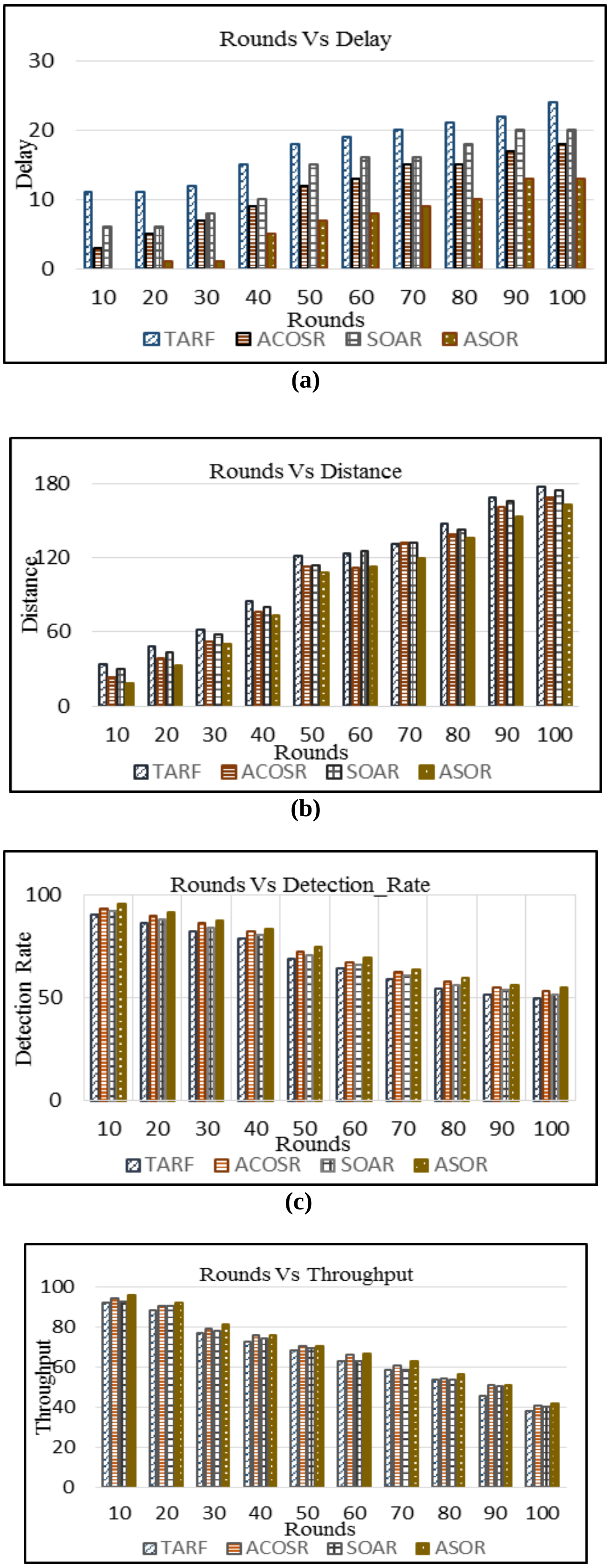
Figure 4: ASOR performance with Worm Hole attack.

Moreover, table 1 presents more comprehensive results, which indicates comparatively higher performance of proposed ASOR over competing methods in all 100 rounds in presence of wormhole attack with respect to the considered performance metrics.

