Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/130603

Improvements in Cluster-Based Routing to Protect Malicious Node Attacks on TAODV Routing Protocol using MANET

N. Satheesh[1,*] *and K. Prasadh*[2]

[1] Department of CSE, St. Martin's Engineering College, Secundrabad, India.
[2] Vijnan Institute of Engineering & Technology, Ernakulum, Kerala, India.

Received: 3 Apr. 2019, Revised: 2 May 2019, Accepted: 11 May 2019
Published online: 1 Nov. 2019

Abstract: In MANET resources are trivial with a controlled environment with extreme mobility and do not have any centralized directorial control. Self-motivated topological variations occur because of the excellent mobility of the nodes for creating experiments in routing and constructing protected message passing. Here, the impact of WormHole (WH) Attack analyzed is by the Ad hoc On-Demand Distance Vector Routing Protocol (AO-DDRP) in the existence of WAs. Cluster formation is the mechanism for grouping wireless nodes in the form of clusters under CH for easy management of the network. The Hash Function (HF) proposed when there is a tie between nodes based on calculated weight for the selection of CH enhances the existing algorithms and minimizes the chance of any weak node to become CH. It prevents malicious behavior and the uniform utilization of network resources. The self-explanatory intercommunication grounded among the agents, and Sophisticated Diffusion Search (SDS) is a multi-agent collective exploration and optimization procedure consisting of a robust mathematical structure to define the behavior of the algorithm with its advantages, such as resource distribution, meeting the universal best, strength and minimal meeting benchmarks as well as exact time involvedness. The limits, such as throughput, end-to-end delay and the sum of stored responses, were recycled to estimate the recital. Results proved that the throughput and the number of stored responses improved; reaching to 50% in the incidence of malicious nodes and the end-to-end delay was arbitrarily enhanced.

Keywords: MANET, Cluster Head, Attacks, Malicious Node

1 Introduction

The independent system of mobile nodes and hosts connected through wireless links is called MANET. Also, it is ad hoc network termed as a group of wireless nodes which can give or receive packets for each other to allow a node to communicate beyond its direct wireless transmission range. As ad hoc networks do not need a fixed infrastructure, base station or access points it can build quickly in an inexpensive setup. Nodes within each other's range of transmission can communicate directly in MANETs. When a node is situated outside the scope of communication and requires sending a message to another node, it has to trust other specific new nodes to transmit the messages [1]. The term Mobility used for denoting actions of hosts remaining in a different domain on the internet which has their IP address without the necessity to change it regularly and its mobile IP technology. These networks have no fixed access points; each node could be either a router or a host. All nodes can and are dynamically connected in an arbitrary manner. These networks can configure by themselves autonomous systems consisting of hosts and routers. There is a restriction of power consumption, bandwidth, and computational power. The security mechanism of MANETs is different from that of conventional networks because is no central administration or prior organization. Because of wireless links, they are more susceptible to attacks. Intruders can easily hack this network and gain entry to confidential information. The system can also be directly attacked to delete messages or add malicious messages/masquerade as a node. The primary network goals of integrity, availability, confidentiality, authorization, and authenticity are violated [2].

* Corresponding author e-mail: nsatheesh1983@gmail.com

In MANETs, routing is the most active area of research, and various protocols have introduced to address the issues of path [3]. There is no fixed infrastructure for MANETs and for the adequately functioning of the MANETs, so the protocol should function appropriately on a frequently changing network topology. The method of exchanging information from one host to another is called routing. The process of forwarding packet from its destination with the use of the most efficient track is routing. Various metrics are used to measure the efficiency of the path including the number of hops, traffic, and security, etc. Every node acts as a specialized router in ad hoc network itself [4]. Securing MANET is challenging due to its limited computational capacity, memory, and bandwidth. Challenges in MANET security include detection and mitigation. WH attacks are one of the most common attacks in MANET and securing the network is challenging. Recent research has shown that the efficacy of Trust-based systems for networking when integrated with routing the QoS is affected. This work proposed methods for the detection and mitigation of WH attacks as well as a confidential mechanism to improve QoS. It proposed novel optimization algorithm to solve the issues of managing multiple QoS and Non-deterministic parameters.

The author focused on the insiders' attacks fundamental attributes of one/more specific attacks survey without performance analysis [5]. The authors had briefly analyzed the attacks over MANETs of the black hole attack, sinkhole attack, selfish node behavior, RREQ flood, *hello* flood, and selective forwarding attack. NS-2 simulator launching execution of such attacks performed by AODVRP provided a comparative investigation of such attacks. They had employed packet efficacy, routing overhead, and output as per expected techniques performance measures. The author's investigation had proved that overflowing attacks, namely RREQ flood and *hello* flood, significantly improved the protocol direction-finding overhead. Route alteration attacks, such as a sinkhole and black hole, were lethal, severely affected the packet effectiveness, and reduced the throughput to unsatisfactory levels.

The authors' risk-aware concept is based on improved Dempster–Shafer measured evidence hypothesis with significant features. Also, the experiments illustrated these concepts efficiently with different performance measures. To identify and preserve exceptional attacks like snooze Denial, Black Hole, Grey Hole, and Rushing/Sybil attacks [7], they had presented a comprehensive intrusion finding and prevention system. In addition, they employed anomaly and knowledge-based intrusion detection to secure MANETs from different attacks. They could identify unpredicted attacks. Prototypical results revealed that the authors' paradigm is used to separate the intruders causing attacks with a low-priced network overhead.

WA affects MANET with Preemptive routing protocol and Non-Preemptive routing protocol [8]. The objective was to identify the vulnerable protocol to the WA. The value of OPNET model shows the throughput, end-to-end interval, network load, and traffic attained using WH and without WH on routing protocol called AODV and OLSR. Hence, the MANET application using proactive routing protocol was more material possessed over the reactive one. They attempted to solve a designing problem in a Dynamic Source Routing (DSR) centered routing method as the Cooperative Bait Detection Scheme (CBDS), to incorporate benefits of proactive and reactive defense structural designs [9]. The authors' CBDS technique had been implemented as an inverse locating method to assist in obtaining the province objective. Simulation consequences were presented to show malicious-node attacks presence; the CBDS outperformed the DSR, 2ACK and optimal-effort fault-tolerant routing protocols based on Packet Delivery Ratio (PDR) as well as routing overhead.

On enhancing the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to preserve over flooding and blackhole attacks [10]. The results were performed and experimented with GloMoSim V.2.03. The performance investigation had proved development in PDR on blackhole attack, along with the insignificant upswing in average end-to-end delay and stabilized routing overhead. This scheme for flooding attack worked for the unknown malicious node identification and did not employ additional network bandwidth. It was easy to perform and keep or enhance network throughput which did not encompass any malicious nodes; however, there was a more congested traffic network. The study addressed the effect of network dimension proposed Trust Based Secure on Demand Routing Protocol called "TSDRP" and AODVRP to impede Blackhole attack [11]. To assess the metrics recitals, it had concerned Packet Delivery Fraction (PDF), Average End-to-End Delay (AED), Average Throughput (AT) and Normalized Routing Load (NRL).

