Cluster Computing
https://doi.org/10.1007/s10586-017-1622-9

Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust

Deepak C. Mehetre[1] · S. Emalda Roslin[1] · Sanjeev J. Wagh[2]

Received: 13 October 2017 / Revised: 12 December 2017 / Accepted: 23 December 2017
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract
In the recent era, security is the major problem in sensor networks. Wireless sensor networks (WSNs) are mostly used for various real-world applications. However, WSNs face a lot of insider and outsider attacks, and it is complex to identify and protect towards insider attacks. Generally, an insider attack, in which the intruders choose several received data packets to drop, threatens the clustered WSNs. This situation has occurred because of the unattended clustered environments in the network. To overcome this problem, this paper proposes a trustable and secure routing scheme using two-stage security mechanism, and dual assurance scheme, for selecting the node and securing the data packet for WSNs. Both schemes are based on Active Trust to protect several kinds of attacks, such as black hole attack, and selective forwarding attack, during routing. Therefore, this paper identifies the trusted path and provides the secure routing paths using trust and Cuckoo search algorithm. Energy is the performance parameter utilized in the proposed scheme. The experimental result proves that proposed system provides the assurance to prolong the network lifespan and the probability of secure routing path in the network.

Keywords Routing · Active Trust · Security · Black hole attack · Selective forwarding attack · CS algorithm

1 Introduction

Over last few decades, the popularity of a topic, which is more prone to be important for civil and military applications are increasing. Several applications of WSNs are emergency scenarios, manufacturing environments, battlefields, etc. Due to the advancements in fields, like microelectronics, integrated electronics, the development of sensor nodes is intensified [1]. The properties that combined in networks are mobile, sensors, wireless, and ad hoc. These properties are implemented in the real world for energy emergency response information [2], and monitoring factory environments [3]. The networks are vulnerable to various kinds of security threats from intruders at the network layer [4]. The main motivation is that the sensor nodes form a structure to observe the actions in unpredictable environments by acting in a self-compositely, self-harmonize ad hoc manner, i.e., without the need of human intervention [1].

Routing is the process of selecting the most efficient paths in a network. The router presents the direction of traffic activated on the web [5]. The routing of data packets from a source to a sink through the network is of a more interesting challenge for the researchers in the WSN domain. Limitation of energy resources is a major impact, as energy is an important and fundamental component in designing of the routing protocols [1]. Routing is operated for various forms of sensor networks that consist of electronic information sensor networks, transportation networks, and the public switched telephone network. The main requirement of WSN is the trust on the behavior [6]. The data packets can be routed in the largest routing network around eloquent areas so that a complete mishap of the network can be overlooked [1]. The secure routing protocols [7] are not effectively averting malicious nodes that are authorized to the sensor network from doing any illegal activities [8]. In extension with, to dodge a strain of certain nodes to curtail the jeopardy barrier of the network, the routing algorithm should haul load balancing into rationale, directing to misplaced paths between the

✉ Deepak C. Mehetre
dcmehetre14@gmail.com

[1] Computer Science Department, Sathyabama University, Chennai, India

[2] Information Technology Department, Govt. COE, Shivaji University, Karad, India

Published online: 14 March 2018

source and the sink. Furthermore, to lessen superfluous transmissions of the same data, the coalition of sensed data needs to be considered in WSN routing protocols [1].

A malicious node randomly declines to drop the packets or forward the communications [9]. There is no requirement to fix the positions of the malicious nodes because the sensor nodes are applicable in the field of high risk. Therefore, there is no security for most of the WSN, which averts the simple intrusions on the sensor nodes [3,4]. The Principle service in WSNs is the routing of data packets. In preference, most of the current routing protocols endeavor at metrics, like reliability, robustness, responsiveness, and preserving energy [1]. However, the network protocol and techniques are self-managed. Therefore, few of the design issues are subsisted in sensor nodes and sensor networks. These issues are considered in the design of network protocols. The collision of these issues is employed to evaluate various types of methods [10]. The issues include fault tolerance, scalability, power consumption, network topology, hardware constraints, production cost, transmission media, and environment [4]. But, the non-forbearance of possible security obstacles in the area of routing is dangerous because, in almost all application areas, in which WSNs are used, sensor nodes are deployed in unfavorable environments, providing the opportunity for the attacker to launch certain attacks [11] against the sensor nodes. Specifically, the arresting of nodes [12] is an imperative issue because it is easy for adversaries to access the sensors substantially [1]. The majority of the research fields of security in WSN [13] contain the secure location, secure routing, key management, intrusions and prevention [14].

Traditionally, various methods have been initiated to avert malicious nodes from the clustered network, finding the best routing path using trust-based systems, and intrusion detection system. Though these methods have some benefits, still they are facing some contradicting problems in energy efficiency, security, and complicatedness, for attaining the trusted node in the clustered network. Therefore, the main purpose of this paper is to identify and avoid the malicious nodes based on Active Trust for Cluster-based WSNs. In this paper, a two scheme security mechanism is designed using Detection Packet (DP), and trust, to detect the malicious nodes. Then, dual assurance scheme, which is comprised of Selective Forwarding-based packet validation and ECC-based packet security, is used to ensure that the data packet is securable among multiple numbers of nodes. Finally, the secure routing path is identified using the CS algorithm.

The main contributions of this paper developed to provide secure and trustable data routing path are as follows,

- Two scheme security mechanism namely, Detection of attack node by DP, and trust to detect, and prevent the node from the attacker, to select the trusted paths that are based on the minimal threshold value.
- Dual assurance scheme is divided into two types, such as selective forwarding based packet validation, and ECC based packet security, which is used to transmit the secure data packets from source to destination.

The rest of this paper is organized as follows: The brief information about the related works from the literature is given in Sect. 2. Section 3 provides the system description that is used for the experimentation. Section 4 provides the results and discussion. Finally, Sect. 5 concludes the paper.

2 Literature survey

This section depicts a review of the literature on various existing techniques in WSN to perceive the disadvantages. Several routing protocols and security techniques have been presented and implemented for the detection and prevention of attacks in the network.

Liu et al. [15] have developed an Active Trust routing system that depends on active detection. This system had high security, routing, expectation as well as scalability. The active trust system could sense the trust model and thereby, stop doubtful nodes from participating in routing. It had high energy efficiency and made the use of silt energy for the procreation of multiple detection routes. This paper proposes a trustable and secure routing scheme using two-stage security mechanism, and dual assurance scheme, for selecting the node and securing the data packet for WSNs. Both schemes are based on Active Trust to protect several kinds of attacks, such as black hole attack, and selective forwarding attack, during routing. Das et al. [16] have utilized the genetic algorithm (GA), for the dynamic formation of cluster heads as well as clusters depending on the distance of the nodes from cluster node utilizing the trust of the sensor nodes. This paper identifies the trusted path and provides the secure routing paths using trust and CS algorithm.

Sharmila et al. [17] have implemented lightweight detection scheme for the detection of the sinkhole attack inside the WSN. The message digest technique was designed for identifying the sinkhole attacks and provided few collision resistant. The system identified the sinkhole attack, when the message digest technique broadcasted in the trustable route, which is varied from nature. The proposed work protects several kinds of attacks, such as black hole attack, and selective forwarding attack, during routing based on active trust. Karlof et al. [3] have worked on muting security in WSN. None of the sensor network protocols had acknowledged the security in the grant. After this observation, the authors have found and given few security goals for routing in a sensor network, which gave the possible ways of attacks on ad-hoc as well as peer-to-peer network, were adapted in potent attacks in protest with sensor networks. Also, the authors have implemented two classes of new kinds of attacks against sensor network, known as sinkholes and HELLO Roods.

Alajmi et al. [4] have suggested a selective forwarding detection (SFD), and monitoring approach, for finding and monitoring the selective forwarding attack in WSN. The approach could detect selective forwarding attack in network layer without considerable efforts. In this sort of attack, the attacked node could work as like the different nodes present in the network, but it could change or drop the private data before sending the packet to other sensor nodes. The system provides guaranty for the data while transferring between nodes. The proposed method selects the node and secures the data packet for WSNs based on the two-stage security mechanism and dual assurance scheme. Geethu et al. [18] have developed a multipath transmitting system. The built-up system was utilized as a defense technique against selective forwarding attack. In this system, if a node could sense a packet drop at the time of routing, then the packet was forwarded via an alternate route. Because of the resending technique, the reliability of the routing mechanism was maximized. The proposed work protects the network from several kinds of attacks, such as black hole attack, and selective forwarding attack based on active trust.

Motamedi et al. [19] have designed unmanned aerial vehicles (UAVs) for finding the black hole attacks inside WSN. In black hole attack, a faulty node that could show that the route to the destination was shortest and feasible, attract more network traffic, and drop all the data packets. To solve this issue in the minimum time, the authors had developed a method, finding the faulty node with maximum probability. The method was utilized for verifying nodes, and Sequential Probability Ratio Test technique was used as a dynamic threshold system for avoiding malicious nodes. The proposed work detects the malicious nodes based on a two scheme security mechanism which is designed by DP, and trust. Latha et al. [14] have implemented a security method, used to search the routing path as secure, and also used to find trustable sensor node. But, while executing this method in the real world, and in an active system is not possible to transmit the secure node. It provided the possibility of few of the feature to enhance the system. In the proposed method, the secure routing path is identified using the CS algorithm.

