Secure and Shortest Path Routing Bypassing Attackers in Wireless Sensor Networks

K Pavan Kumar Reddy[a], KasaVikramReddy[b], Dr.K.Kalaiselvi[c]*, Dr.K.DeepaThilak[d]

[a,b,c,d]Department of Computer Science and Engineering, SRM Institute of Science and Technology,
Kattankulathur, Kancheepuram(D.t), Tamil Nadu, India,
[*] Corresponding Author Email ID: mkkalai1981@gmail.com

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: In wireless sensor networks (WSNs), energy constraint of node is the major issue, as the sensor may be deployed in the area where energy backup or quick replacements may not be available. In such cases, preserving the node energy and prolonging the network life time play crucial role in wireless sensor networks. Similarly, sensor nodes are highly vulnerable to attacks, attackers can easily tamper the sensor node and compromise it. Thus to overcome above stated two problems, the proposed work ensures shortest path routing, which ensures network life time of sensor nodes and the trust based routing, which avoids node compromise attacks. The proposed shortest path routing algorithms takes route through multi-hop nodes to corresponding sink. The shortest path based on the geographical routing strategy chooses the nodes nearest to the routing node and sink node. The novel routing framework proposed in this work considered shortest path with trust based routes. The node's energy is considered to taking reliable node on the routing path, which ensure the packet delivery and avoids any node failure due to less energy. The node's trust value is evaluated with three type, which ensure that the paths created are more reliable

Keywords: Wireless Sensor Networks, Sensor Nodes, Trust based routing, shortest path routing, Node reputation, Node compromise attacks.

1. Introduction

Wireless sensor networks (WSNs) are made with huge number of small hardware namely sensor, which collects information from environment such temperature, humidity, moisture, obstacle detection for even more purposes. Sensor nodes has limited power, resources like energy backups, computational capacity and storage capacity. Wireless sensor networks are deployed in many real world applications and the emerging Internet of Thing (IoT) combining sensor nodes to cloud storage are used for smart cities, traffic monitoring and many more. Whereas the applications like animal monitoring in forest, military activity surveillance, tracking, forest fire detection, and in many operational industries. The collected data from the above applications are aggregated and sent to sink node, though multi-hop routing strategies. Most of IoT applications send the information via internet to the storage servers.

Base station or Sink node are the one, which is placed in center of the network to collect the information sensed by the huge number of sensor nodes deployed in different geographical locations in distributed manner. The main objective of wireless sensor networks is to provide services in a distributed manner to cover the most geographical locations with less number of nodes and high coverage with wireless connectivity. But the problem is with node's availability for prolonged time, due to the less power backup and storage capability, these node cannot store large amount of data, it forwards data as when the information is arrived. Thus most of the traditional systems also used sleep and awake methods to save the network lifetime of sensor nodes, the node only wake up when the event is arrived, it forwards the event and goes to sleep mode to save power, whereas these created problem with accurate detection of event.

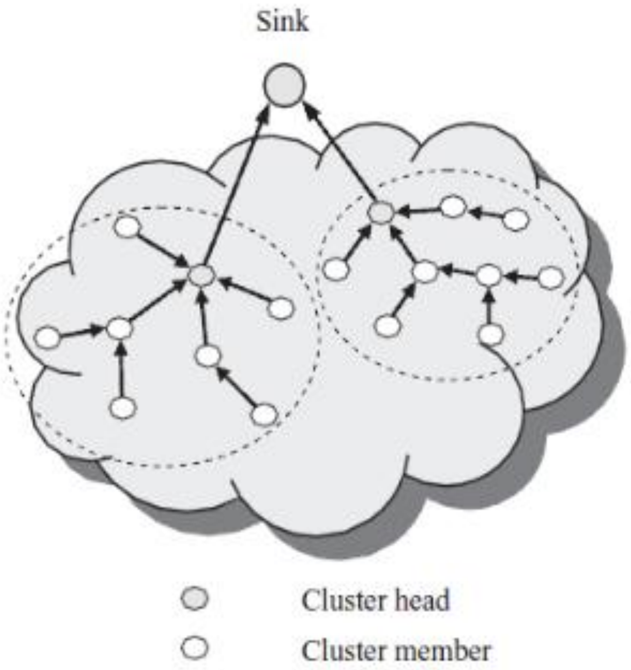


Figure: 1 Overview of Wireless Sensor Network

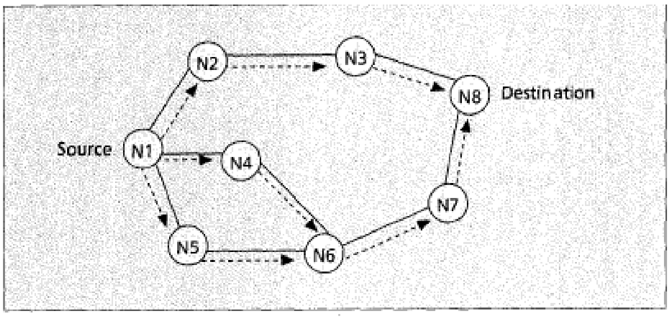
Wireless sensor networks highly prone to many threats including node compromise attacks, black hole attacks, sink hole attacks, and other internal, external attacks. Attackers may compromise sensor nodes by getting nodes identity and keys may corrupt the data packets or even drop the packets without delivering. Routing protocol can be even tampered by attackers, which may give serious threat for the whole network packet delivery. Thus by the neighbor node's reputation values the node behavior can be monitored by the sink.

Delivering the packets through compromised node is highly risk due to the fact that compromised nodes may drop or corrupt the packets. Most of the wireless sensor networks assumes that they are highly reliable and not error prone. To solve this problem, highly effective solutions to be needed to update the compromised node periodically to sink. Thus the routing table can be updated and sent to all neighbor node in network to create a new routing path. Though this process requires an addition transmission cost and considerable energy, the network can be more safe and reliable.