The literature indicated different attacks on multiple layers in the protocol stack. This technique had been discussed on routing and security problems related to MANETs to offer secure communication. Based on attack interaction over MANET, they had been categorized as active and passive attacks. Attackers on the network were categorized into two groups: insider and outsider. The researcher offered and executed current IDS of Enhanced Adaptive ACKnowledgment (EAACK) mainly intended for MANETs [12]. The comparison of the modern concepts EAACK had demonstrated higher malicious-behavior-detection rates in particular situations without a huge impact on network performances. The author had employed Digital Signature. Cluster-Based Secure Routing Protocol (CBSRP) assures secure communication as energy effective to segment the entire network as small cluster sets [13].

The study presented comprehensive literature MANETs security threats. The author described every routing threat to target routing protocol operation to either

self-centered actions or malicious attacks, and countermeasures on these attacks [14]. To investigate the active countermeasures in a structured way, the results had proved based on cryptography IDSs; and, trust management, and reputation-based solutions. Denial-of-Service (DoS) attacks were reviewed on the network layer of WH attack, Blackhole attack and Gray Hole attack of critical MANET's threats. The author created a few solutions to find and keep such attacks. The author had also selected a trust module to course routing measure value. Simulation outcomes proved that this proposed protocol reduced delay, routing overhead, and improved packet delivery ratio through devouring lower energy once contrasted over AODV and DSR the well-known existing routing protocols.

2 Impact of Worm-Hole Attack in MANET

In this impact, a small communication assortment is made for each MANET node by the wireless medium. The nodes directly transfer data within the communication range—multi-hop paths are used for communication among nodes with farther distance. The most important task of the MANET is to find the shortest route between two more distant nodes. Several routing protocols are used in MANET. They improve the reliability of the network. To improve the performance of the entire system, energy proficient, confident and QoS awake routing is desired [15]. Proactive, reactive and hybrid routing protocols are the major categories of the path. The path stands consequent from the new topology of the network to define the dynamic routing protocols. Each node maintains the possible routes of all its reachable nodes. They occasionally check and update the routing information in the table. The contents of the routing table are accessed whenever a new-fangled route has to be set-up. Hence, maintenance of the routing structure results in network overhead which increases the new directions found rapidly—finding the maps occurs at the beginning of the algorithm. Reactive protocols are on-demand algorithms. Thus, although this is a reliable method, it increases the network overhead. Hybrid protocols combine the techniques of proactive and reactive protocol methods. The data from the parent to end node are delivered in two possible ways, i.e., unicast routing and multicast routing.

In this existing method, data are sent to single destination from a single source. In the other method, information is delivered to multiple destinations that belong to the same group, from a single source. Two types of routings are possible: Mesh centered and tree-based routing. Tree-based routing has only a single route from the source node to the objective, but mesh-based routing comprises many paths to reach the destination. Anon reactive demand protocol is called the AODVR.

The neighboring nodes broadcast a packet called Route REQuest (RREQ). Forwarding occurs till the target is reached. All the transitional nodes record the routing structure at the time of forwarding. Later, the information is stored in the intermediate nodes a reply is sent by the destination node in reverse. For the maintenance of route in case of a source, the node moves again and RREQ packet is sent. Information on connection letdown is sent to the source node wherever the node goes.

2.1 Attacks in MANET

In a passive attack, the standard network operations disruptions are not done. Without touching the data exchanged in the network, the attacker snoops on it. Despite the breach of confidentiality. As the network operation is untouched, it is hard to detect these attacks. It is necessary to encrypt the data using a powerful encryption mechanism which makes obtaining useful information from the the exchanged data a challenge for the attacker. Traffic monitoring, snooping and traffic analysis are the listed passive attacks [16]. The types of network layer attacks are

WH Attack: The data obtained from a specific position by malicious nodes are sent to another location, and the packets are resent. The attacker creates the WH for the packets not addressed to them.

Black Hole Attack: The requests of routing are monitored by the malicious nodes in the network claiming them to be the intermediate nodes with short routes of destination. Thus, the false path is created when the response of the malicious nodes' reply extends the source. Subsequently, the nodes derive date from source nodes, and they may be dropped or altered based on the communication.

Byzantine Attack: For the performance of attacks, such as the selective dropping of data, forwarding the data to non-efficient paths and creating loops in the routes, an intermediate node gets compromised.

2.2 WH Attack

In the circumstance of a WH attack, two conniving nodes are involved in this attack. At a distance from one another, an illusion is created that the neighbor nodes get created by a new tunnel. RREQ message is delivered to the Colliding Nodes (CN) through the tunnel where one of these nodes receives the RREQ message resent from another node. The data passed through the WH tunnel and two CNs performing a multipoint relay. Once the interpretation is complete, the honest nodes participate in forwarding data, and the control messages prevented by incorrect information on the topology is forwarded. WH attacks have two types. Band/Out-of-Band WH attacks. In the former, a tunnel is created by using an existing wireless medium.

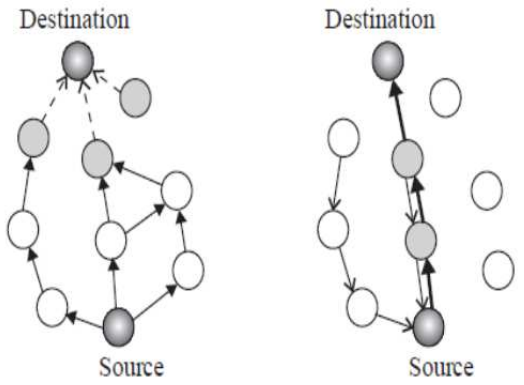


Fig. 1: RREQ broadcast and RREP propagation and subsequent route

Self-sufficient WH attack: The two planning nodes of the WH channel perform the attack.

Extended WH attack: This attack prolong above the planning nodes in a channel. Hardware is needed for connecting two of these nodes, and the band of WH attack may be exposed or hidden.