Performance metrics																
1: Delay				2: Distance			3: Detection_rate					4: Throughput				
Rounds	TARF				ACOSR				SOAR				ASOR			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
10	10	33	91.1	94.1	3	22.7	94.4	96.4	7	28.3	92.8	95.1	**1**	**19**	**96.4**	**97.3**
20	11	46.1	87	89.4	4	38.2	90.3	92.2	8	41.9	88.8	91.7	**1**	**36**	**92.4**	**93.5**
30	12	63.9	83.2	77.8	4	51.7	86.2	80.5	9	59.7	85	80.1	**3**	**49**	**88**	**81.3**
40	16	88.3	79.4	73.3	7	79.5	82.8	76.3	12	84.3	81.1	75.4	**5**	**74**	**84.1**	**75.4**
50	18	122	69.6	69.7	11	113	73.2	71.9	16	116	71.2	71.1	**8**	**106**	**74.2**	**71.8**
60	19	122	64.7	63	12	117	67.8	64.6	15	119	66.4	64.2	**9**	**116**	**70.2**	**68.1**
70	21	137	60	59.8	14	123	63.6	61.8	18	137	61.8	60.2	**11**	**126**	**64.8**	**63**
80	22	152	55.1	54.1	13	142	58.9	56.1	19	148	56.6	53.9	**11**	**137**	**60.7**	**59.4**
90	24	171	52.1	48.1	16	160	55.4	47.9	21	167	53.8	51	**12**	**156**	**57.2**	**51.6**
100	23	178	50.1	39.7	16	172	53.4	40.8	21	174	52	40.8	**13**	**168**	**55.6**	**44.1**

Table 1: Results in presence of wormhole attack

In presence of Black Hole attack: Based on the above mentioned measures of evaluation of performance in presence of black hole attack is represented in fig 5. Analysis based on delay is shown in fig 5(a) and for effectiveness of the scheme this measure should be minimum. Methods TARF, ACOSR, SOAR and ASOR indicate delay at the end of 100 rounds as 24, 18, 20 and 13sec. For the effectiveness of routing scheme distance measure should be minimum which is indicated in fig 5(b) where the distance reflected by the methods TARF, ACOSR, SOAR and ASOR are 177.3, 168.6, 174.3 and 162.5 respectively. Similarly for high performance and accuracy the detection_rate parameter should have significantly high value and after all the prescribed rounds the detection rate of TARF, ACOSR, SOAR and ASOR are 49.7, 53.2, 51.3 and 54.9 accordingly which is represented in detail in fig 5(c). Nevertheless the effective performance of scheme also depend on the throughput which must be high. Throughput after all 100 rounds of the methods TARF, ACOSR, SOAR and ASOR are 37.6, 40.5, 40.1 and 41.6 respectively, fig 5(d). Based on the results obtained on various phases of working of proposed routing mechanism, ASOR shows comparatively less delay and distance however at the same time it shows comparatively high detection_rate and throughput.



(a)

(b)

(c)

(d)

Figure 5: ASOR performance with Blackhole Attack.

Additionally, more comprehensive results are presented in table 2 which is indicating higher performance of our proposed method ASOR as compare to the competing methods in all 100 rounds in presence of blackhole attack with respect to the considered measures of performance.

Performance metrics																
1: Delay			2: Distance				3: Detection Rate					4: Throughput				
Rounds	TARF				ACOSR				SOAR				ASOR			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
10	11	33.6	90	92.1	3	23.2	93.3	94.4	6	29.7	91.9	92.8	**0**	**17.96**	**95.6**	**95.6**
20	11	48.1	86.1	88.1	5	38.3	89.5	90.4	6	43.7	87.8	90.1	**1**	**33.28**	**91.3**	**92.1**
30	12	61.7	82.4	76.8	7	51.8	86	79	8	57.8	84	77.7	**1**	**49.82**	**87.5**	**81.2**
40	15	85.2	78.5	72.6	9	76.5	81.9	75.5	10	80.2	80.4	74	**5**	**72.97**	**83**	**75.8**
50	18	121	68.8	68.4	12	113	72.3	70.2	15	114	70.5	69.5	**7**	**107.7**	**74.4**	**70.2**
60	19	123	64	62.9	13	112	67.1	66.1	16	125	65.8	63	**8**	**112.8**	**69.5**	**66.5**
70	20	131	59.2	58.5	15	132	62.2	60.6	16	132	60.9	58.5	**9**	**119.2**	**63.9**	**62.7**
80	21	147	54.5	53.4	15	139	57.5	54.3	18	143	56	53.4	**10**	**136**	**59.3**	**56.3**
90	22	168	51.6	45.4	17	160	55.1	50.7	20	166	53.5	50.6	**13**	**153.4**	**56.2**	**50.8**
100	24	177	49.7	37.7	18	169	53.2	40.6	20	174	51.3	40.1	**13**	**162.6**	**54.9**	**41.6**