Some of the serious threats for wireless networks are available, among them blackhole is cause major problem in packet delivery.

Blackhole attack is a form of denial of service, in which the attacked node attracts all packets to itself claiming that node is nearest to destination node. Thus the routing all considered are shortest path, most of the node sent packets to blackhole node. Once receiving the packet, it may drop or modify the packets without forwarding to destination. Cooperative black hole is another serious threat, in which all the compromised nodes acts as group and co-operatively denies the services to network. Ad-hoc On-demand Distance Vector (AODV) is widely used routing protocol, which can handle multi-hop routing in wireless networks, creates routes when desired by the source node.

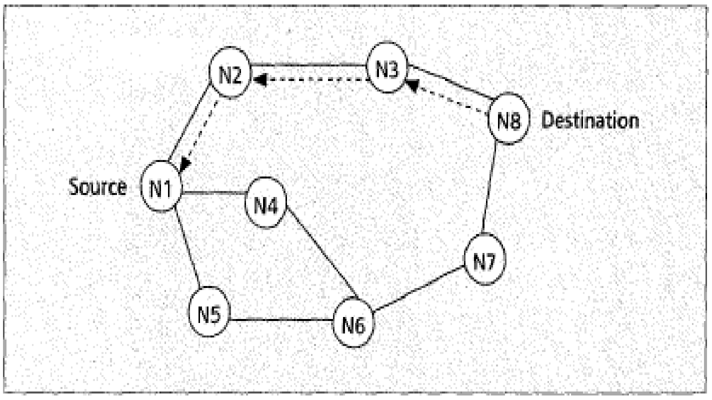
The following figure shows the route request method handled by AODV protocol, when a source node requests a route to destination, the AODV protocol initiates route discovery process, in which multiple requests are sent to sensor nodes available in the network. This protocol broadcasts a route request (RREQ) packet to all sensor nodes in network.



Propagation of RREQ.

Figure: 2 Route Request Process

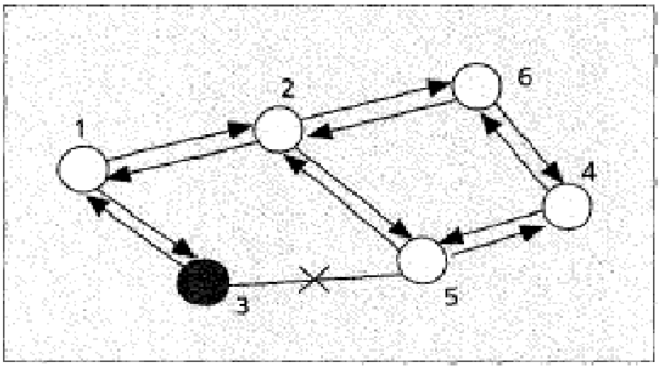
The route request (RREQ) sent till destination is reached through the intermediate nodes, the destination node replies to RREQ, it is called route reply packets RREQ. RREQ is also sent through intermediate nodes to source node. The following figure shows the route reply method in the wireless sensor networks forwarding RREP to source node.



The path of a routing reply.

Figure: 3 Route Reply Process

If intermediate nodes found route then it may reply to RREQ to create a new routes. The blackhole node may claim wrongly that it has routes to destination and sends RREP to source node. Source node hence send packet through the blackhole node, which it can drop or modify. The below figure shows the blackhole node sending wrong information of RREP packets to the source node, which claims it to be normal legitimate node, however it can drop packet while receiving from source node.



The black hole problem.

Figure: 4 Black hole Process

When a node detects a packet delivery it given increment to trust value to the node it has forwarded.The credibility of the node increase as when it transmits a packet to neighbors successfully. This information is broadcast to all nodes in network. Thus the sender node or source node is aware of trust node and energy available node for routing by means of collaborative transmitting of energy and trust information.

Updating or distributing the information is another important issue. Updating function Updates Information energy and trust and key values. The nodes may have neighbors information including NodeID, Trust Value, Energy value, Ipaddress and port number of node. A node can transmit packets through direct trust information and indirect trust information.

Node Reputation

Node reputation = Direct trust + indirect Trust info

Direct information = Increment by 1 for every transactions

Indirect Trust = Increment by 1 for every transactions

Function Trust = Increment by 1 for every transactions

Energy Calculation

Energy value = Decrement energy value by5 when the node transmits packets

Nodes reputation is based on direct, indirect and functional trust provided by monitoring system and updates to all nodes by updating module. Depending on the reputation value, the sensor node for routing will be chosen. If the reputation of node is above zero, then the sensor node is considered and chosen for routing.

The update of information on trust and energy parameters requires additional cost and computation power is also needed. However, once achieved the network can be attack free and more reliable with high lifetime for sensor nodes. The proposed work combine all four criteria trust, security, shortest path and node energy for secure network and prolonged lifetime of network. This are achievable easily in this distributed wireless sensor networks. In our implementation, two clusters with sink node each cluster is considered on deployment.

In the upcoming chapters related works on wireless sensor networks, trust based routing and shortest path routing are discussed. In chapter 3, the proposed methodology and implementation modules, Shortest path algorithm, Trust based algorithm are discussed in detail. In chapter 4, results of our proposed work is discussed. Finally, last chapter studied about Conclusion and further directions further work are discussed.

2. Related Work

In Literature, many existing works were proposed for energy based routing, shortest path routing for wireless sensor network to enhance the network life time. Some of these researches are discussed in this chapter in details for finding the gaps and problem statement for our proposed work.

In existing system, Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol for routing is used requires complete reconstruction of clusters, transmitting packages from the cluster head to the sink node directly is impractical for large WSNs.

In many existing model, only routing is considered, whereas in our proposed work, the reputation of node and compromised nodes are considered for routing.The conventional method in shortest path routing has been studied and their methodologies and limitations are listed in the below table.