3 Proposed Methodologies for AODVRP

The impact of the WH attack is observed in MANET in this work. Reactive routing protocols that use Route Reply (RREP), Route Error (RERR) and Route Request (RREQ) as the control signals are AODV. The Source node broadcast RREQ packet is considered when trying to send a packet to the target node. The RREQ packets received by the neighboring nodes get forwarded to their neighbors. It takes place until RREQ reaches the destination. Intermediate nodes record all the tables of routing at the time of forwarding. Using information of the intermediate nodes helps the destination nodes send a response to the inverse route. If the node moves again, the RREQ packet is sent to maintain the paths. When a source node needs a destination node and doesn't have it in the routing table, the route discovery initiates. When the route is requested, a source floods a network with an RREQ packet for preliminary route discovery. Node authorizes the node to get if it is a route to the end of the endpoint itself, on the receipt of the RREQ package. If one of them is valid, an RREP packet is generated by the node which sends it back along the reverse route. An advancing cursor to the node is expected RREP from its set-up from every node on the inverse path. Thus, from source to destination, a forward route is ensured. A node resends the RREQ packet if it is not the destination and if it has no destination route [17]. At the intermediate nodes, duplicate RREQ packets are thrown out. A source node begins sending data to the destination when it first gets the RREP. RREQ broadcast and RREP propagation and the subsequent route are shown in Fig 1.

Route request RREQ is sent to the whole network for transmitting data packets. There may be three possible outcomes when RREQ is received at a node. First, in case the message receiving node affords a path to the destination requested in its routing structure, it replies with RREP. Second, if there is no destination information, the message is re-sent to the neighbors that have not received it. A Route Error message is sent if all the neighbors from the time-honored equal message/node have vanished link. Source node sends data packets on the shortest path [18–20] when receiving a reply message. Some parameters, such as strength, length, attraction, and robustness are used for identifying nodes that are involved in WH attacks. To evaluate the performance, the quantitative measures, such as the end-to-end delay; the actual cache reply number and the throughput are used. The bits are successfully transferred to the destination from the source distributed by the interval taken for diffusion and used for throughput computation. The mean time needed for the transmission of one single packet to the destination node from the source is the End to the delay time.

3.1 Proposed Message Packets for AODV

In the course of WH attacks, the channel is monitored by a hostile node, packets overheard in the precincts are recorded and sent to the tenuously placed conniving node which reiterates them in their flow. When routing control packets like *HELLO* messages and RREQ are targeted during tunneling, it may not be possible to find out legitimate routes in the nodes close to the attackers that start and end near the two attackers respectively. This authentic route time has more hops than one or two hops affirmed by WH attackers in a typical WH attack scenario. Accordingly, network operation is severely disrupted. For identifying and precluding WH attacks in AODV, the proposed method proposed here by research is *Hello_src* and *Src_reply*. This solution pinpoints the links that belong to the WH tunnels. Through an interchange of hash keyed probing packets between source and destination, it applies an appropriate WH detection mechanism to suspicious links.

HELLO messages are regularly sent by every node for discovering one-hop neighbors. The *HELLO* message source reports the neighbor on receiving the message. However, it is broadcast from more than one hop technique in a WH attack. It can give erroneous information to the core routing protocol, thereby causing failure in finding sufficient routes even if it does not compromise the nodes. If two nodes are in the transmission range of each other, they are regarded as neighbors. In this approach, the network links that have a high possibility of being involved in a WH attack are detected.

The extension of an existing *Hello* packet of AODV the *Hello_src* packet is introduced. As soon as a node is

assumed in a network, the clock interval of a node is harmonized. Harmonize phase is involved in a reticent bit in UNIX time set-up when transmission of the *Hello* text occurs during the discovery of a neighbor. Through joining *Hello* text with recent known time in UNIX layout and response, all the adjacent nodes in the receiving range of the *hello* messages receive a response. Once the reply is received, imprecise remoteness between two nodes is calculated as follows:

$$t_i = \frac{2d}{l}$$

where t_i = time taken for $\text{Hello}_{\text{src}}$ to reach destination and back, l = speed of light and d = distance between the two nodes.

When d is better than MAX broadcast of sender node, WH is suspected. A substitute route is open when a vicinity node is guarded. However, the proposed AODVRP implements a secure-reply packet approving the packet success destination if an alternate route is not located. *Src_reply*, a novel packet secure-reply is hosted. Message Digest (MD) can be more for the reply message to verify the message integrity. The algorithm HAVAL uses the principles behind the design of the MD family. It also uses Boolean functions.

The HF HAVAL is a simple rehearsal compression function and termed as $H_0 = IV$, $H_j = \text{compress}\left(H_{j-1}, M_j\right)\ (1 \leqslant j \leqslant t)$, $\text{hash}(M) = H_t$. M message is allocated into t blocks of the M_j of about 1024 bits each. The initial value of the 256 bits and H_j here denotes the binding variables that have 256 bits span. All compression function applies to the transform chaining that functions as a 256-bit hash value of the message M. The collision of two words takes place regarding a one-way hashing algorithm if they are densed to same the digest. There are two unique possibilities for a message pair to collide, for HAVAL hashing [21]. The messages are decoded by the source which also sends *Src_reply* packet with data packets for all the critical integer posted by target with current UNIX time. With a confident ack-reply packet, hash value and receipt time of *Src_reply* packet, destination replies to the source. A source can be assumed if there is no WH attack by protected ack-reply extents within *1.2 times* of total *Hello_src* time calculated from source to destination. Thus, WH attacks are mitigated by this additional security.

3.2 Trust-Based (T-B) AODV Methodology

The T-BAODV protocol is suggested in this study. On every successful data transmission, the field that shows the trust value is updated. The route selection value that intended for each RREQ path determines the forthcoming data transmission. Rather than selecting the shortest or the longest route, this route selection is recycled for picking the most reliable route. The trust factor of one node over the others in the network is significantly increased and will be useful in the network communication in the future.

3.2.1 Trust Evaluation

The confidence of one node on the other is called the Trust as defined in the model. Various evaluation factors that define the trustworthiness are also known as the trust. In this model, the sensor nodes accumulatively compute the trust values of the neighbor's nodes rather than those of the other nodes in the network.

Trust Evaluation Factor: There are k dependence estimate conditions for each node. The trust assessment causes for k neighbor nodes are stored here. Trust evaluation matrix has several trust evaluation factors defined as follows:

Link quality: The ability of connection and devices to maintain traffic compactness for the link period is a promising parameter called the Link Quality. Parameters, such as distance, battery-operated power and mobility affect the link state between two neighbors.

Distance: The distance between two nodes contained in this. x coordinate is x_i and y coordinate of node I is y_i as:

$$D_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2},$$

where $0 \leqslant i, j \leqslant k$ and $i \neq j$.

Distinguishing Message: Communication dimension information included in this scenario. It shows a node's level of self-regard and regularity.

S_i: significant message value of node i, where $1 \leqslant i \leqslant k$
ss_i: identifying achievement count of node i
sf_i: determining letdown count of node i.

Sensing Result: Sensing result information for detected events is represented. It also has to sense data and to sense time for measures.