2.1 Challenges

- The major challenge of Active Trust routing system [15] is that the method is not suitable for maximizing the performance of the network security and energy efficiency in WSNs.
- In lightweight detection scheme [17], there is a possibility of generating similar digest values through some sensor nodes for the dissimilar communications, while a large number of digest values generated in the sensor network, and that led to the rate of false negative error, is considered as the drawback in this method.
- The major factor in muting security [3] is that the cryptography only is not adequate because the authentication methods and link layer encryption methods are more expensive to provide security against outsiders' attacks.
- UAVs [19] are not suitable to verify the sensor nodes, which are similar to least visited the first node, and also this method cannot employ clustering techniques to transmit the nodes to the cluster head (CH).

3 System model

This section presents the system model [20], as shown in Fig. 1. WSN contains a number of sensor nodes, denoted as j, with only one sink or BS, M_H. The wireless connection signifies straight transmission among the sensor nodes in the radio range. Every sensor node is consistently shared within the dimensions of P_m and Q_m in meters, with its maximal transmission radio range. Every node has its ID, and the nodes are collected to form a cluster. BS is situated in the position of $\{0.5P_m, 0.5Q_m\}$, which is the optimum location to obtain the entire data representations from the sensor nodes associated with the sensor network. The coordinates of the nodes are given as $(P_i,\ Q_i)$. The data is transmitted to the sink from each sensor node by cluster head based routing methods. Herein, H_C is the possible number of nodes that are activated as cluster heads (M_G). H_C^j is a group of sensor nodes that are situated in the cluster group M_G. This indicates that the network is separated into H_C cluster number, whereas the calculation of the ordinary sensor nodes is equivalent to $j - H_C$. If the groups of the cluster are created within the network, then the data packets are transmitted from every sensor node N_i to its consequent cluster head M_G, and the cluster head gathers the entire data packets. The gathered data packets are forwarded to BS, M_H. After deploying all the sensor node to a permanent position, the distance among the fth ordinary sensor node to the gth cluster head is indicated as, r_{fg} and the distance between the gth cluster head to the BS, M_H is indicated as, s_g. The system model of the clustered WSN (CWSN) is shown in Fig. 1.

4 Detecting and preventing the malicious attacks in clustered WSNs using trust and Cuckoo search algorithm

The main objective of this paper is to develop a trustable secure routing scheme for clustered WSNs and to provide a mechanism that consists of active detection routing protocol and data routing protocol, which minimizes the probability of malicious nodes or compromised nodes being selected as

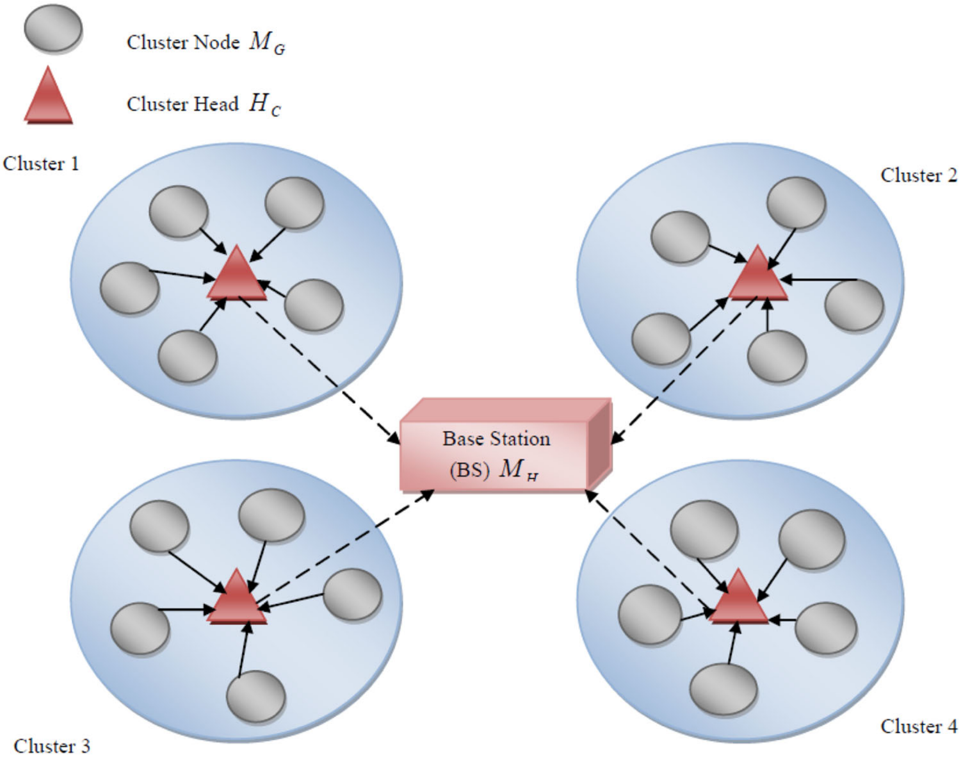


Fig. 1 Overview of clustered WSN

mutual nodes. The proposed work is intended to maximize the lifespan of sensor nodes by distributing the data packets to a better route path. To attain this objective effectively, a protocol is presented to find the trustable path from source to destination for the WSNs. Therefore, the source node is generated, while the network transmits the data from source to destination. The transmitted data is encrypted using the elliptic curve cryptography (ECC). The encrypted data is selected and verified at each sensor node using the two-stage security mechanism, which is used for selecting the possible number of the sensor node. The first stage represents the majority of the paths. Accordingly, the estimated paths detect the malicious nodes based on DP. After detecting the malicious node, the minimum threshold value is considered for the entire path to secure the routing path. Then, dual assurance scheme that employs selective forwarding-based packet validation, and ECC-based packet security is used to ensure that the forwarded data packet is securable. The secure routing path is identified in the entire path transmission using the trust path selection, and CS algorithm, so as to protect the network from the black hole and selective forwarding attacks.

4.1 Generation of k-paths

In a network, a graph structure is deployed to select the source and the destination nodes. The process of node selection describes that the user can choose the source and destination nodes along with their corresponding identification address. After that, generate the k path routing scheme to find the shortest path in the network. This k path routing scheme is based on the correlation of finding the minimum number of possible bandwidth or minimum path among two sensor nodes in the transmission networks, which believe that every edge in the sensor network has the shortest bandwidth value. CS algorithm has been employed to find the optimal solution, i.e., the best route. Herein, I denote the intruder that tries to attack the system, and the structure of the proposed scheme is shown in Fig. 2.

4.2 Two-stage security mechanism for node selection

The generated path is selected to transmit the secure data from the source node to destination node using the proposed two-stage security mechanisms. The first phase depicts that the majority of the paths are estimated. The malicious nodes in the computed paths are identified using detection packet (DP). i.e., after estimating the path, if it satisfies the node based on the condition, then it is the authentic node. Otherwise, it is considered as a malicious node (black hole attacker node). Therefore, the unsecured path and thereby, the malicious attacks, can be eliminated by the system. After identifying the black hole, and selective forwarding attack node, the low-level threshold value is measured for the entire path to transmit the secure routing path using the trust-based mechanism, whereas the threshold value is estimated for each