Title	Methodology	Issues/Limitations
Reputationbased Intrusion Detection	Intrusion Detection System (IDS) among WSNs	Only reputation of neighbor node considered. if the neighbor node is malicious, attack is possible.
Cluster Heads Model for Secure Data	Double Cluster Heads Model (DCHM) for secure and accurate data fusion in WSNs	Cluster head based collection, which not considered any security of network.
Trajectory Based Forwarding	Trajectory based forwarding (TBF) through Local Positioning System (LPS)	Only routing is considered and there is no security considered.
Greedy Perimeter Stateless Routing	GPSR makes greedy forwarding decisions using only information about a router's immediate neighbors in the	Network routing is considered and trust based routing is not considered.

	network topology	
Directed Diffusion for Sensor Networks	This enables diffusion to achieve energy savings by selecting empirically good paths and by caching and processing data in-network.	This work considered diffusion based routing only.
LEACH protocol	LEACH protocol for routing is considered and data aggregated sent to ensure data redundancy problem	Data Security and node security is not considered
Gradient data dissemination	Packets are diffused and propagated through the routes generated through hop message acknowledgement	Node reputation is not considered

Table 1: Related work analysis

Some of the work studied about sleep and awake methodologies, when an even detected, the sensor node will wake up and transmit the packet and then go to sleep mode. The work in [1] discussed the role assignment to nodes for event detection. Information fusion algorithm is proposed for role assignment. The coordinator nodes in the network finds the event and informs sensor node, sensor node thus awake and send event to sink. This system will work even when single event is detected.The node for forwarding is chosen based on number of hops to destination for selecting a shortest path. The role is migrated to other node if it necessary to save the network energy. However, this work has considered shortest path routing with role assignment, the security of the network is a major concern is not addressed.

Some workshave studied on clustering algorithm as such as LEACH protocol for cluster formation in wireless sensor network. To maintain the energy of cluster head (CH), CH is chosen dynamically in such environments. This is the vast area of study, in work [2], the author used LEACH protocol along with data aggregation model to save network energy. The concept of redundant data filtering improves the network performance. As all the sensor node may given same or relevant data, the redundancy avoided by data aggregation, this decreases energy usage for routing all data and also memory space can be handled effectively. In this work, the node cluster is formed based on density of nodes in particular location and the cluster head will be changed dynamically to forward message to sink, thus energy of cluster head can be saved. Though the work studied on cluster head formation with LEACH, the energy efficiency only can be achieved and network security is not considered.

Another work studied about data aggregation and forwarding is [3], the shortest path is also achieved in this work. They built a tree with shortest number of hops to destination by flooding the hop configuration message to all neighbor nodes. This tree parameter starts from sink as 1 and increase the number of hope when it reaches the branches of sensor node, which transmits packets. This hop count message will be stored in every nodes for cluster formation. The cluster formation happens whenever the node finds an event, though all sensor node may eligible as leader, only the node with less hop count is considered for leader election as it decrease energy consumption for transmission. The routes are established and the algorithm runs to elect next leader and will be updated to all nodes periodically. The result proved that overhead decrease and increase in packet delivery ratio. However the sensor node's individual energy is not considered, which is mandatory selecting a sensor node in routing path selection.

Gradient mechanism for packet diffusion is carried out in work [4] with gradient calculation. The gradient process is started for data propagation in network, this is achieved by sending hop message to all nodes by the sink. Not only one path is created to deliver packets, there are also all possible alternate routes are generated. If one path fails, the data delivered through the alternate path, thus ensuring the packet delivery. Through the process of dissemination the data is forwarded to the neighbor node who is having high gradient values. once that neighbor received, it also follow the same principle of gradient and sent to next neighbor. This process is carried till it reached the destination. Once the data transfer done, the energy decrease with transaction and gradient value also decreased. Thus for the next transaction another high gradient node will be chosen. Results shows that the energy utilization of network is good and lifetime is increased in this routing strategy. The data packet delivery is high in this work, whereas the work not considered the node reputation for packet transmission or any security for the network.

Low Duty Cycle is another area of study for energy efficient routing, the work [5] accomplished Dynamic Switch Forwarding (DSF) for supporting unreliable networks. Increased Packet delivery ratio, delay of communication reduced and with less energy consumption is achieved in this work. This is evaluated in Carrier Sense Multiple Access (CSMA). The concept of sleep and awake is used here. The sensor node awake in time and get event then forward to sink, once forward it sends to sleep mode, then it will awake when the timer is on. The sensor node cannot transmit the packets received from other node on sleep time, only on awake time it can do. Thus when the node is in awake time, the end to end delay of packet delivery can be reduced by reducing the number of hops to transmit the data packets received. The sleep latency is fixed by network admin, which is the delay or time to wakeup in specified intervals. Though this method can achieve highly energy efficient, the data packets delivery are not highly reliable. As the nodes goes to sleep, when no neighbor nodes are available, the packets may drop due to link failure. Moreover, the network security or node reputations are not studied here.

The low duty cycle routing studied in literature were facing issues on packet re-transmission. When no neighbors are detected, the sensor node re-transmits packet to check the availability of neighbor to deliver the packets to sink. However, the studied work were not much energy efficient, thus the author in [6] studied which handles link monitoring and measurement algorithm, this finds the reliable path using Time to live (TTL) packets. The work considered the node reliability by transmission success rate this is monitored by acknowledgement packets received by the sender from the neighbor node on each delivery transmissions. When there is missing of end to end acknowledgment, the sender attempts for re-transmission of same packets. Density of deployed node is important factors which affects the delivery in this type of low-duty cycle routing, as the sensor nodes goes for sleep, if the network is highly dense, then there is a high probability of packet delivery through any one of the available node which is awake that time. Thought this work achieved highly energy efficient on routing, the trust values of nodes are important factors to considered in highly dense network to maintain the network security, thus our proposed work considered three types of trust values to maintain the node reputation.