$R_i = \langle sr_i, st_i \rangle$: sensing result value of node i, where $1 \leqslant i \leqslant k$
sr_i: sensing data of node i
st_i: sensing time of node i

Mobility: A critical evaluation parameter of the mobile MANET network is mobility. A rigorous mobility definition illustrates topological network change assumed through the equations:

$$mob = \sum_{i=1}^{n} \frac{M_i}{n}$$

$$M_x = \sum_{t=0}^{T-\Delta t} \frac{|A_x(t) - A_x(t+\Delta t)|}{T}$$

$$A_x(t) = \sum_{i=1}^{n} \frac{dist(n_x, n_y)}{n-1}$$

where
$dist(n_x, n_i)$: space amid nodes x and y

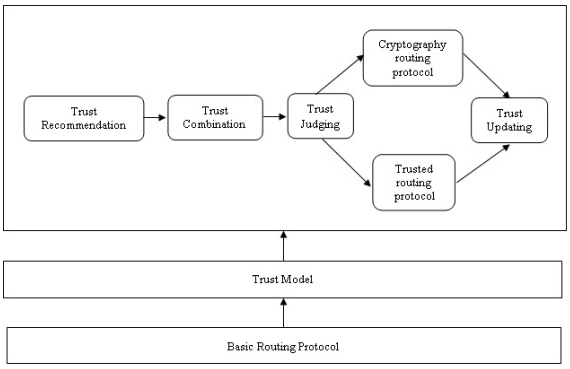


Fig. 2: Framework of trustworthy AODV

N: nodes quantity
$A_x(t)$: Average space among node x and very other nodes, at time t
M_x: medium qualified mobility of node x concerning other nodes during the imitation phase
T: Imitation phase
A_t: To compute the time trust value: A node's entire reliability is estimated on other confidence assessment causes.
T_i: trust significance of node i, where $1 \leqslant i \leqslant k$.

4 Proposed Trust-AODV with Route Optimization Using SDS

4.1 Framework of the Trusted-AODV

The TAODV involves three dissimilar models: basic AODVRP, a trusted AODVRP and a trust prototypical. This routing protocol of TAODV includes correct procedures, such as cryptographic routing response, trusted permutation, and trusted endorsement, trusted apprising, trusted direction-finding behavior and trust judging. According to Fig. 2, the structure and the relationship of these components are depicted. The following method describes the procedure adopted for establishing a trust-based relationship among the nodes and for performing a routing discovery.

MANET is highly mobile, infrastructure less, self-organizing and requires safe routing. For enhancing communication quality, a routing protocol is used. AODV routing protocol is used for this purpose through optimizing it. Several researchers have recently utilized the optimized routing concept. Many Bio-inspired algorithms have proved their effectiveness. These algorithms are adaptive, robust and effective.

4.2 Methodology

Trust AODV with route optimization using SDS is proposed in this work. It helps prevent malicious behavior and the uniform utilization of network resources. It is established on the collaboration between the agents, and SDS is a multi-agent inclusive in examining optimization procedure.

4.2.1 Proposed Trust AODV with Route Optimization Using SDS Algorithm

The main difference between the proposed TAODV and AODV is that TAODV can spawn many RREP packets and the packet can be changed to carry the path's trust. For uniform resource utilization, TAODV also updates a routing path at constant intervals. The SDS finds the best match for a particular model in a defined space. This work can draw the analogy of a model in a transcript certificate. Every agent independently operates during the searching process. They meet only to exchange the information that they find. In SDS, the concept of the time reserved for an agent to pass to its ideal position does not exist. Every agent, throughout SDS, is unable to access the whole search space, but it also carries information regarding the target model's entirety [22].

For example, all-inclusive certificate of the text with the complete term searches for the accessed agent. When the test function of the selected hypothesis returns a positive result, an agent becomes active, as seen in the restaurant game. Otherwise, the agent remains inactive. While searching for a word, the index position is stated as a hypothesis in the document with a counterweight from this point. This proposition checks a distinct character at an offset from the catalogue compared to the role at the same offset in the prototype. Many methods are organized to define the communication among agents with diffusion after the evaluation of their hypotheses.

Algorithm 1: The standard SDS algorithm

Beginning Stage: Entire agents to create primary evidence while a tentative criterion is not satisfied.
Test Point: Entire agents perform premise calculation.
Diffusion Stage: Communication strategy is performed.
Interconnected Stage: Active with the identical proposition aimlessly neutralizes.
Halt Phase: This involves the evaluation of tentative criteria.

Initialize: The agents provide the entrance to the objective model. The hypothesis locations randomly initialized can be partial to some positions known as a priori knowledge. There are two kinds which may impact the initialization point, as shown by Bishop: It assures that the minimum one is set with the best hypothesis if the ratio of the model and search space size is greater than 1. The former location of the model is known while executing the continuous examination

Table 1: Advantages and Disadvantages of GA, PSO, and ACO

Algorithm	Advantages	Disadvantages
GA	– Exchange information – Solve continuous problems in an well-organized way	– No space for the memory – Early junction – Weak native examines talent – Great computation strength – Testing to encode a problem in the form of a DNA
PSO	– Exchange information – Solve continuous problems in an efficient way	– Precipitate gathering – Weak limited examine capability
ACO	– It has a memory space – Speedy detection of virtuous results – Proficient in resolving TSP problem also, other discrete problems – Prospect sharing variations by reiterations	– Precipitate gathering – Weak, limited examine capability – Inactive in unraveling the uninterrupted harms

on the analogous examined spaces, such as consecutive video frames.

Test: At this stage, the agent decides its step by sedentary. It is attained by applying a task to check its existing hypothesis. The check function is the part of hypothesis valuation, and it varies based on the application domain. If the restricted assessment of the theory proceeds success, the agents set to lively. Otherwise, they remain inactive.

Diffusion: Hypothesis information is exchanged during this phase. This method is disseminating the current hypothesis of the active agents to inactive agents in the underlying idea. Three different strategies, known as recruitment strategies, are present for this dissemination. There are passive, dynamic and a combination of the two enrollments. This exchange of information results in agents involving the most significant hypotheses that recruit the inactive agents to their situation. Several agents associate around the most significant hypothesis if the connected phase is used in the search space. The typical SDS approach is the impassive method that is positioned.

Passive Enrolment: If the inactive agents are active, they randomly select other agents during passive recruitment, adopting their hypothesis. Though it is doubtful, many agents may converge into one iteration as per the ideal suggestion [23].

Algorithm 2: Passive enrolment algorithm

```
for respectively agent P in population do
    SWITCH
    CASE 1: agent P NOT dynamic
    Agent P implements agent Q
    CASE 1: agent Q in active
    Agent P assumes a novel unsystematic hypothesis
    END SWITCH
end
```

Active Recruitment: The active agents randomly select other agents in the actual enrollment procedure. The recruited agents receive the selected agent's prediction in case they are inactive. Hence, the active agents can grow to determine their different twin dimension. Every agent, in dynamic enrollment, should preserve an added variable which is involved if there has been a change in the agent's hypothesis. If an explanation from a lively agent is not received by an inactive agent in the process of recruitment, there must be a new random hypothesis that must be obtained to evade the inactive agents in the same situation of assumption for a long time.