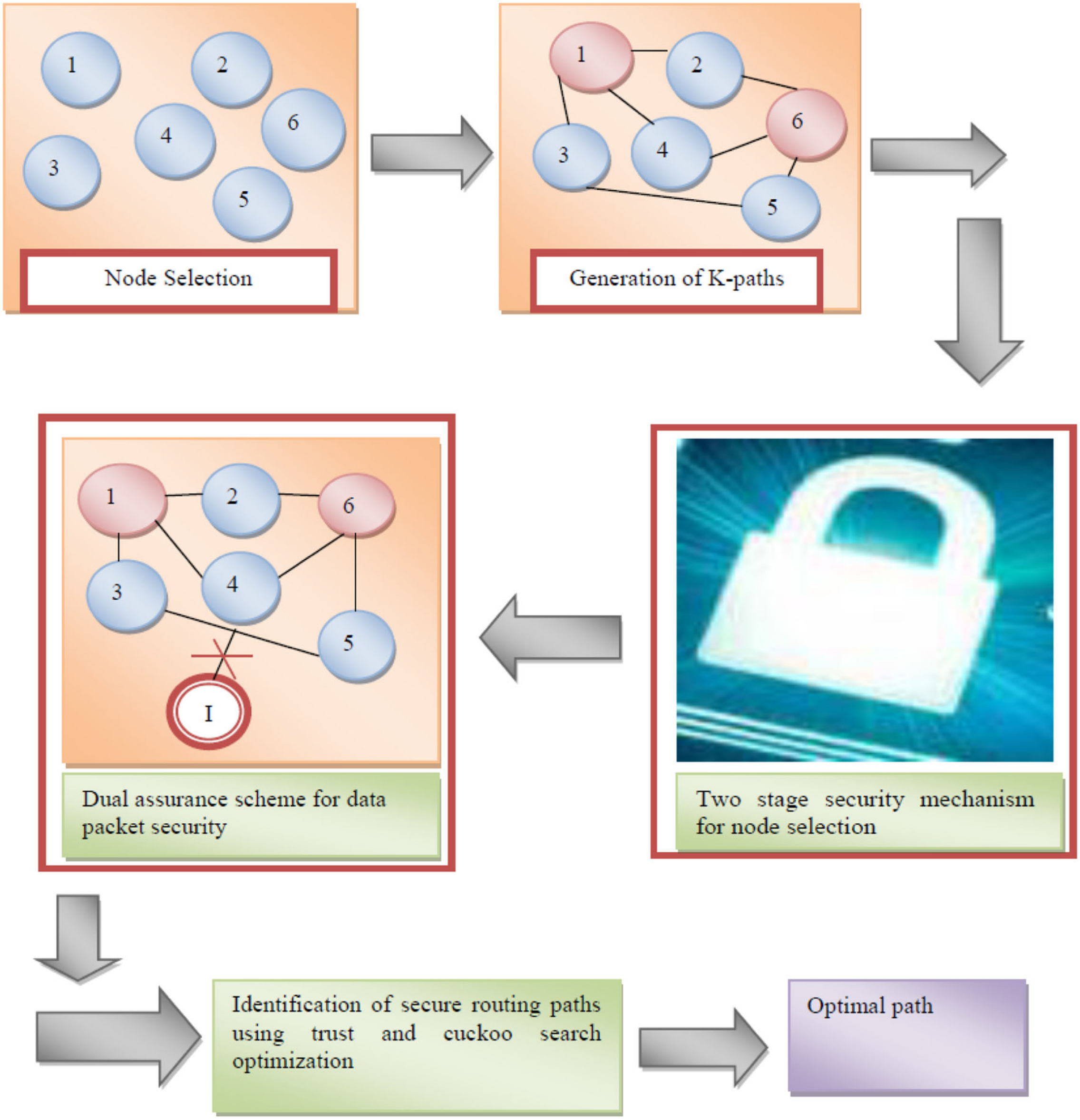

1
2
3
4
5
6
Node Selection
Generation of K-paths
Two stage security mechanism for node selection
I
Dual assurance scheme for data packet security
Identification of secure routing paths using trust cuckoo search optimization
Optimal path

Fig. 2 Block diagram of the proposed system

path with the minimum threshold value for data routing. Both of these mechanisms are deeply described in the following sections.

4.2.1 Detection of malicious nodes by detection packet

The possible number of paths is computed from source to destination as mentioned in Sect. 4.1. Therefore, for each path, the DP that contains the information, such as source node, destination node, and path length, is forwarded, as given in the following equation,

$$DP = \{SourceID, DestinationID, Pathlength\} \tag{1}$$

where, DP is the detection packet. Herein, the path length is the number of hops that forward the DP from the source to the destination node. After transmitting the DP to the destination node, each node in the path sends the feedback packet (FP) to the source node, which signifies that the node successfully reached the final node.

$$FP = \{SourceID, DestinationID, Pathlength\} \tag{2}$$

where, $FP$is the feedback packet. According to the Eqs. (1) and (2), the source node compares the FP with the DP. If the particular node is the attacker node, it will make path length == 0, which means that it is the destination node. Otherwise, the source node already has the ID of the destination node. In FP, if the ID in DP is equivalent to the ID of destination node, and the Path length is equivalent to 0, then there is only one node is a genuine node. Otherwise it is attacker node. If such case occurs, the system discards this path to the destination node and thus, both the black hole and the selective forwarding attacks are prevented. The main problem that arises in mobile node is the inadequate battery. Thus, the intruders take this drawback as its benefits and try to manage the nodes as alert until the entire energy is gone and then that condition left to deep snooze. To avoid this type of attacks, the network is deployed by entering the possible number of nodes and the source and destination is selected by the user.

4.2.2 Detection of attack nodes by trust

The working of trust mechanism [15] has been discussed in this section. This mechanism depicts the trust systems by the following aspects, such as securing the routing path and addressing the trust based optimum threshold value under several conditions with two folds, i.e., impacting the performance of trust system, and influencing the trust factors based on the threshold value. In this case, the threshold value is calculated for each path with the minimum threshold value that considers the most secure path for data routing. Therefore, each sensor node achieves a trust node estimation to avoid the black hole, and selective forwarding attacks during the routing of detection, and data packets. While node N_1 attains a routing for the node N_2 at the given duration u_i, then the identified data are effectively routed, and if the detection node is successfully routed from $N_1 to N_2$, then considered the trust node as $\Delta_{N_1}^{N_2}(u_i)$, otherwise, consider the trust node as $\wedge_{N_1}^{N_2}(u_i)$. Therefore, examining that N_1 has y transmissions with N_2 during u, the value of detection can be represented as follows,

$$\left\{ \Delta_{N_1}^{N_2}(u_1)/\wedge_{N_1}^{N_2}(u_1), \Delta_{N_1}^{N_2}(u_2)/\wedge_{N_1}^{N_2}(u_2), \ldots \Delta_{N_1}^{N_2}(u_y)/\wedge_{N_1}^{N_2}(u_y) \right. \tag{3}$$

where, $N_1$and N_2 are the nodes. According to that, each node has its trust value depending on the threshold value, during the given duration$u$, and the trust considered for N_1 to $N_2$is calculated using Eq. (4),

$$NodeTrust = \begin{cases} M_{N_1}^{N_2} = \sum_{i=1}^{y} \{\Delta_{N_1}^{N2}(u_i)/\wedge_{N_1}^{N_2}(u_i).(g_i/y)\}, \ldots, y \neq 0 \\ 0, \ldots, y = 0 \end{cases} \tag{4}$$

After estimating the trust values for each node, the distance from the source to the destination node is calculated. For each sensor node, the trust-based threshold value is computed with the following Eq. (5) as,

$$TrustThreshold_{Node} = \frac{NodeTrust}{Dis\tan ce} \tag{5}$$

The threshold values for the node can be calculated by dividing the values of trust with distance. Once the trust based threshold values have been computed for the sensor node, then the threshold value is calculated for each path in the node using Eq. (6),

$$TrustThreshold_{Path} = \sum_{fornodeoton} TrustThreshold_{node} \tag{6}$$

Therefore, this equation expresses the summation of the entire node with the threshold value in each path. Finally, the computed path with the minimum threshold value is considered as the most trusted and secured path for data routing.

4.3 Dual assurance scheme for data packet security

This section provides the detailed explanation of dual assurance scheme for data packet security. Here, the scheme is divided into two levels, such as selective forwarding- based packet validation, and ECC-based packet security. The first level depicts how the network identifies the selective forwarding attacks and detects the malicious node. The second level indicates how it provides the secure routing path for data packets.

4.3.1 Selective forwarding-based packet validation

The main aim is to plan a scheme that recognizes the selective forwarding attacks and discovers the malicious nodes. If a malicious node is recognized, the routing protocol prohibits the suspect node from the routing paths, i.e., after route selection, the packet information is sent through this path.

$$PI = \{Type\ of\ Data,\ Size\ of\ Data\} \tag{7}$$

Herein, PI is the Packet Information, including a type of data, and Size of data. i.e., when a node receives the data packet, it verifies the data with PI. If the type of data is not matched, it is found that the data attack occurs on its previous node. In this case, the sensor node drops the packet and forwards the remaining packets to the next node. In selective forwarding attack, the size of data is not matched with the type of data in the data packet. Therefore, the node recovers this type of data from the attacker node. Hence, the packet loss ratios are minimized.

4.3.2 ECC-based packet security

When any data is forwarded from one location to another location on the network, the protocol separates the data file into the small-sizes for efficient routing. Every packet is individually numbered and contains the address of destination node in the network. The individual packets can be forwarded from various routes through the network. When the entire packets are arrived, the packets are reconstructed into the normal file. Meantime, if there is any intruder in the node, the packet loss occurs. Therefore, to avoid this, the network system provides the security mechanism to send the packet without any data loss. The security mechanism secures the data from the fraud alert. To protect the information, the system makes use of ECC algorithm. By using this algorithm, data is encrypted before actual routing. After encryption, original data is protected from unauthorized entities. SHA-1 Hashing method is used to check the data integrity at the sensor node, as given in the following steps. The data generated at the source node is converted into packets. After that, each packet is encrypted using ECC encryption algorithm. The hash value is created using SHA-1 hashing algorithm, for the generated encrypted packet. Accordingly, the network sends the encrypted packet and its corresponding hash value through the selected trustful routing path. At each receiving node in the path, the hash value is calculated for the received encrypted packet. If new hash values == received hash, then the data is protected, indicating that the node is not affected by an attacker.