Underwater sensor network is another area of study using sensor networks, this USN are highly active research area these days. The author in [7] discussed depth based routing strategy, which is a major issue in under water networks. This work studied with multiple sink as the message delivery is more difficult in highly immerse environment. The exact localization of sensor node is not required when going for depth based, only node depth is calculated. This type of routing is initiated when the sensor node broadcast a packet, the neighbor node receives and compares the sender node's and itself depth of packet. The depth is lesser then it forwards the packets otherwise it drops the packets. As many nodes may be selected for packet forwarding, the data packets sent can be repeatedly sent, this redundancy of data is also handled by this work by suppressing the redundancy. The priority queue is used reduces number of forwarding nodes. Packet holding time is calculated and along with node depth comparison, the packet redundancy is reduced. Though the work addressed underwater routing with depth based knowledge, the path and number of routes are not controlled, this may lead to sever security problems.

Sensor node privacy is one of the major concern, as the attacker may be interested to get the sensor node information such as node id, node key, location details etc, the work in [8] addressed node privacy by all location random routing. To overcome the problem of attackers gaining node information through very few attackers deployed in parasitic networks.To achieve source location privacy, the proposed work used different routing algorithm, when the source node detects a packet is it sent to the neighbor node depending on geographical routing based on node's perimeter distance. As the perimeter only considered as routing parameter selection, the exact location of node not need by the algorithm and it forwards data packets. As the outing every time take in dynamic, breaching the perimeter information is also not a major issue as the node privacy is completely protected. This work is much of our implementation on considering routing, however this is considered based on perimeter and our proposed work is based on three type of reputation.

Node reputation is also considered for intrusion detection in wireless sensor network, this type of study done in [9], the author proposed intrusion detection framework with use of beacon nodes, which are special nodes used for monitoring sensor node's reputation. The IDS monitor both local and global responses then final decision done by cooperative detection engine Based on shared opinion the reputation of node is fixed by the neighbors. Local agent monitors network activity and inform IDS, if any anomaly activity detected, then can able to identify node identity. IDS achieves this by certain rule provided by network admin. Though this system used reputation based anomaly detection, the routing strategy is not available in this work.

The inference from these work is arrived here to conclude that there is demand for secure, shortest path routing for wireless sensor networks to achieve the network performance in terms of energy and reliability in terms of nodes reputation. The existing work discussed above were studied either routing strategy or security of network. However, there is a need for novel strategy which is a combination of both.

3. proposed work

The Objective of proposed work is to implement a shortest path routing to achieve high network lifetime and by-pass attackers nodes if any on the path. Thus to provide a secure and shortest path routing in wireless sensor network is the aim of this work.

The innovation of the project is to provide Secure Shortest Path Routing to deliver packages properly, for this proposed approach uses latest algorithms and techniques for network lifetime and secure network. The below figure shows the network with trust, security and privacy as mandatory modules.

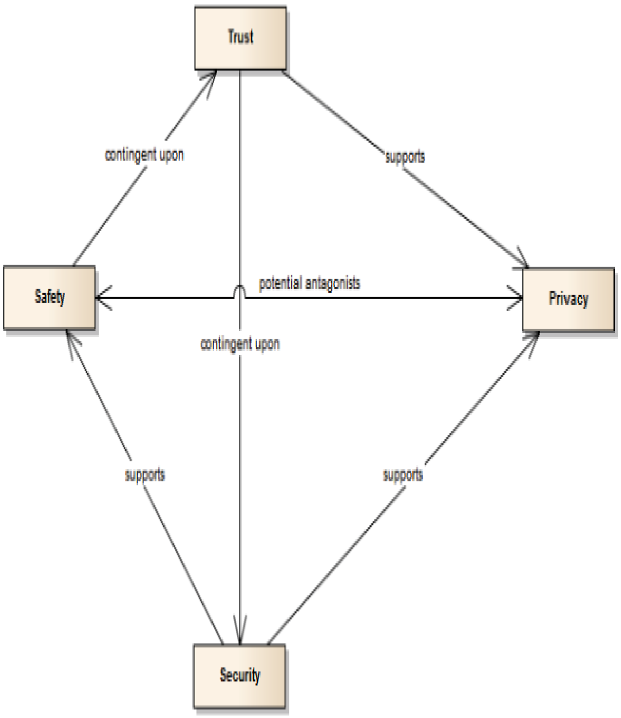


Figure:5 System Architecture

The proposed Shortest path algorithm is takes shortest path also defend against attacker nodes. This process is handled by arriving at the reputations of the sensor nodes the based on the reputation values and sensor node has been considered for the routing path from all available neighbors. Sink node receives periodic reputation values of all available sensor nodes also the energy of the sensor nodes will reduce on every transactions will be updated periodically to sink nodes. Sensor nodes also get the reputation updates and energy updates to get their right neighbour for routing path. This avoids any suspicious nodes on routing path and packet delivery can be ensured through selected higher energy node compared with the given threshold levels.

Node Deployment

The n number of sensor nodes is dispersed deployed and randomly in distributed manner to coverage area. On node instantiation, all nodes are assigned with unique identities. The sensor nodes have homogeneity in characteristics and limited constraints. There are two clusters considered on deployment. Each cluster has one sink node, which has no restriction on resources. Base station node receives all information from all deployed sinks from each cluster. The routing will take place in a multi-hop manner.

Neighbour Detection

In wireless sensor networks, routing is considered through AODV protocol as multi-hop transmission. It is mandatory to get routing table, which includes neighbour sensor nodes in the networks. In this module, one hop neighbours of every node is identified dynamically. The communication among the nodes is based on a tree topology admitting destination as the root. The sender node first broadcast a message with a hop counter to its neighbour node. The sensor node, which receive message set sender as the parent, increase the hop then send to neighbours. The edges are created along the nodes and packets transmitted on this communication tree. The following figure shows the system architecture of proposed system.