Algorithm 3: Active recruitment algorithm

```
for all agents P in population do
    SWITCH
    CASE 1: agent P Active
    Select random agent Q from population
    Case 2: agent q In Active
    Agent Q adopts agent P hypothesis
    Agent Q become engaged
    End Switch
    for all agents P in the population do
        if agent P In active & & Agent P Not involved
          then
            Agent P accepts a fresh arbitrary
              hypothesis
        end
    end
end
```

Dual Enrollment: The reflexive enrollment directly followed by dynamic registration is referred to as a combination enrollment strategy.

Relate: This is optional and incorporated in case there are many models in the search space. The preservation of several collections worthy hypotheses of active agents as well as a unit of self-motivated reordering of agents is allowed in this technique. This phase can assist in dynamic search spaces. In turn, it allows agent clusters to align themselves according to the right hypothesis.

Context-free mode and context-sensitive modes are the two modes of the narrate level.

Halting: The SDS procedure fixes whether the agent population has extended a state that regulates the end of the quest after every iteration of test and diffusion along with optional relate phase. This criterion is called the halting benchmarks. As soon as the paramount hypothesis/hypotheses in the search space are found, the search stops. However, this may be difficult to ascertain due to noisy data. The active populations of the agents remain small, during the initial search iterations, till an optimal suggestion reaches more agents allowed into this population group. Then size of the cluster increases. The cluster finds the finest hypothesis to stabilize the provisional search space and model parameters. The criteria that determine whether the SDS search process should come to an end are weak halting and robust halting principles.

Weak Uncertain Standards: This situation states that when a percentage of all the agents, nevertheless of their hypothesis, is active, the SDS should stop. The population should stabilize at a certain level once this threshold is crossed. It can view the number of active agents that remain fixed, with some tolerance edge, for some iteration. The search stops once this criterion is reached.

Robust Uncertain Standards: The termination state is defined as being associated with the number of active agents in the most extensive collection. It means considering the hypothesis which contains maximum agents clustered around it and then relating the equal acceptance law applied to the weak, uncertain standards. The current difference is that we are looking at the percentage of the active agents inside this leading cluster.

5 Results and Discussion

The simulation investigation accompanied with 25 nodes to spread over 2 sq. km AODVRP is recycled. Two tests are accompanied by the paramount without malicious nodes and the next with 20% of the malicious nodes. Fig. 3a demonstrates the throughput in bps.

Fig. 3(b) indicates that throughput is condensed by 58.63% in the occurrence of 20% of malicious nodes in MANET. The proposed AODV routing drastically improves the throughput in a malicious environment achieving a throughput which is 5.05% less than the throughput achieved by AODV in a non-malicious environment.

5.1 Analysis of SD Routing Technique with Trust Based Ad Hoc

In this section, the trust AODV-without attack, trust AODV-with 10% malicious node, trust AODV-with 20% malicious node, trust AODV with route optimization using stochastic diffusion, trust AODV with route optimization using stochastic diffusion-with 10% malicious node and trust AODV with route optimization using stochastic diffusion-with 20% malicious node methods are evaluated. Tables 2–4 show the summary of average PDR, average end-to-end delay and middling quantity hops to drop. Figs. 4(a)–(c), 5(a)–(c) and 6(a)–(c) show the average PDR, end-to-end delay and number hops to sink without attack, with 10% and 20% malicious nodes.

Fig. 4(a) reveals that the trust AODV with route optimization using stochastic diffusion has higher average PDR by 2.22% for 75 nodes, by 3.96% for 150 nodes, by 4.89% for 225 nodes, by 4.13% for 300 nodes and by 4.85% for 375 nodes compared with trust AODV without attack.

Fig. 4(b) shows that the trust AODV with route optimization using stochastic diffusion-with 10% malicious nodes has higher average PDR by 5.08% for 75 nodes, by 3.96% for 150 nodes, by 2.24% for 225 nodes, by 2.57% for 300 nodes and by 3.07% for 375 nodes compared with trust AODV with 10% malicious nodes.

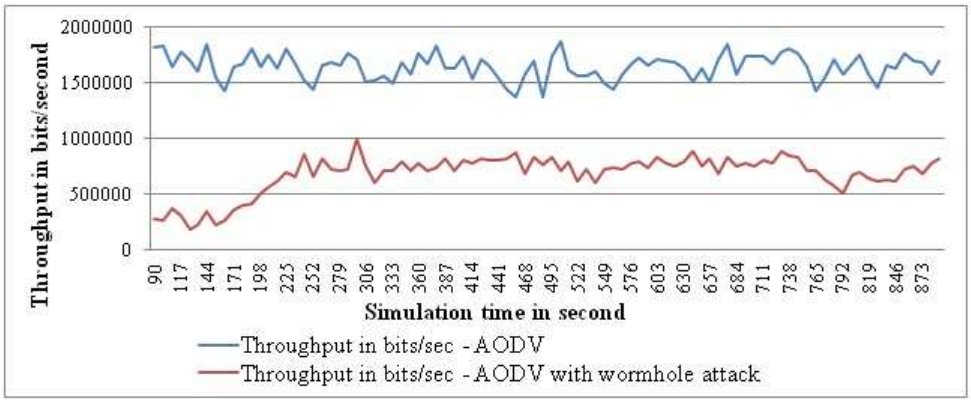
Fig. 4(c) illustrates observed that the trust AODV with route optimization using stochastic diffusion-with 20% malicious nodes has higher average PDR by 3.79% for 75 nodes, by 2.5% for 150 nodes, by 2.67% for 225 nodes, by 4.23% for 300 nodes and by 4.87% for 375 nodes compared with trust AODV with 20% malicious nodes.

Fig. 5(a) exhibits that the trust AODV with route optimization using stochastic diffusion has subordinate average end-to-end delay by 3.33% for 75 nodes, by 2.54% for 150 nodes, by 2.15% for 225 nodes, by 4.88% for 300 nodes and by 2.73% for 375 nodes compared with trust AODV without attack.