4.4 Identification of secure routing paths using trust and Cuckoo search optimization

To effectively transmit the data via the optimal and the secure routing path [21], CS algorithm [22] is utilized. CS algorithm is a meta-heuristic algorithm with the familiar concept, parasitic brood bird. The CS algorithm is used for selecting the optimal secure path, and also employed for avoiding numerical malicious available in the sensor node. The goal of the CS is to find the better solutions to modify the worst solution in the set of solutions. Accordingly, it expressed that each set of the solution has only one best solution. The algorithm can be developed to find more difficult cases in which each set of solutions has multiple solutions. The CS algorithm deals with the problem of multi-condition optimization that discards the black hole, and selective forwarding attack from the node. Therefore, it is trouble-free to implement the optimization problems. The goal of CS is to speed up the convergence rate with its single parameter value.

4.4.1 Solution encoding

This section describes the solution representation, describing how the optimal path is selected from the k paths between the source node and the destination node. Therefore, the solution can be represented as a vector, given as, $k = \{1, \ldots, k_n\}$where, $k_n$is the total number of solutions or the paths, generated at random. Hence, the size of the solution is represented as $1 \times k_n$. The optimal path from the k generated path can be obtained using CS algorithm based on the fitness function.

4.4.2 Fitness calculation

Herein, the fitness value can be calculated by considering the entire threshold path in the network, whereas, the trustable routing path is selected for forwarding the data packets. Therefore, by estimating the threshold path, and threshold node using Eq. (8), the fitness value can be obtained.

$$Fitness = \sum_{for\ all\ path\ considered} TrustThreshold_{path} \tag{8}$$

4.4.3 Algorithmic description

In this section, the following steps describe the CS algorithm, which is employed to find the best optimal solution for the given data.

Generation of initial population The first step of CS optimization depicts that each of the time instants; the algorithm produces one solution from the random set of solution. This concept can be shown by the following ways such as, each egg and a cuckoo egg represents a solution and a new solution in a nest that depicts a set of solutions. Therefore, the new solutions can be represented in vector form is given as

$$Y = \{Y_1, \ldots, Y_p\} \tag{9}$$

where, $p$is the population size. $Y$is the new solution.

Evaluate its fitness function Once the population is initialized, the fitness value of each solution can be calculated by the fitness function to attain the best optimal solution. The fitness of the solution is estimated using Eq. (8). Then, compare the fitness of the new solution with the fitness of solution in the previous iteration.

Replace the worst solution If the fitness of the new solution is better than that of the previous, replace the solution with the new solution. When the fitness value of the new solution is lower than or similar to the fitness value of the existing solution, then it remains unchanged. Else if the fitness value of the new solution is higher than the randomly selected set of the solution, the host solution terminates the condition. The generation of new solutions follows Levy flight [23], as represented in the following Eq. (10).

$$Y_p^{(l+1)} = Y_p^{(l)} + a \oplus \text{Levy (b)} \tag{10}$$

where, $a > 0$ is the step size that could be associated with the extent of the problem of interests. In most of the cases, it employs $a = 1$. The product $\oplus$ represents exclusive OR operations. Equation (10) is the theoretical equation for random walk function. Thereby, the Levy flight presents a random walk, when the length of the random step is strained from the Levy distribution,

$$Levy \ \sim v \ = \ l^{-b}, (1 < b \leq 3) \tag{11}$$

The number of the possible set of solutions is predetermined, and the host solution identifies that the solution is an unknown solution with its probability $q_m \ \in \ \ [0, 1]$. Then, the host solution decides whether to terminate the worst solution or discard the set of solutions to construct the new set of the solution. This can be done to eliminate the problem of local optimization. If the condition is not satisfied, the best set of the solutions with the high quality of solutions will transmit to the next generation using the Levy's Flight to achieve the suitable results for the optimization problem. For ease, the hypothesis that can be estimated by the fraction q_m of the j set of solutions are changed by a new set of solutions with new randomly selected solutions.

Termination If all the conditions are satisfied, then terminate the entire process and determine the best solution for the given solution. Otherwise, iterate all the stages until it becomes satisfied. Thereby, it finds the best optimal solution for the randomly selected solutions.

5 Function of proposed secure routing path

An overview of system flow, which is composed of two-stage mechanism, dual assurance scheme for data packet security, and identification of secure routing path using trust, and cuckoo search optimization, is shown in Fig. 3. The main aim of this system flow is to maximize the network lifespan. The lifetime of the network is a significant metrics for WSNs, and also intended to balance the energy consumption for security purposes.

An overview of system flow, which is composed of two-stage mechanism, and dual assurance scheme for data packet security, and identification of secure routing path using trust, and CS algorithm, is shown in Fig. 3. The main aim of this system flow is to maximize the network lifespan. The lifetime of the network is a significant metric for WSNs, to balance the energy consumption for security purposes.

Network deployment The network is deployed with the help of sensor nodes and connecting edges to handle the routing algorithm effectively. It is denoted as, $Network = \{N, E\}$ where, the network is the number of nodes (N) and number of edges (E). Every node and edges have a unique ID in WSN.

Selection of source and destination nodes After deploying the network, use the idea of choosing source node, and the destination node with the corresponding IDs.

k-path generation Then, generate the k path routing scheme, which is used for finding the shortest and secure routing path in a network using two-stage security mechanisms namely, detection of attack node by DP, and trust to prevent from the malicious node.

Trusted path selection Select the trusted paths that are based on the minimal threshold value. The dual assurance scheme is divided into two types, such as selective forwarding based packet validation, and ECC based packet security, which is used to detect and prevent the malicious node, and transmit the secure data packets.

Finding multi-paths Once the trust is assured, find the possible number of paths from the source node to the destination node.

Secure path finding Then, identify the secure routing paths from the estimated multiple paths using trust and CS algorithm, which is used for finding better routing path for the security. Therefore, if the trusted path is adequate, then send the data packet through the trusted path, otherwise select other trusted paths that are available in the network. If the packet size is greater than the expected size, then reject the sensor node, and forward the data straightforwardly from the previous node to the next node. Otherwise directly forward the data and terminates the condition. After forwarding the data, if the previous node is not in the range of next node, find the common neighbor node, and send the data. Else, send the data to the node and terminate the condition. Finally, it achieves the better routing path with given mechanism.

Termination If the packet size is greater than the expected size at the sensor node, reject the node and forward the data from the previous node to next neighbor node. If not, send the data until the condition for stop reaches. If the previous neighbor node is not in the range of next node besides discarding the node, select the common neighboring node and forward the packet. Otherwise, forward the data and terminate the condition.

6 Results and discussion

This section describes the experimental results of the proposed trustable secure routing path in WSN based on two-stage security mechanism, and dual assurance scheme, together with trust and CS algorithm for the identification of secure routing path.