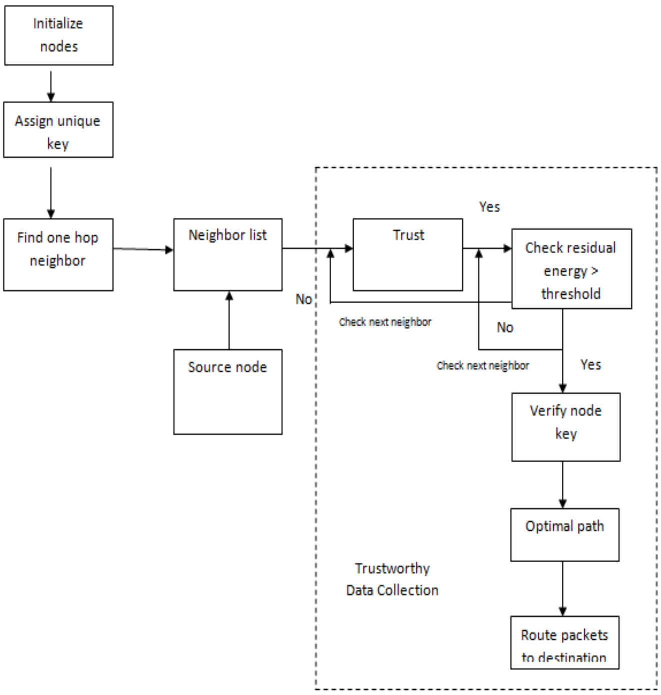


Figure: 6 System Architecture

Trust Calculation

Calculating trust and its maintenance for every node and updating the information along to the network is a tedious task due to the unpredictable nature of sensor nodes and complexity arises in computational and energy constraints in the sensor nodes. A novel trust mechanism is proposed, which composes of three different methods for trust calculations on each sensor nodes. These trust values are calculated by the node's ability and reliability of packet receiving and packet forwarding. This calculations based on reputation of nodes and these vector is outcome of previous transactions made by sensor nodes and registered by neighbour node or sink nodes. The length of the trust value vector is considered as 8 bit with values around 10. The high the trust value, the high the node's trust on legitimate, whereas lowest trust value means lowest trusted node or illegitimate node.

Node trust values are calculated using formula 1.

Trust value = Communication Trust (CT)+ Recommendation Trust (RT)   -----(1)

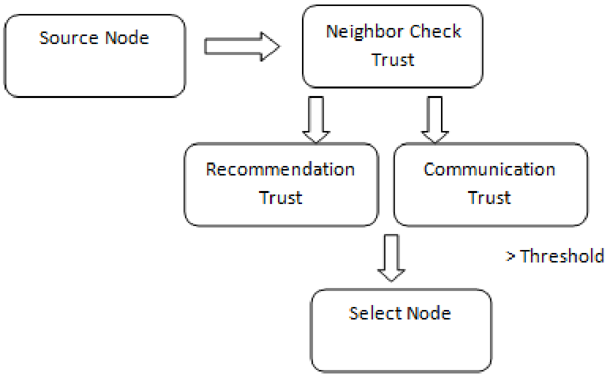


Figure:7 Trust Based route Selection

This trust vector is maintained in network for all deployed nodes in all clusters. Once the packet transmission is done, the trust values of trans-receiver node is updated automatically. The trust value is increased from Least Significant Bit (LSB) to Most Significant Bit (MSB). Once the transaction is done, sensor node's trust value is updated for LSB, which is the lowest value to MSB, which is the highest values.

The objective of this module is to find reliable routes which high energy node and less cost for packet transmission. Reliability and energy cost of routes are most important factor to be considered in route selection.

The energy cost of a route is related to its reliability. If routes are less reliable, packet retransmission probability increases. High amount of energy will be utilized for packet transmission and retransmissions of the packets. It is designed an energy-aware reliable routing algorithms for proposed systems. Whenever the node transmits packets, the energy will be reduced by count '5'. Similarly trust values are assigned to nodes are '10', whenever the node transmits packets, the trust value is increase by '1'.

The trust value is evaluated as follows:

$$T = C_1 \left[\sum_{i=1}^{4} \frac{N_i * I_i(t)}{N_i} \right] + C_2 \left[\sum_{i=1}^{4} \frac{N_i * E_i(t)}{N_i} \right]$$

Where,

T is Trust value [1 <T < 0]

Ni is Rating i=l, 2, 3, 4 and N>N-l

Iit isith value of Initial Trust at time t

Ejt is ith value of End Trust at time t

C 1 and C2 is the constant to manage trust

The energy and trust aware routing as described above is given in pseudo code format below, which represents the detailed steps involved in this routing strategy. If the packets are delivered through the constructed path, the attackers cannot able to identify the path. The complexity behind attacking route for the attackers persists that every time, the trust methodology changes and the route will be taken along with the calculated path by the trust mechanism, which allows attackers a tedious process to capture the route, in which the packets are traversing.

Energy and Trust Aware Secure Routing

Input: Set of Node SN| = Sink1, Sink2, SN1, SN2....SNn , Where SN is Sensor nodes

Output: Delivering data packets from Source 'S' to Destination 'D' based on secure route 'SR'

```
Step 1: Deploy a Server node 'S', two sink to show two cluster Sink1 & Sink2 and 'N' number of Sensor nodes in the wireless network
Step 2: Choose source node 'S' and destination node 'D', whereas D is Sink1 or Sink2
Step 3: Create a socket connection among the deployed nodes
Step 4: Declare energy value 'E' for all nodes in the network, initially assigned as 100. and Trust values assigned as 10.
Step 5: Create Routing Table, one- hop neighbour for all nodes deployed in Wireless network
Step 6: Create Routing path
    For Node (i=0, i<=n)
    If {
    If energy > threshold; and trust >threshold assign the node to routing table Rt
        }
        Return Rt
Step 7: Start the packet delivery by using the router derived above
Step 8: Destination receives packet from source using multihop routing mode
```

Dynamic routeconstruction

Deliver the packets from the source node to the sink node based on the dynamic routes. A data packet is transmitted through the optimum path, which is constructed using above two modules, which decided based on the energy, security to transmit and process a data packet. The route created are shortest to the destination, which boosts the networks energy and achieves high lifetime to network. The below figure represents the dynamic routing of path construction.