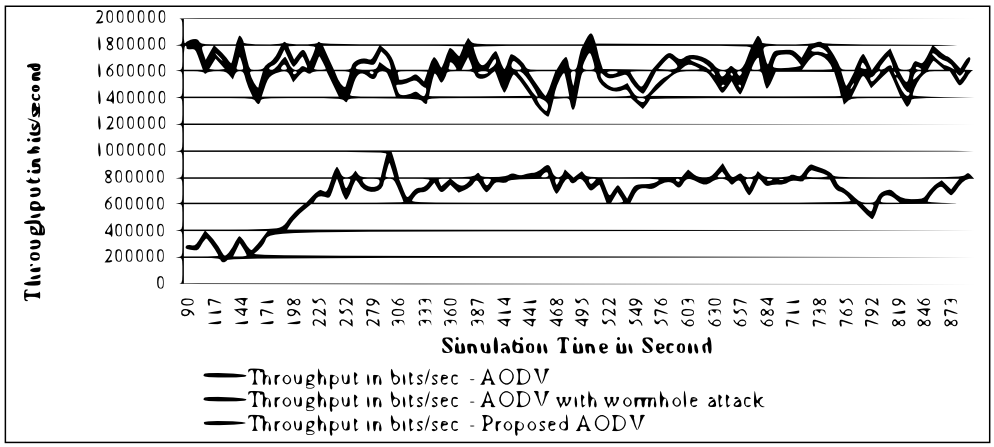
Fig. 5(b) indicates that the trust AODV with route optimization using stochastic diffusion-with 10% malicious nodes has subordinate average end-to-end delay by 4.65% for 75 nodes, by 2.4% for 150 nodes, by 2.94% for 225 nodes, by 4.26% for 300 nodes and by 2.66% for 375 nodes while associated with trust AODV with 10% malicious nodes.

Fig. 5(c) reveals that the trust AODV with route optimization using stochastic diffusion-with 20% malicious nodes has average subordinate end-to-end delay by 4.47% for 75 nodes, by 2.24% for 150 nodes, by 3.94% for 225 number of nodes, by 3.75% for 300 nodes and by 2.19% for 375 nodes once associated with trust AODV with 20% malicious nodes.

Fig. 6(a) exhibits that the trust AODV with route optimization using stochastic diffusion has lower average number of hops to sink by 4.34% for 75 nodes, by 6.55% for 150 nodes, by 4.58% for 225 nodes, by 6.06% for 300



(a) Throughput in bps



(b) Throughput in bps

Fig. 3

Table 2: Summary of average PDR

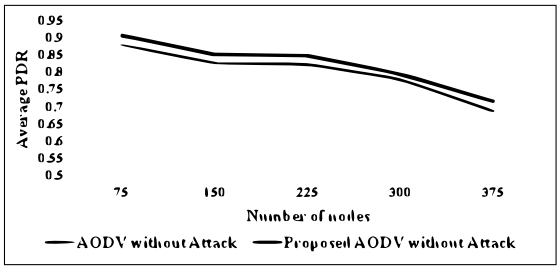
No. of nodes	Trust AODV			Trust AODV with route Optimization		
	without attack	with 10% malicious node	with 20% malicious node	using stochastic diffusion	using stochastic diffusion with 10% malicious node	using stochastic diffusion with 20% malicious node
75	0.9409	0.778	0.7579	0.9621	0.8186	0.7872
150	0.8807	0.7383	0.7253	0.9163	0.7682	0.7437
225	0.8693	0.7392	0.7185	0.9129	0.756	0.738
300	0.8292	0.7021	0.6754	0.8642	0.7204	0.7046
375	0.7523	0.654	0.6263	0.7897	0.6744	0.6576

Table 3: Summary of average end-to-end delay

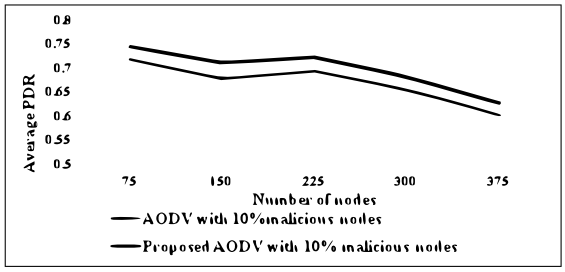
No. of nodes	Trust AODV			Trust AODV with route optimization using stochastic diffusion		
	without attack	with 10% malicious node	with 20% malicious node	using stochastic diffusion	with 10% malicious node	with 20% malicious node
75	0.00122	0.00132	0.00137	0.00118	0.00126	0.00131
150	0.00159	0.00168	0.00135	0.00155	0.00164	0.00132
225	0.00328	0.00344	0.00155	0.00321	0.00334	0.00149
300	0.00482	0.00503	0.00163	0.00459	0.00482	0.00157
350	0.0152	0.01635	0.00969	0.01479	0.01592	0.00948

Table 4: Summary of average number of hops to sink

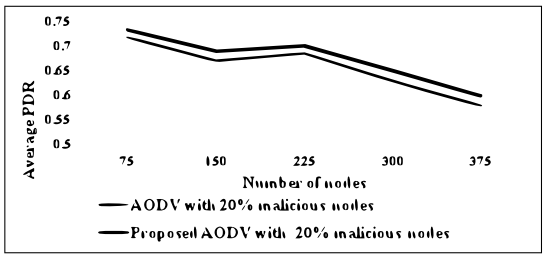
No. of nodes	Trust AODV			Trust AODV with route Optimization		
	without Attack	Trust AODV with 10% malicious node	Trust AODV with 20% malicious node	Using stochastic diffusion	Using stochastic diffusion with 10% malicious node	Using stochastic diffusion with 20% malicious node
75	4.7	5	5.3	4.5	4.8	5
150	6.3	6.6	7	5.9	6.1	6.5
225	6.7	7.1	7.6	6.4	6.5	7.1
300	6.8	7.4	7.9	6.4	6.9	7.3
375	7.3	7.7	8.7	6.9	7.4	8.2



(a) Average PDR (without attack)

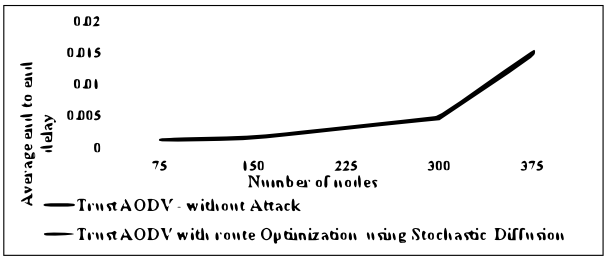


(b) Average PDR (with 10% malicious nodes)

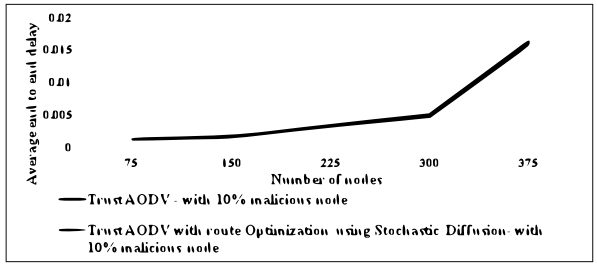


(c) Average PDR (with 20% malicious nodes)