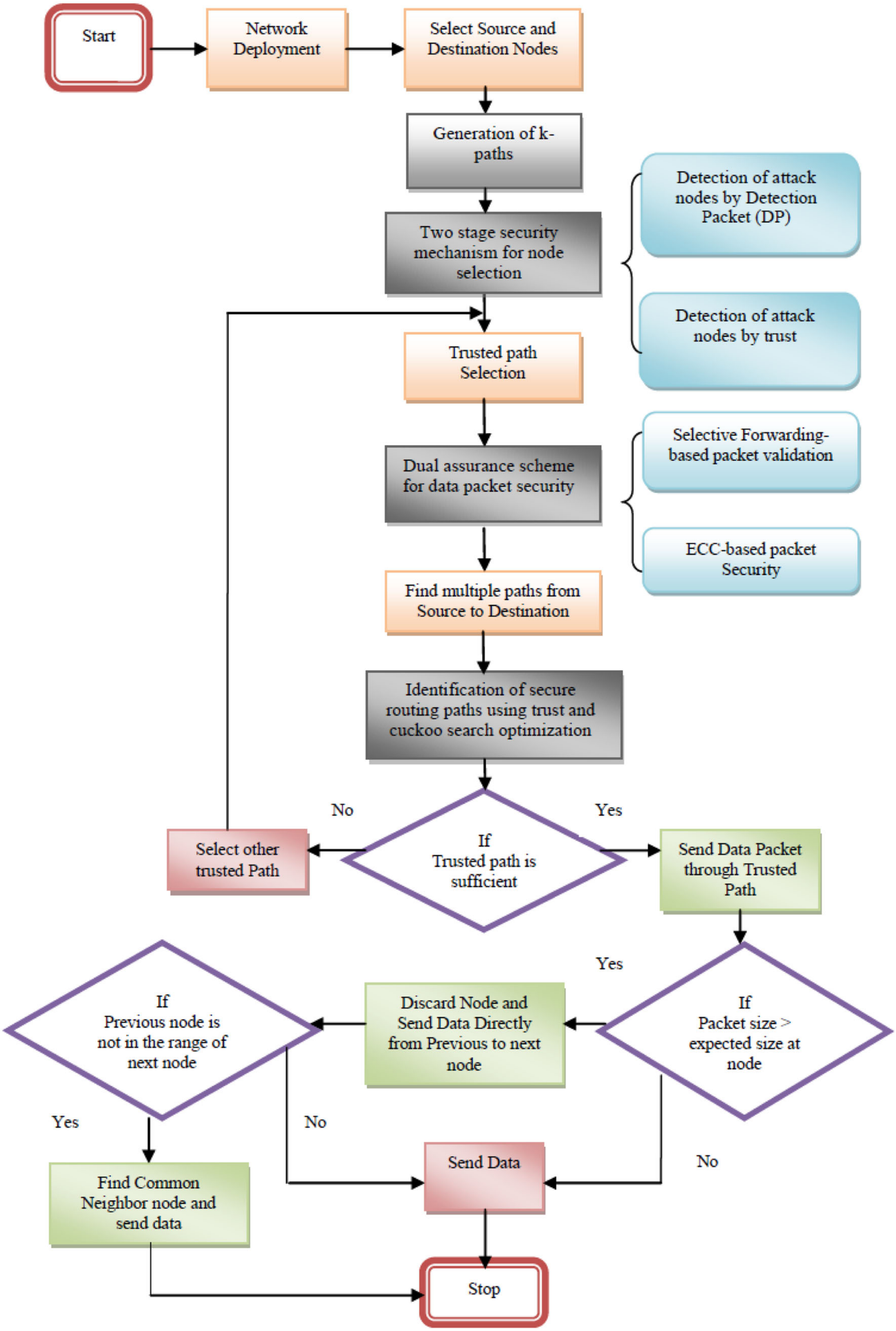

Start
Network Deployment
Select Source and Destination Nodes
Generation of k-paths
Two stage security mechanism for node selection
Detection of attack nodes by Detection Packet (DP)
Detection of attack nodes by trust
Trusted path Selection
Dual assurance scheme for data packet security
Selective Forwarding-based packet validation
ECC-based packet Security
Find multiple paths from Source to Destination
Identification of secure routing paths using trust and cuckoo search optimization
No
Yes
If Trusted path is sufficient
Select other trusted Path
Send Data Packet through Trusted Path
Yes
If Packet size > expected size at node
Discard Node and Send Data Directly from Previous to next node
If Previous node is not in the range of next node
Yes
No
No
Find Common Neighbor node and send data
Send Data
Stop

Fig. 3 System flow

Table 1 Basic simulation parameters

Simulation parameters	Values
Comparative methods	SFD, E2TRP, Active Trust
Simulation area	100 m × 100 m
Number of nodes available in the network	50–100
Initial energy level	1 J
Population size	10
Energy transmitter	0.454 J
Energy receiver	0.25 J
Mobility speed	1 m/s
Simulation time	1800 s

6.1 Experimental setup

In this section, the simulation setup is explained, and then, the results are presented. Accordingly, the system is built using Java framework (version JDK 6) on Windows platform. The NetBeans (version 6.9) is used as a development tool. The system used Jung tool for creating the network. The system doesn't require any specific hardware to run, and some standard machine has the capability to run the application. Then, the number of nodes is varied during the experimentation. Herein, the proposed scheme is predicted through the simulation parameters. The basic parameter values employed in the simulations are showed in Table 1.

6.2 Performance measures

In this section, the results are compared with existing approaches, such as, SFD, E2TRP, and Active trust, in terms of energy consumption, packet delivery ratio, throughput, and latency.

6.2.1 Energy consumption

Energy consumption of the sensing device must be minimized, and the sensor nodes must be energy efficient, as the limited energy resource determines their lifetime efficiently. Energy consumption formula for sending c bit message to a distance d is given below,

$$E_{Tx}(c,d) = E_{elec} \times c + \in_{amp} + c \times d^2 \tag{12}$$

where, E_{Tx} defines the energy loss, while sending the data, E_{elec} represents the loss of energy transmitter, $\in_{amp}$ is the amplifier energy, and d is the distance. Energy consumption formula for receiving a K-bit message is given by,

$$E_{Rx}(c) = E_{elec} \times c \tag{13}$$

where, E_{Rx} defines the energy loss while receiving the data, c is constant. Therefore, the energy consumption is given as,

$$E_{Tx}(c,d) = E_{Rx}(c) + \in_{amp} + c \times d^2 \tag{14}$$

Equation (14), supports to minimize the energy consumption in the sensor network, prolonging the lifetime of the network.

6.2.2 Packet delivery ratio (PDR)

The PDR is predicated on the basis of received and generated packets as recorded within the trace file. In general, PDR is outlined, because the quantitative relation between the received packets by the destination and the generated packets by the supply. The formula for PDR is estimated by dividing the total number of packets at destination, with total number of packets generated at source node, and also multiply the generated result with the percent to obtain suitable results is shown as below,

$$PDR = \frac{t_d}{t_s} \times 100 \tag{15}$$

where, PDR is the packet delivery ratio, t_d is the total number of packets at the destination, and t_s is the total number of packets generated at the source code.

6.2.3 Throughput

Throughput defines the number of data transmitted from one location to another or processed within the given time. It can be estimated by using the following Eq. (16),

$$Throughput = \frac{t_p}{t_t} \times 100 \tag{16}$$

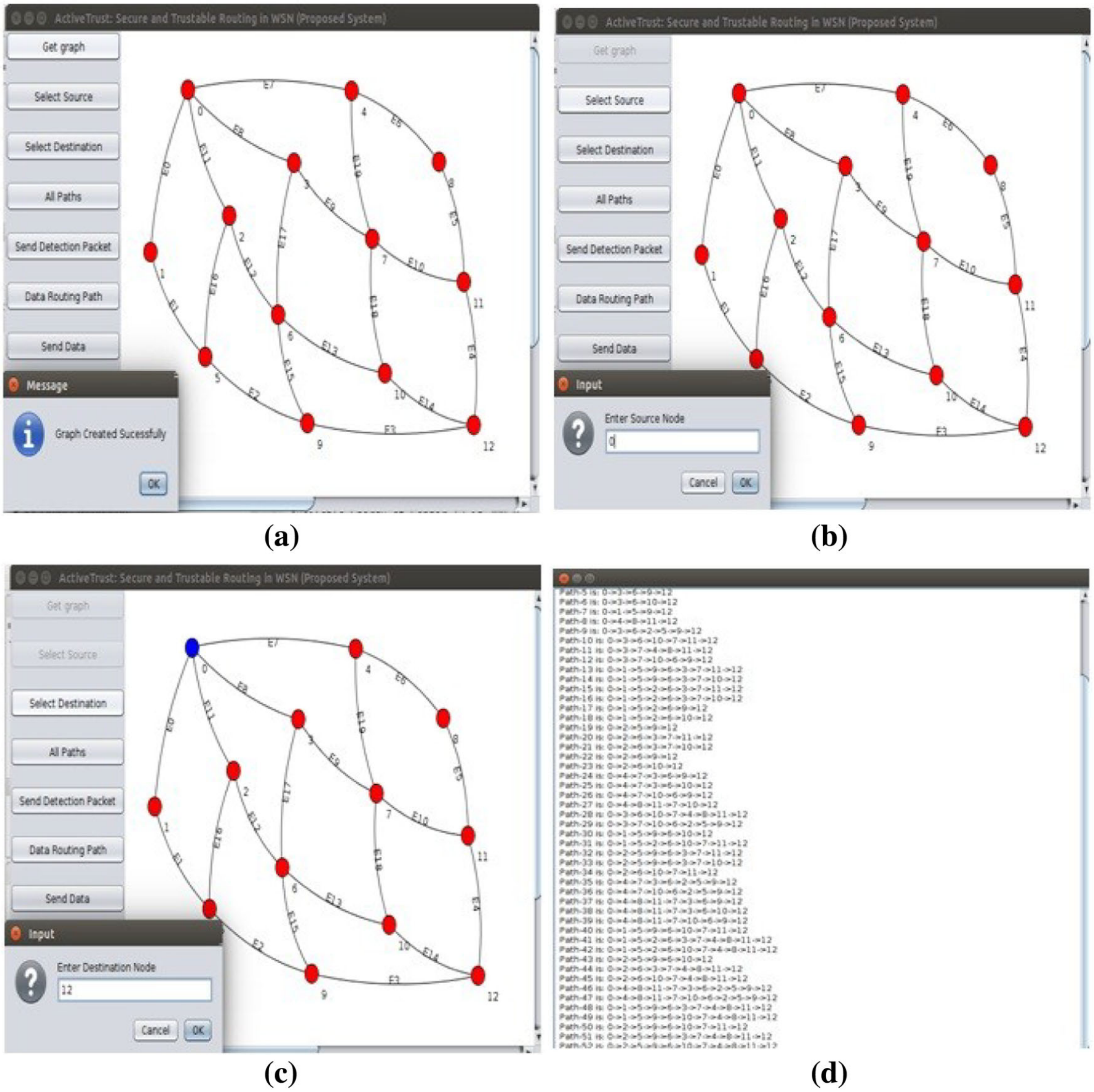
where, t_p is the total number of packets delivered at the destination, and t_t is the total simulation time.

6.2.4 Latency

Latency depicts the time duration among the response and stimulation or a delay of time between the source and the target of the physical modification in the system being examined, which can be estimated using the given Eq. (17) to avoid the energy loss,

$$Latency = t_d \times s_t \tag{17}$$

where, t_d is the time of packets received at the destination, and s_t is the time of packets generated at the source node.