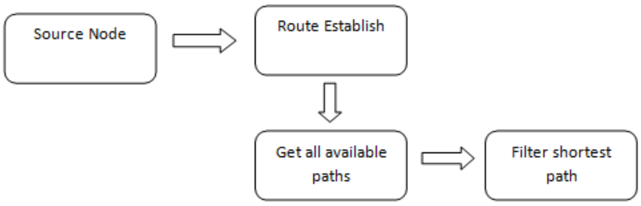


Figure: 8 Dynamic route construction

Dynamic route construction as explained is given in pseudo code format below, which represents the detailed steps involved in this dynamic route creations. The algorithm try get the shortest path with minimum number of hops to transmit the packets in considered.

Pseudo code - Dynamic Route Construction

```
Input: Set of Node SN| = Sink1, Sink2, SN1, SN2....SNn , Where SN is Sensor nodes
Output: Routing path 'p'
Step 1:    Choose source node 'S' and destination node 'D',    whereas D is Sink1 or Sink2
Step 2:    Choose neighbor nodes based on energy based routing        algorithm
Step 3: Get all available node
Step 4:    Create Routing path
Step 5:    Get all available path
Step 6:    Select path which has total_number_of_hops
Step 7:    Route packets on the filtered route in step 6
```

Deliver the packets from the source node to the sink node based on the dynamic routes. A data packet is transmitted through the optimum path, which is constructed using above two modules, which decided based on the energy, security to transmit and process a data packet. The route created are shortest to the destination, which minimizes networks energy consumption and achieves high lifetime to network.Proposed a reputation system model, which maintains the reputation of nodes and considered for the routing. The routing taken such that it will not considered compromised nodes on the routing path.

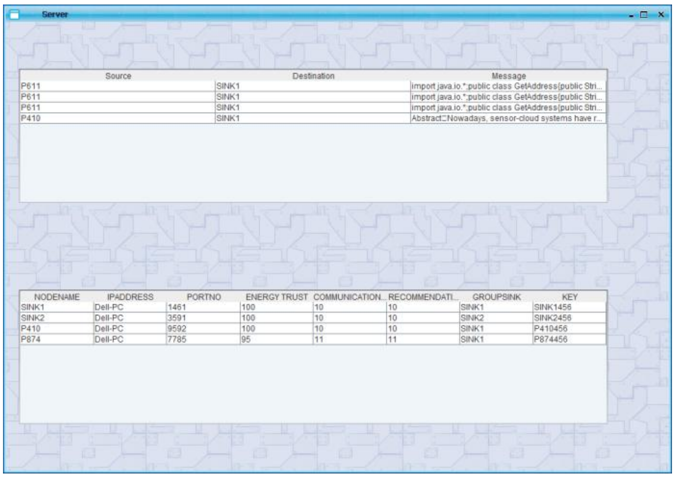
4. Results And Discussions

Implementation is done in JDK 1.8 with Swing application. The hierarchy of wireless sensor network is constructed in this implementation with Base station node, cluster head as Sink node and sensor nodes. The below screen represents the home page of base station node. Base station node design considers providing information in two tables. One table with information of messages transmitted by sensor node. Each sensor node assigned with unique ID, thus base station node received acknowledgment whenever node forwards message to destination. As the implementation has considered two clusters, Sink 1 and Sink2 are the destination nodes. Sensor node ID, Destination to which it has forwarded, and message.

The second table lists the information of monitoring part, which has node ID, IP address of node, port number, Node energy, Communication trust value of nodes and recommendation trust value of nodes, the cluster of node as Sink1 or Sink2 and node Key value.

The routing path hops can be controlled by the network admin, the paths generated during the routing is more than one. All eligible nodes are selected thus all available routing paths are generated. The number of minimum hops and maximum hops can be defined such that optimum path can be obtained through our proposed routing protocol. The performance of routing path creation is highly effective in this method compared with all other existing algorithms.

Similarly, the global optimum value and local optimum values can defined, which can represents, the internal cluster routing for local and cluster to cluster routing for global optimum values respectively. The two differs in way that one considers the geographical location of node and the other considered shortest path according to the number of hops to sink. The below screen represents the graphical user interface design for base station node.

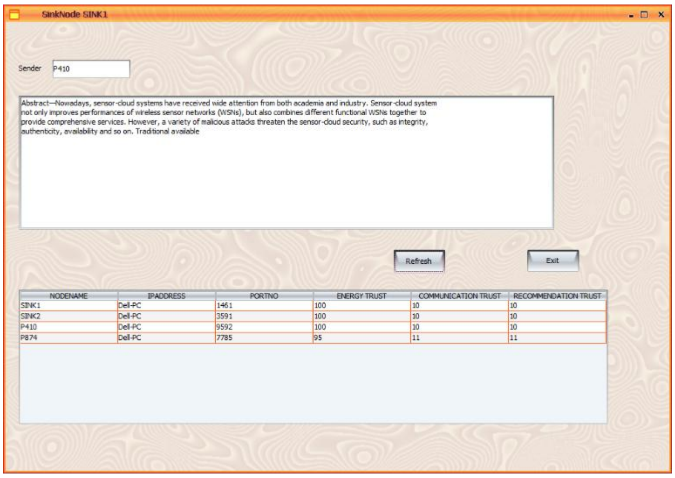


Source	Destination	Message
P611	SINK1	import java.io.*;public class GetAddress{public Stri...
P611	SINK1	import java.io.*;public class GetAddress{public Stri...
P611	SINK1	import java.io.*;public class GetAddress{public Stri...
P410	SINK1	Abstract□Nowadays, sensor-cloud systems have r...