Table 2: Results in presence of blackhole attack

Furthermore, the average performance over performance metrics, of ASOR in presence of wormhole and blackhole attacks, in all 100 rounds is also higher as compare to the competing methods. Table 3 collectively presents the average performance of competing methods and ASOR with respect to the performance measures. This gives a clear view on the scalability in performance of proposed scheme.

Performance Metrics	Wormhole				Blackhole			
	TARF	ACOSR	SOAR	ASOR	TARF	ACOSR	SOAR	ASOR
Delay	17.6	10	15	**7.4**	17	11	14	**6.7**
Distance	111.24	102	107.5	**98.67**	109.7	101.41	106.5	**96.5**
Detection_Rate	69.2	72.5	70.9	**74.36**	68.48	71.805	70.2	**73.56**
Throughput	66.91	68.8	68.35	**70.54**	65.59	68.177	66.96	**69.27**

Table 3: Average results of methods.

V. CONCLUSION

Associative and secure routing is performed in WSN with opportunities and optimization, which is carried out in two stages, identification and selection of associative nodes and optimization. Indulgent Constant(IC) is formulated in the first stage, which classifies the associative nodes out of initialized nodes. Functioning of IC is through explicit_trust, strength_of_link, and node quality parameters. Only these classified associative nodes are permitted to take part in the routing process whereas other nodes are not allowed. Associative Secure Optimized Routing(ASOR) is proposed as a part of realizing optimization, in the second stage. Functioning of ASOR is based on the defined Aptness Function(AF) which is formulated using explicit_trust, strength_of_link, link_quality and distance parameters. Identified associative nodes are placed in two groups initially, i.e. noticing and hunting. Then the network is assisted by given vector frame to choose the appropriate associative nodes for the communication between source and sink. Implementation of ASOR is done using simulation with 100 dynamic nodes WSN in NS-2 platform. Evaluation of performance and analysis is done through the performance metrics delay, distance, detection_rate and throughput with worm hole and black hole attacks. Simulation results reveal the effectiveness of the proposed method as compared to the existing schemes considered in evaluation phase. Minimum delay and distance of 13 and 165.4 respectively, are realized through ASOR however the scheme indicates higher detection_rate and throughput of 55.3 and 42.9 respectively.

During the design of strong routing scheme, reduction of computation overhead is always be the challenge. Depending on the precise application requirements, this scheme can be further extended to reduce this complexity and design more robust and optimized routing scheme.

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 at JSPM’s Imperial College of Engineering and Research, Wagholi, Pune, 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 has 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).

Pradeep B. Mane, received his B.E. (E&Tc) and M.E. (E&Tc) degree from Government College of Engineering Pune, India and Ph.D. from Bharati Vidyapith University. He worked in Philips India ltd. for 3 years, 15 years in Bharati Vidyapeeth University COE Pune and currently working as a principal in AISSMSs Institute of Information Technology, Pune. He was a member of the BOS for Electronics faculty in Bharati Vidyapeeth University. He has co-authored five books for engineering courses with Technova publications pune in the subjects of Radio and TV engineering and computer networks. He has published 40 papers in National, International Conferences and seminars. He has more than 45 National and International Journal publications. He is a regular reviewer for Springer Wireless Personal Communications journal. His area of interest is Wireless Communication and Networking. He is a fellow of IETE and ISTE.