(a)

Graph Created Sucessfully

(b)

Enter Source Node: 0

(c)

Enter Destination Node: 12

(d)

```
Path-5 is: 0->3->6->9->12
Path-6 is: 0->3->6->10->12
Path-7 is: 0->1->5->9->12
Path-8 is: 0->4->8->11->12
Path-9 is: 0->3->6->2->5->9->12
Path-10 is: 0->3->6->10->7->11->12
Path-11 is: 0->3->7->4->8->11->12
Path-12 is: 0->3->7->10->6->9->12
Path-13 is: 0->1->5->9->6->3->7->11->12
Path-14 is: 0->1->5->9->6->3->7->10->12
Path-15 is: 0->1->5->2->6->3->7->11->12
Path-16 is: 0->1->5->2->6->3->7->10->12
Path-17 is: 0->1->5->2->6->9->12
Path-18 is: 0->1->5->2->6->10->12
Path-19 is: 0->2->5->9->12
Path-20 is: 0->2->6->3->7->11->12
Path-21 is: 0->2->6->3->7->10->12
Path-22 is: 0->2->6->9->12
Path-23 is: 0->2->6->10->12
Path-24 is: 0->4->7->3->6->9->12
Path-25 is: 0->4->7->3->6->10->12
Path-26 is: 0->4->7->10->6->9->12
Path-27 is: 0->4->8->11->7->10->12
Path-28 is: 0->3->6->10->7->4->8->11->12
Path-29 is: 0->3->7->10->6->2->5->9->12
Path-30 is: 0->1->5->9->6->10->12
Path-31 is: 0->1->5->2->6->10->7->11->12
Path-32 is: 0->2->5->9->6->3->7->11->12
Path-33 is: 0->2->5->9->6->3->7->10->12
Path-34 is: 0->2->6->10->7->11->12
Path-35 is: 0->4->7->3->6->2->5->9->12
Path-36 is: 0->4->7->10->6->2->5->9->12
Path-37 is: 0->4->8->11->7->3->6->9->12
Path-38 is: 0->4->8->11->7->3->6->10->12
Path-39 is: 0->4->8->11->7->10->6->9->12
Path-40 is: 0->1->5->9->6->10->7->11->12
Path-41 is: 0->1->5->2->6->3->7->4->8->11->12
Path-42 is: 0->1->5->2->6->10->7->4->8->11->12
Path-43 is: 0->2->5->9->6->10->12
Path-44 is: 0->2->6->3->7->4->8->11->12
Path-45 is: 0->2->6->10->7->4->8->11->12
Path-46 is: 0->4->8->11->7->3->6->2->5->9->12
Path-47 is: 0->4->8->11->7->10->6->2->5->9->12
Path-48 is: 0->1->5->9->6->3->7->4->8->11->12
Path-49 is: 0->1->5->9->6->10->7->4->8->11->12
Path-50 is: 0->2->5->9->6->10->7->11->12
Path-51 is: 0->2->5->9->6->3->7->4->8->11->12
Path-52 is: 0->2->5->9->6->10->7->4->8->11->12
```

Fig. 4 Experimental results. **a** Network deployment, **b** source node selection, **c** destination node, **d** all path computations

6.3 Experimental results

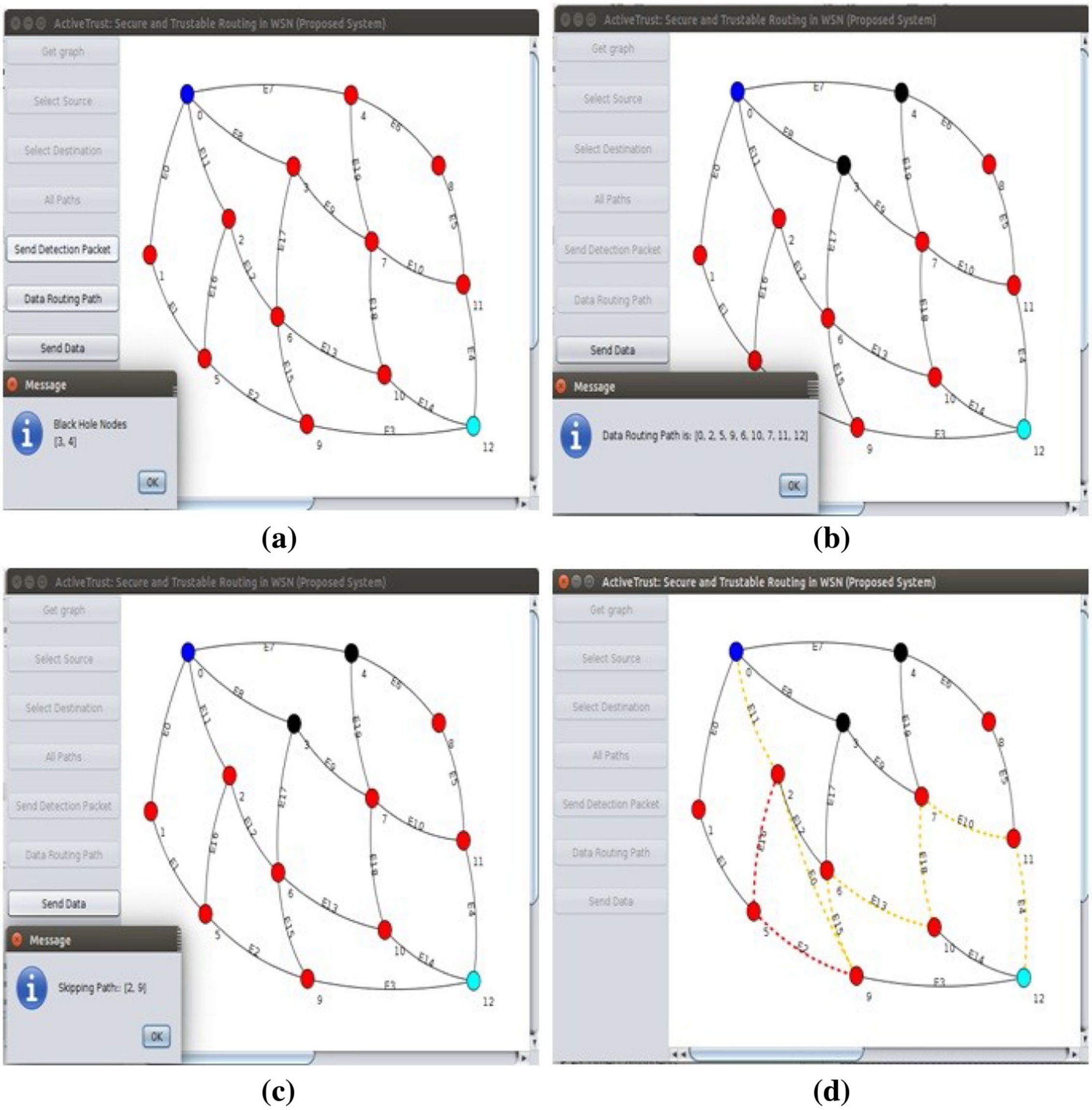
In this section, the experimental results of the proposed system are shown in Figs. 4 and 5. Figure 4a represents the network deployment, where the sensor nodes are marked red. Figure 4b and c show the selection of source node, and the destination node in the network, indicating 0 as the source and 12 as the destination node. Figure 4d depicts the computation of all the paths, which are generated from the process of node selection.

Figure 5 represents the detection of attack nodes in the network. Figure 5a shows the results of both black hole, and selective forwarding attacks, detected by the proposed system. Figure 5b depicts the secure routing path selection performed and Fig. 5c represents the skipped path. Figure 5d shows the path through which the data is forwarded.

6.4 Comparative analysis

Here, the comparative analysis based on the comparison of existing techniques, such as SFD (selective forwarding detection), E2TRP (energy efficient and trustable routing protocol), Active trust with the proposed approach is explained, based on the performance evaluation metrics.

In Fig. 6a, the energy consumption for different size of the network in proposed system and the existing systems compared is represented. Energy consumption is minimum in the proposed system because the black hole attacker is detected before actual data routing and the data is recovered



Black Hole Nodes
[3, 4]

Data Routing Path is: [0, 2, 5, 9, 6, 10, 7, 11, 12]

Skipping Path:: [2, 9]

Fig. 5 Experimental results. **a** black hole and selective forwarding attack detection, **b** secure routing path selection, **c** skipped path, **d** send data

after a packet drop. When the network size is 8, the energy consumption for SFD [4], E2TRP [16], and Active Trust [15] is 145, 119, and 100, while the energy consumption for the proposed system is 98. When compared with existing system the energy consumption is low in the proposed system, and produced better results with high energy efficiency.

Figure 6b shows the latency comparison for different size of the network in proposed system and existing system. As shown in the figure, the latency for the proposed system is in minimum than the other techniques. It is an expression of how much time it takes for a packet of data to get from one designated point to another. When the network size is 8, then the latency for SFD, E2TRP, and Active Trust are 41,500 ms, 35,900 ms, and, 27,000 ms, while the latency for proposed system is just 16,000 ms.