NODENAME	IPADDRESS	PORTNO	ENERGY TRUST	COMMUNICATION...	RECOMMENDATI...	GROUPSINK	KEY
SINK1	Dell-PC	1461	100	10	10	SINK1	SINK1456
SINK2	Dell-PC	3591	100	10	10	SINK2	SINK2456
P410	Dell-PC	9592	100	10	10	SINK1	P410456
P874	Dell-PC	7785	95	11	11	SINK1	P874456

Figure: 9 Base Station Design

The below screen represents the home page of Sink node. Sink node design also considers providing information about sensor nodes. The node which is covered under particular sink node are provided details to the corresponding sink. Node name, IP address of node, port number, Node energy, Communication trust value of nodes and recommendation trust value of nodes. The design also constructs message sent be sensor node will be shown on display with sender node.



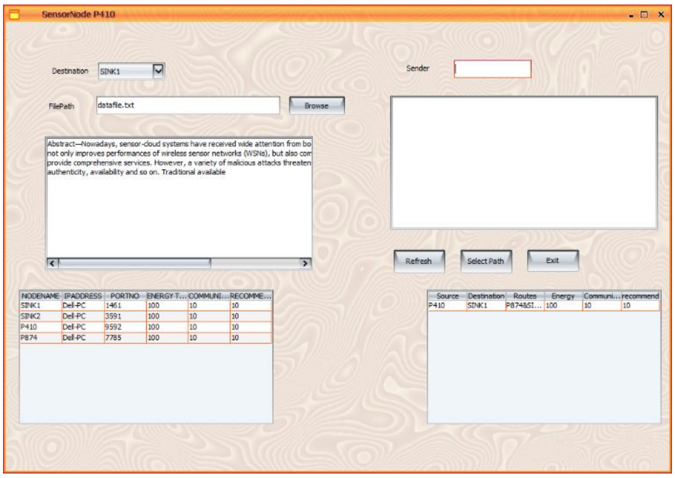
Sender: P410

Abstract—Nowadays, sensor-cloud systems have received wide attention from both academia and industry. Sensor-cloud system not only improves performances of wireless sensor networks (WSNs), but also combines different functional WSNs together to provide comprehensive services. However, a variety of malicious attacks threaten the sensor-cloud security, such as integrity, authenticity, availability and so on. Traditional available

NODENAME	IPADDRESS	PORTNO	ENERGY TRUST	COMMUNICATION TRUST	RECOMMENDATION TRUST
SINK1	Dell-PC	1461	100	10	10
SINK2	Dell-PC	3591	100	10	10
P410	Dell-PC	9592	100	10	10
P874	Dell-PC	7785	95	11	11

Figure: 10 Sink Node Design

The below screen represents the design of Sensor node. Sensor node design also considers providing information about sensor nodes and its neighbour nodes on its own cluster. They are designed with two tables. One table shares the information of node monitoring module, including Node name, IP address of node, port number, Node energy, Communication trust value of nodes and recommendation trust value of nodes. The next module of information is about node selection and routing information. This considers providing knowledge on Source node ID, Destination Node ID, Established shortest route, Updated energy and updated trust values of communication trust and recommendation trust.In this routing model, there is no necessary for packet re-transmission as the route are generated by valid RREQ and RREP packets. Moreover, the retransmission are required only in Sleep and wake type of network, whereas our model does not considered the one.



Destination SINK1

FilePath datafile.txt

Sender

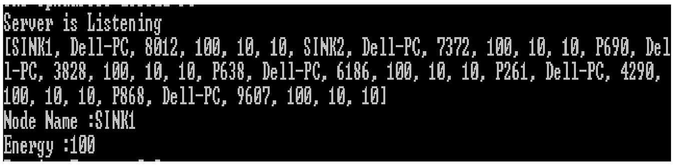
Abstract—Nowadays, sensor-cloud systems have received wide attention from bo
not only improves performances of wireless sensor networks (WSNs), but also com
provide comprehensive services. However, a variety of malicious attacks threaten
authenticity, availability and so on. Traditional available

NODENAME	IPADDRESS	PORTNO	ENERGY T...	COMMUNI...	RECOMME...
SINK1	Dell-PC	1461	100	10	10
SINK2	Dell-PC	3591	100	10	10
P410	Dell-PC	9592	100	10	10
P874	Dell-PC	7785	100	10	10

Source	Destination	Routes	Energy	Communi...	recommend
P410	SINK1	P874&SI...	100	10	10

Figure: 11 Base Station Design

The figure shows the list of neighbour nodes given to sensor nodes. The node has sensor node ID of all available neighbour with IP address and port number. In this time of node instantiation, every node assign an energy of 100 as minimum value. For every successful transaction, the node energy will be reduced in number 5. The energy and Trust value will be updated immediately to all nodes.



```
Server is Listening
[SINK1, Dell-PC, 8012, 100, 10, 10, SINK2, Dell-PC, 7372, 100, 10, 10, P690, Del
l-PC, 3828, 100, 10, 10, P638, Dell-PC, 6186, 100, 10, 10, P261, Dell-PC, 4290,
100, 10, 10, P868, Dell-PC, 9607, 100, 10, 10]
Node Name :SINK1
Energy :100
```

Figure: 12 Neighbour details

Data security, privacy, data integrity plays role in wireless sensor networks. As there are three type of node including source, relay and destination. The node which send data should maintain privacy for data. The relay nodes are one, which forward data from source to destination. The node gets data and forward to sink node of its own cluster.

Security key infrastructures creates security key for sensor nodes, sink and base station and assigned on instantiation. This will avoid any risk of attackers, by checking the key value on data packets forwarding. The time consumption of the packet forwarding is also registered on each sensor nodes.

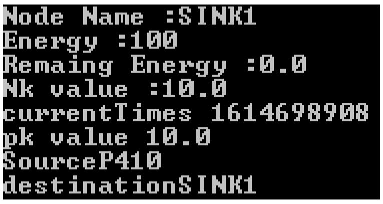
The routing paths are the shortest to the destination, which minimizes consumption of routing energy and achieves high lifetime to network.Proposed a node reputation model, maintains the two type of trust are recommendation trust and communication trust are considered for the routing. The routing taken such that it will not considered compromised nodes on the routing path.