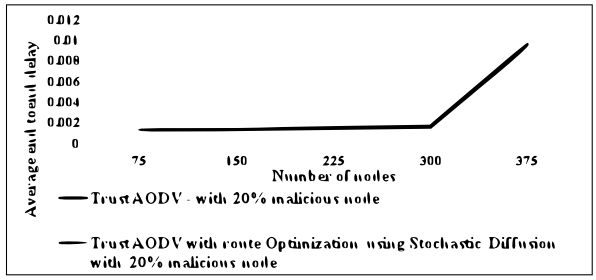
Fig. 4



(a) Average end-to-end delay (without attack)



(b) Average end-to-end delay (with 10% malicious nodes)



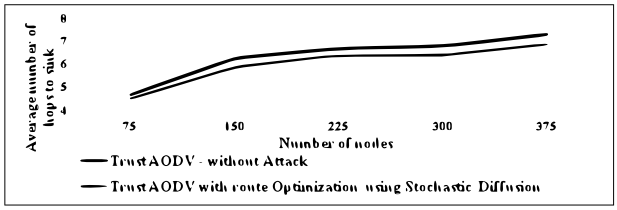
(c) Average end-to-end delay (with 20% malicious nodes)

Fig. 5

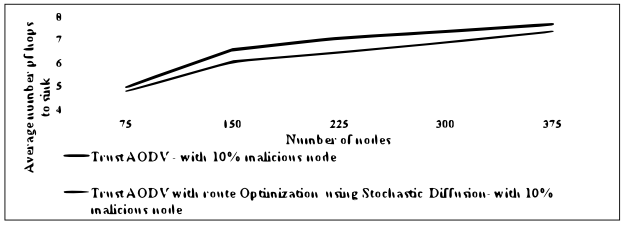
nodes and by 5.63% for 375 nodes when compared with trust AODV without attack.

Fig. 6(b) indicates that the Trust-AODV with route optimization using stochastic diffusion-with 10% malicious nodes has lower average hops to sink by 4.08% for 75 nodes, by 6.87% for 150 nodes, by 8.82% for 225 nodes, by 6.99% for 300 nodes and by 3.97% for 375 nodes after comparing with trust AODV with 10% malicious nodes.

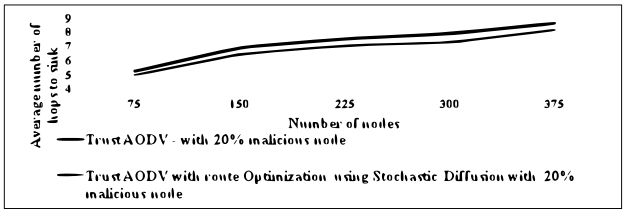
Fig. 6(c) shows that the trust AODV with route optimization using stochastic diffusion-with 20% malicious nodes has lower average hops to sink by 5.82% for 75 nodes, by 7.4% for 150 nodes, by 6.8% for 225 nodes, by 7.89% for 300 nodes and by 5.91% for 375 nodes compared with Trust-AODV with 20% malicious nodes.



(a) Average number of hops to sink (without attack)



(b) Average hops to sink (with 10% malicious nodes)



(c) Average number of hops to sink (with 20% malicious nodes)

Fig. 6

5.2 Analysis Discussions on SD Routing with Trust Based Ad Hoc

MANET does not verify the user identity before data access, so these networks are susceptible to unauthorized data manipulation. Hence, it is difficult to design the authentic systems that protect MANETs from routing attacks in the occurrence of malicious nodes. Scheming nodes create an illusion that two remote MANET regions directly connect through nodes, in a WH attack on the MANET routing protocols. These connected nodes appear to be neighbors, but they are very remote from one another. Trust evaluation is calculated after a route optimized with TAODV for SDS proposed.

Results have shown that the trust AODV with route optimization using the stochastic diffusion has higher average PDR by 4.85% for 375 nodes, by 4.13% for 300 nodes, by 4.89% for 225 nodes, by 3.96% for 150 nodes, by 2.22% for 75 nodes compared to trust AODV without attack. With the route optimization using stochastic diffusion, the Trust-AODV-with 10% malicious nodes have higher average PDR by 3.07% for 375 nodes, by 2.57% for 300 nodes, by 2.24% for 225 nodes, 3.96% for 150 nodes and by 5.08% for 75 nodes, while related with trust AODV with 10% malicious nodes. The same with 20% malicious nodes have higher average PDR by 4.87% for 375 nodes, by 4.23% for 300 nodes, by 2.5% for 150 nodes, by 2.67% for 225 nodes and by 3.79% for 75 nodes when compared with Trust-AODV with 20% malicious nodes.

6 Conclusion

In MANET environment, the WH attacks are formed by the changes in performance due to the examination of the presence of malicious nodes because they form the WH attack. An improved AODV with packets *Hello_src* and Src_reply to mitigate the WH attack is proposed. The *Hello_src* packet is broadcast by neighbor discovery and synchronized time is involved to a reserved bit in UNIX time set-up. All neighbor nodes in a delivery assortment of receiving Hello message reply by joining Hello message with recent acknowledged time in UNIX set-up and response. A wormhole is suspected based on the delay, and an alternate route is discovered ignoring suspicious neighborhood node.

The proposed AODVRP implements a secured-packet reply, *Src_reply*, confirming the packet reaching the destination if an alternative way is not available. In this work, the presence of the malicious node is measured by performance variances in MANETs. A novel solution for trust evaluation in all nodes was constructed on limits like node stability which is well-defined by its mobility, time interval, and enduring battery energy. Transmission route is the necessary selection for the Node trust. This work proposes the TAODV protocol. MANETs are susceptible to unlawful data management as it does not validate user uniqueness previously certifying data entrance. Thus, it is perplexing to design safety machines that protect MANETs from routing attacks in the occurrence of malicious nodes. WH is an attack on MANET routing protocols where plotting nodes form an impression that two foreign MANET states are openly coupled over nodes which are neighbors, but are genuinely far from each other. The proposed route is enhanced with TAODV for SDS and trust evaluation is computed.

References

[1] A.K. Abdelaziz, M. Nafaa and G. Salim, Survey of routing attacks and countermeasures in mobile ad hoc networks. In Computer Modelling and Simulation (UKSim), 15th International IEEE Conference on UKSim, 693–698 (2013).

[2] A.M. Adrian, A. Utamima and K.J. Wang. A comparative study of GA, PSO and ACO for solving construction site layout optimization. KSCE Journal of Civil Engineering, **19**(3), 520–527 (2015).

[3] R.K. Bar, J.K. Mandal and M.M. Singh. QoS of MANet through trust based AODV routing protocol by exclusion of black hole attack. Procedia Technology, **10**, 530–537 (2013).