Figure 6c represents the length of routing paths for different sizes of the network in the proposed system and the existing systems. In the proposed system, length of routing path is minimized, so that the energy consumption gets reduced during data sending. Path length is nothing but the number of hopes from source to destination in particular path. If the network size is 8, the path length is 7 for SFD, 5 for E2TRP, 6 for the Active system, and 4 for the proposed method. Thus, the routing path length is same for active trust and proposed method.

Figure 6d shows the network lifetime comparison of the existing and proposed system in the heterogeneous environ-

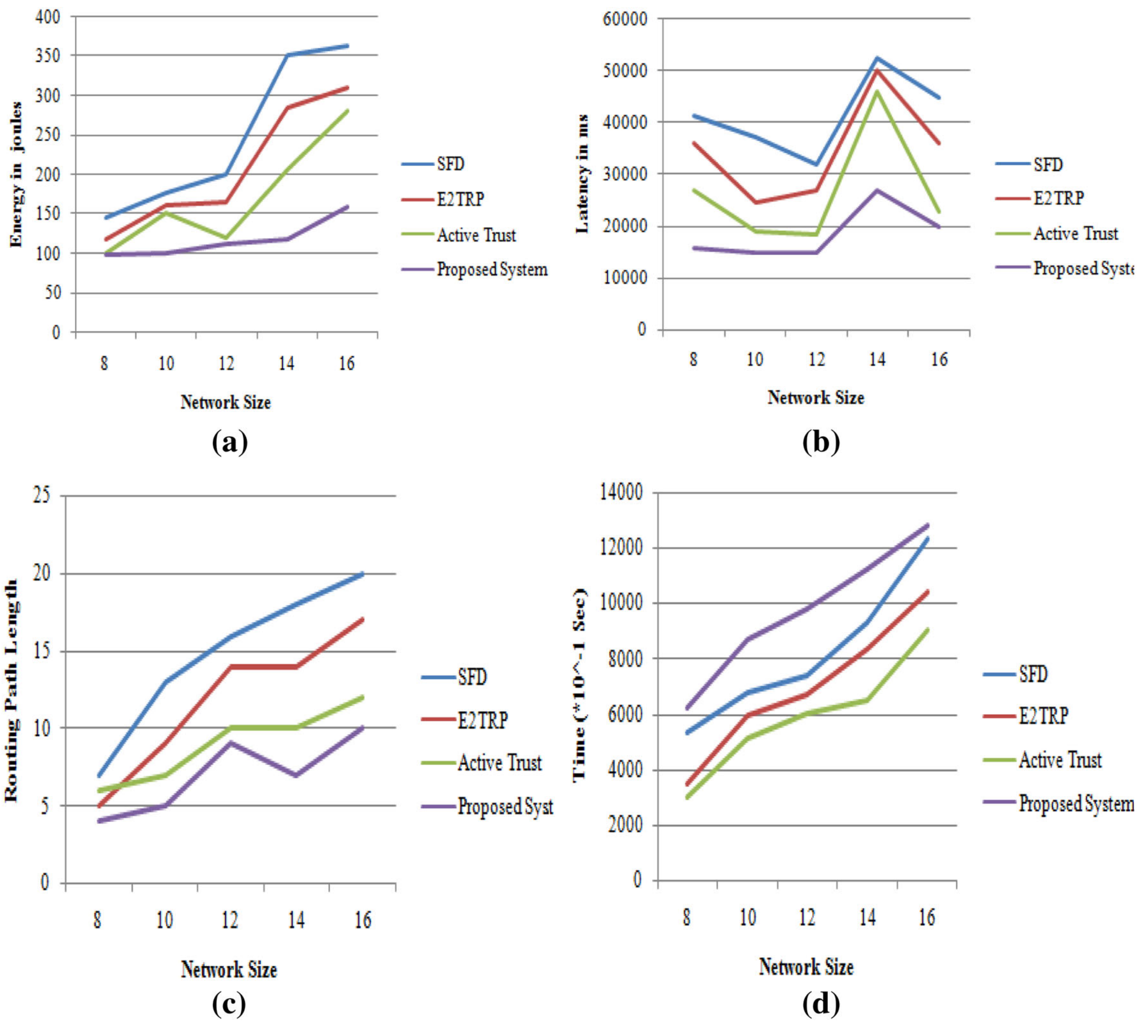


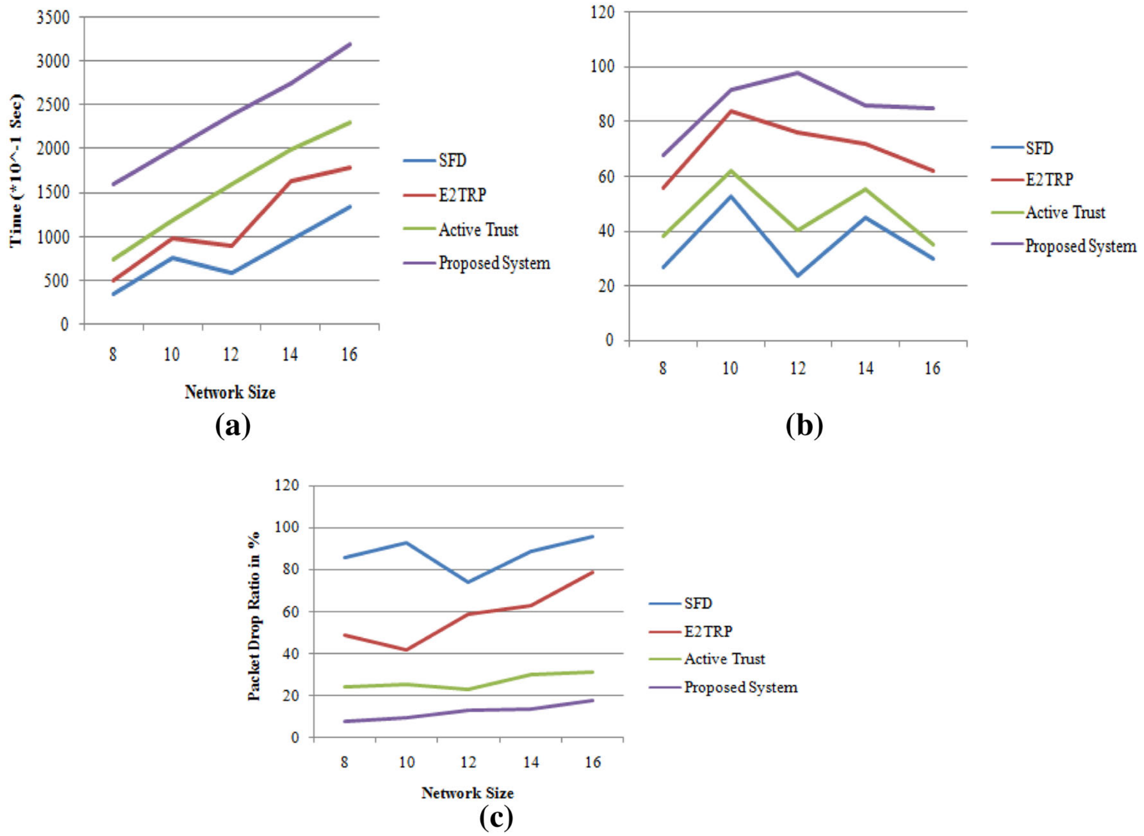
Fig. 6 Analysis based on **a** energy consumption, **b** latency, **c** path length, **d** network lifetime in a heterogeneous network

ment. The network lifetime increases in the proposed system because it removes both black hole, and selective forwarding attack before actual data routing. When the network size is 8, the time at which the system remains alive for existing approaches, such as SFD, E2TRP, and, active trust is 535, 346, and, 300 s, but in the proposed system, it is 620 s.

Figure 7a shows the analysis of energy efficiency of the existing and proposed system in the homogeneous environment. For a homogeneous network, the energy is high in the proposed system, i.e., when the network size is 8, the time at which the system remains alive for the existing approaches, SFD, E2TRP, and, Active trust, is 34.8, 50, and, 75 s, but in the proposed system, it has 160 s.

Figure 7b represents the throughput analysis of the comparative techniques. When the network size is 8, the throughput ratio in the SFD, E2TRP, and, Active trust, is 27, 56.23, and 38, but, in the proposed system, it is 68. Comparing the throughput values with that of the existing techniques, it is low for the proposed method. The PDR in the proposed system is in minimal than the existing systems compared, as shown in Fig. 7c. The PDR analysis shows that, when the network size is 8, 10, 12, 14, and 16, the PDR of the existing approaches is much higher. When the existing values are compared with that of the proposed method, there is a drop for packet drop ratio, i.e., 86.23, 49.43, 25.5, and 8 for SFD, E2TRP, Active trust and, proposed system. The PDR of the proposed system is much lower than the SFD, E2TRP, and Active trust, and hence, it produced good results with high energy efficiency in the network, as shown in Fig. 7c.

Table 2 depicts the comparative analysis of existing and proposed system on the basis of network size, energy consumption, latency, throughput, and PDR. The performance of the system is tested with the network size 16. For the network size of 16, the proposed method has the energy consumption of 160 while the existing methods, such as SFD, E2TRP, and Active Trust have the energy consumption of 364, 310, and 280 respectively. The proposed method has the latency of 20,000 on the other hand, the existing methods, such as SFD,



(a)

(b)

(c)

Fig. 7 Analysis based on **a** network lifetime, **b** throughput comparison, **c** packet drop ratio

Table 2 Comparative discussion

Methods	Network size	Energy consumption	Latency	Throughput	Packet drop ratio
SFD	16	364	45,000	30	96.23
E2TRP	16	310	35,820	62.02	24.3
Active Trust	16	280	23,000	35	24.3
Proposed system	16	160	20,000	85	18

E2TRP, and Active Trust have the latency of 45,000, 35,820, and 23,000 respectively. The throughput of the proposed method is 85, and the throughput of the existing methods, such as SFD, E2TRP, and Active Trust is 30, 62.02, and 35. The existing methods, such as SFD, E2TRP, and Active Trust have the packet drop of 96.23, 24.3, and 24.3. On the other hand, the proposed method has the packet drop of 18. From the Table 2, it can be concluded that the proposed method has the minimum energy consumption, latency, packet drop ratio and the maximum throughput than the existing methods.

7 Conclusion

This paper focused on detecting and preventing the black hole and selective forwarding attacks in the WSN. To detect, and prevent such type of attacks, this paper proposed two schemes, named as a two-stage security mechanism, and dual assurance scheme, for transmitting the data packet securely in the network. Moreover, this paper identified the untrusted path and provided secure routing paths using trust and CS algorithm, with active trust scheme in the clustered based sensor networks. This proposed scheme can quickly identify malicious nodes in the network with high energy efficiency. Finally, the avoidance of black holes and selective forwarding attack is done by the proposed secure routing scheme, which maximizes the ratio of packet delivery. The proposed system provides various features that are helpful in the real-time applications of WSN. For instance, it has maximal accuracy, minimal energy loss, ease of use, privacy, and reliability. These are very essential as they easily analysis to use in risk management, and assessment of the system as well as providing data packet, and secure routing path. Therefore, the experimental result shows that the proposed system is better than existing work in terms of energy consumption, latency, path length, Network lifetime in the heterogeneous and homogeneous network, throughput, and packet drop ratio. From the results, it is observed that the proposed system yields better performance with 20,000 ms latency power, and 85% throughput with maximum network size.

References

1. Kellner, A., Alfandi, O., Alfandi, O., Hogrefe, D.: A survey on measures for secure routing in wireless sensor networks. Proc. Int. J. Sens. Netw. Data Commun. **1**, 17 (2012)
2. Dewal, P., Narula, G.S., Jain, V.: Detection and prevention of black hole attacks in cluster based wireless sensor networks. In: Proceedings in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp. 3399–3403 (2016)
3. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. In: Proceedings in the First IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA, pp. 113–127 (2003)
4. Alajmi, N.M., Elleithy, K.: A new approach for detecting and monitoring of selective forwarding attack in wireless sensor networks. In: Proceedings in 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, pp. 1–6 (2016)
5. Pavan Kumar Guptha, Y., Madhu, M.: Improving security and detecting black hole attack in wireless sensor network. Int. J. Prof. Eng. Stud. **8**(5), 260–265 (2017)
6. Momani, M., Challa, S.: Survey of trust models in different network domains. IJASUC **1**(3), 1–19 (2010)
7. Sathishkumar, R., Ramesh, C.: A modified method for preventing black-hole attack in mobile ad hoc networks. J. Eng. Appl. Sci. **11**(2), 182–191 (2016)
8. Jain, A.: Trust based routing mechanism against black hole attack using AOMDV-IDS system in MANET format. Int. J. Emerg. Technol. Adv. Eng. **2**(4), 653–661 (2012)
9. Chan, H., Perrg, A.: Security and privacy in sensor networks. Computer **36**(10), 103–105 (2003)
10. Zhu, T., Zhong, Z., He, T., Zhang, Z.-L.: Energy synchronized computing for sustainable sensor networks. Ad Hoc Netw. **11**(4), 1392–1404 (2013)
11. Khan, W.Z., Yang, X., Aalsalem, M.Y., Arshada, Q.: The selective forwarding attack in sensor networks: detections and countermeasures. Int. J. Wirel. Microw. Technol. **2**, 33–44 (2012)
12. Tiwari, M., Arya, K.V., Choudhari, R., Choudhary, K.S.: Designing intrusion detection to detect black hole and selective forwarding attack in WSN based on local information. In: Proceedings in Fourth International IEEE Conference on Computer Sciences and Convergence Information Technology, Seoul, South Korea, pp. 824–828 (2009)
13. Bin, T., Xian, Y.Y., Dong, L., Qi, L., Xin, Y.: A security framework for wireless sensor networks. J. Chin. Univ. Posts Telecommun. **17**(Supplement 2), 118–122 (2010)
14. Latha, D., Palanivel, K.: Secure routing through trusted nodes in wireless sensor networks a survey. Proc. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **3**(11), 3792–3799 (2014)
15. Liu, Y., Dong, M., Ota, K., Liu, A.: Active Trust: secure and trustable routing in wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **11**(9), 2013–2027 (2016)
16. Das, S., Barani, S., Wagh, S., Sonavane, S.S.: Energy efficient and trustable routing protocol for wireless sensor networks based on genetic algorithm (E2TRP). In: Proceedings in IEEE International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, India, pp. 154–159 (2016)
17. Sharmila, S., Umamaheswari, G.: Detection of sinkhole attack in wireless sensor networks using message digest algorithms. In: Proceedings in 2011 International Conference on Process Automation, Control and Computing, Coimbatore, India, pp. 1–6 (2011)
18. Geethu P.C., Mohammed, A.R.: Defense mechanism against selective forwarding attack in wire-less sensor networks. In: Proceedings in 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, pp. 1–4 (2013)
19. Motamedi, M., Yazdani, N.: Detection of black hole attack in wireless sensor network using uav. In: Proceedings in 2015 7th Conference on Information and Knowledge Technology (IKT), Urmia, Iran, pp. 1–5 (2015)
20. Kumar, R., Kumar, D.: Multi-objective fractional artificial bee colony algorithm to energy aware routing protocol in wireless sensor network. Wirel. Netw. **22**(5), 1461–1474 (2016)
21. Sanzgiri, K., Dahill, B., Levine, B., Shields, C., Belding-Royer, E.: A secure routing protocol for ad hoc networks. In: Proceedings of 10th IEEE International Conference on Network Protocols, Paris, France (2002)
22. Amir, H.G., Yang, X.-S., Amir, H.A.: Cuckoo search algorithm: a metaheuristic approach to solve structural optimization problems. Eng. Comput. **29**(1), 17–35 (2013)
23. Yang, X.-S., Deb, S.: Cuckoo search via Levy flights. In: Proceedings of the World Congress in Nature & Biologically Inspired Computing, Coimbatore, India, pp. 210–214 (2009)

Deepak C. Mehetre did his B.E. in Computer Science and Engineering from Dr. B.A.M.U University in 2004. He received his M.Tech. in Computer Science and Engineering from VTU University in 2009. He is pursuing his Ph.D. from Sathyabama University, Chennai. He is working as an Associate Professor in K J College of Engineering and Management Research, Pune. His current research interests include Wireless sensor network mobile adhoc networks, vehicular ad-hoc networks, optimization techniques and network security. He has 20 research papers to his credit, published in International/National Journals & conferences. He is fellow member of ISTE, ACM & CSI.

S. Emalda Roslin received her Ph.D. and M.Tech. degrees in Electronic and telecommunication Engineering from Sathyabama University, Chennai, India, in 2015 and 2009 respectively. She is currently an Professor in telecommunication Engineering in Sathyabama University, Chennai, India. Her doctoral research work focused on Wireless sensor Network. Her current research interests include Wireless sensor Network, high- performance computing and vehicular ad-hoc networks. She has 25 research papers to his credit, published in International/National Journals & conferences.

Sanjeev J. Wagh working as Professor in Department of Information Technology at Govt. College of Engineering, Karad. He has completed his B.E. (1996), M.E. (2000) & Ph.D. (2008) in Computer Science & Engineering from Govt. College of Engineering, Pune & Nanded. He was full time Post Doctorate fellow at Center for Tele Infrastructure, Aalborg University, Denmark during 2013–2014. He has also completed MBA from NIBM (2015), Chennai. His research interest areas are Natural Science Computing, Internet technologies & Wireless Sensor networks, Data Sciences & Analytics. He has 71 research papers to his credit, published in International/National Journals & conferences. Currently 5 research scholars are pursuing Ph.D. under his supervision in various Universities. He is fellow member of ISTE, IETE, ACM & CSI. He is co-editor for 4 International Journal in Engineering & Technology.