[4] N. Chaubey, A. Aggarwal, S. Gandhi and K.A. Jani (2015, February). Performance Analysis of TSDRP and AODV Routing Protocol under Black Hole Attacks in MANETs by Varying Network Size. In Advanced Computing & Communication Technologies (ACCT), Fifth International IEEE Conference on, 320–324 (2015).
[5] J.H. Cho, A. Swami and R. Chen. A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys & Tutorials, **13**(4), 562–583 (2011).
[6] H. Ehsan and F.A. Khan. Malicious AODV: implementation and analysis of routing attacks in MANETs. In Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference on, 1181–1187 (2012).
[7] I.M. El-henawy, and M.M. Ismail. A Hybrid Swarm Intelligence Technique for Solving Integer Multi-objective Problems. International Journal of Computer Applications, **87**(3) (2014).
[8] A. Gagandeep and P. Kumar. Analysis of different security attacks in MANETs on protocol stack A-review. International Journal of Engineering and Advanced Technology (IJEAT), **1**(5), 269–75 (2012).
[9] M. Ganesan, P. Patil, M.D. Fathima and M.S. Saravanan. Stimulated Particle Swarm Optimization Routing Protocol-A Review. International Journal of Computer Science and Information Technologies (IJCSIT), **5**(2), 1106–1111 (2014).
[10] Sudhakar Sengan and S. Chenthur Pandian, Hybrid Cluster based Geographical Routing Protocol to Mitigate Malicious Nodes in Mobile Ad Hoc Network, International Journal of Ad Hoc and Ubiquitous Computing, **21**(4), 224–236 (2016).
[11] A.K. Gupta, H. Sadawarti and A.K. Verma. Review of various routing protocols for MANETs. International Journal of Information and Electronics Engineering, **1**(3), p. 251 (2011).
[12] J. Hur, Y. Lee, S.M. Hong and H. Yoon. Trust management for resilient wireless sensor networks. In Information Security and Cryptology—ICISC 2005, Springer, Berlin Heidelberg, 56–68 (2006).
[13] Y.K. Jain and P. Sharma, Trust based ad hoc on-demand distance vector for MANET. In National Conference on Security Issues in Network Technologies (NCSI-2012), 1–11 (2012).
[14] R.H. Jhaveri, A.D. Patel, J.D. Parmar and B.I. Shah. MANET routing protocols and wormhole attack against AODV. International Journal of Computer Science and Network Security, **10**(4), 12–18 (2010).
[15] J. Kennedy and R.C. Eberhart. Particle swarm optimization. Proceedings of IEEE International Conference on Neural Networks, **IV**, 1942–1948 (1995).
[16] S. Kumar and K. Dutta. Security issues in mobile ad hoc networks: A survey. Security, Privacy, Trust and Resource Management in Mobile and Wireless Communications, 176–221 (2014).
[17] G.S. Mamatha and D.S. Sharma. Network Layer Attacks and Defense Mechanisms in MANETS-A Survey. International Journal of Computer Applications, **9**(9) (2010).
[18] R.S. Mangrulkar, P.V. Chavan and S.N. Dagadkar. Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT. International Journal of Computer Applications, **0975–8887**, 36–39 (2010).
[19] M.M. Morshed and M.R. Islam (2013, February). CBSRP: Cluster Based Secure Routing Protocol. In: IEEE 3rd International Conference on Advance Computing (IACC), 571–576 (2013).
[20] Sudhakar Sengan and Chenthur Pandian. S, Trustworthy Position Based Routing to Mitigate against the Malicious Attacks to Signifies Secured Data Packet using Geographic Routing Protocol in MANET, WSEAS Transactions on Communications, **12**(11), 584–2013 (2013).
[21] V.H. Patel, M.A. Zaveri and H.K. Rath. Trust Based Routing in Mobile Ad-Hoc Networks. Lecture Notes on Software Engineering, **3**(4), 318 (2015).
[22] M. Sadeghi and S. Yahya. Analysis of Wormhole attack on MANETs using different MANET routing protocols. In Ubiquitous and Future Networks (ICUFN), Fourth International Conference on, 301–305 (2012).
[23] H. Said and K. El-Rayes, Performance of global optimization models for dynamic site layout planning of construction projects. Automation in Construction, **36**, 71–78 (2013).
[24] M. Sardar, and K. Majumder. A Comparative Study On Different Trust Based Routing Schemes In Manet. International Journal of Wireless & Mobile Networks, **5**(5), 145 (2013).
[25] E.M. Shakshuki, N. Kang, and T.R. Sheltami. EAACK—a secure intrusion- detection system for MANETs. IEEE Transactions on industrial electronics, **60**(3), 1089–1098 (2013).
[26] Sudhakar Sengan and Chenthur Pandian S, An Efficient Agent-Based Intrusion Detection System for Detecting Malicious Nodes in MANET Routing, International Review on Computers and Software (I.RE.CO.S.), **7**(6), 3037–304 (2012).
[27] N. Sreenath, A. Amuthan and p. Selvigirija (2012), Countermeasures against multicast attacks on enhanced-on demand multicast routing protocol in manets. In Computer Communication and Informatics (ICCCI), IEEE International Conference on, 1–7 (2012).
[28] Sudhakar Sengan and Chenthur Pandian S, Secure Packet Encryption and Key Exchange System in Mobile Ad hoc Network, Journal of Computer Science, **6**, 908–912 (2012).
[29] R. KirubaBuri and T. Jayasankar, Intelligence Intrusion Detection Using PSO with Decision Tree Algorithm for Adhoc Networks , Bioscience Biotechnology Research Communications, Special Issue Recent Trends in Computing and Communication Technology, **12**(2), 27–34 (2019).
[30] E. Vishnupriya, T. Jayasankar and P. Maheswara Venkatesh, SDAOR: Secure Data Transmission of Optimum Routing Protocol in Wireless Sensor Networks For Surveillance Applications, ARPN Journal of Engineering and Applied Sciences, **10**(16), 6917–6931 (2015).

N. Satheesh has worked as a Professor, Dept. of CSE in St. Martin's Engineering College, Dhulapally, Secunderabad since May, 2019. He received B.E.-ECE from Sri Balaji Chockalingam Engineering College, Arni, University of Madras in 2004. He received M.E.-CSE from Annamalai University, Chidambaram in 2008. He was awarded Ph.D. in Computer Science & Engineering from Karpagam Academy of Higher Education, Karpagam University in 2018. His area of specialization is Wireless Security, Wireless Sensor Networks, and Internet of Things. He has 11 years of teaching experience and 2 + years of software experience. He has 05: International Journal Publications and 04: International Conference Publications.

K. Prasadh sreves as Professor & Principal in Vijnan Institute of Technology (VISAT) Elanji, Ernakulum. He B.E. Degree from Madurai Kamaraj University and M.E. Degree from M.S University Tirunelveli, and Ph.D. from VM University Salem, Tamilnadu. He has 23 years of academic experience. He has published more than 22 papers at National and International Journals and Conferences. He is member of Professional Bodies, such as IE, IEEE, CSI, MISTE and Charted Engineer. He is a reviewer of four well-reputed International Journals. He received best awards by New Delhi three times.