When a node is finding an event, the event will be forwarded to corresponding cluster's sink node. The node gets details of neighbour about its energy and trust value, which is shows in below screen, the time of event detected will be registered by the sensor node for reference of event time. Choosing node for routing obeys with condition

Energy > Threshold (Where threshold is predefined by network admin)

Trust = Recommendation Trust + Communication Trust

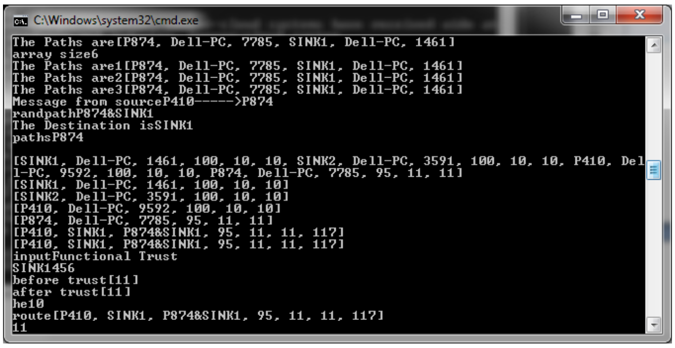
Trust > Threshold (Where threshold is predefined by network admin)



```
Node Name :SINK1
Energy :100
Remaing Energy :0.0
Nk value :10.0
currentTimes 1614698908
pk value 10.0
SourceP410
destinationSINK1
```

Figure: 13 Neighbour Energy and Trust details detection

The following screen shows neighbour detection in each sensor nodes. TheSensor node ID, IP address and port number are listed below.



```
The Paths are[P874, Dell-PC, 7785, SINK1, Dell-PC, 1461]
array size6
The Paths are1[P874, Dell-PC, 7785, SINK1, Dell-PC, 1461]
The Paths are2[P874, Dell-PC, 7785, SINK1, Dell-PC, 1461]
The Paths are3[P874, Dell-PC, 7785, SINK1, Dell-PC, 1461]
Message from sourceP410----->P874
randpathP874&SINK1
The Destination isSINK1
pathsP874

[SINK1, Dell-PC, 1461, 100, 10, 10, SINK2, Dell-PC, 3591, 100, 10, 10, P410, Del
l-PC, 9592, 100, 10, 10, P874, Dell-PC, 7785, 95, 11, 11]
[SINK1, Dell-PC, 1461, 100, 10, 10]
[SINK2, Dell-PC, 3591, 100, 10, 10]
[P410, Dell-PC, 9592, 100, 10, 10]
[P874, Dell-PC, 7785, 95, 11, 11]
[P410, SINK1, P874&SINK1, 95, 11, 11, 117]
[P410, SINK1, P874&SINK1, 95, 11, 11, 117]
inputFunctional Trust
SINK1456
before trust[11]
after trust[11]
he10
route[P410, SINK1, P874&SINK1, 95, 11, 11, 117]
11
```

Figure: 14 Neighbour detection

Energy and trust efficient path is selected, which is one of the effective parameter considered in routing protocol creation. Though there are many works available for energy based routing, the proposed work achieved this along with trust comparisons, the proposed work minimizes any delay in packet delivery ratio. The proposed routing protocol considers direct trust, indirect and functional trusts on routing, thus the routing strategy can be even more dynamic, the attackers cannot identify the route which the packets are sent. This routing protocol can be changed and it is dynamic based on network density, routing type also changes everytime dynamically.

With the proposed routing, the lifetime of battery power increases for sensor nodes, thus the high network lifetime can be achieved. The proposed routing protocol follows the acknowledgement of message delivery to update the trust and reduce the energy of node. If any topological changes are highly ignored, because it may not affect the routing.

5. Conclusions

The wireless sensor networks are resource limited networks and are highly vulnerable to many attacks. These problems are addressed in this proposed work with novel routing framework, which is considering combination of shortest path, sensor node energy and trust values. Internal or external attacks, node compromise attacks can be avoided by proposed routing framework. The novelty of the work increases the network lifetime of sensor nodes and secure routing. Trust based routing is maintained by a reputation system developed in three types. The trust for sensor nodes according to the message delivery rate is considered as one type, the next type is provided when the node communicates to the other node and finally the third type is trust after authenticating by the sink node with key values. The routing considered is multi-hop routing, with relay nodes are satisfied with node's minimum energy and trust value. The node path is the shortest one among all available route to destination.

Future Directions

As future work, data aggregation, data redundancy can be considered along with this secure routing strategy. The network can also be considered with sleep and awake strategy for packet forwarding, location based routing on geographic location of nodes can also be considered as in future work. As the proposed work has not considered any cryptographic algorithm, the future work can also be extended to use some lightweight protocol such as elliptic curve cryptography (ECC)

References

[1] E. F. Nakamura, H. A. B. F. de Oliveira, L. F. Pontello and A. A. F. Loureiro, "On Demand Role Assignment for Event-Detection in Sensor Networks," 11th IEEE Symposium on Computers and Communications (ISCC'06), Cagliari, Italy, 2006, pp. 941-947, doi: 10.1109/ISCC.2006.110.

[2] W. B. Heinzelman, A. P. Chandrakasan and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," in IEEE Transactions on Wireless Communications, vol. 1, no. 4, pp. 660-670, Oct. 2002, doi: 10.1109/TWC.2002.804190.

[3] Villas, Leandro &Boukerche, Azzedine&Loureiro, Antonio. (2009). A reliable and data aggregation aware routing protocol for wireless sensor networks.245-252. 10.1145/1641804.1641846.

[4] J. Wan, J. Wu, X. Xu and Y. Yan, "An Efficient Gradient Mechanism of Directed Diffusion in Wireless Sensor Network," 2008 International Conference on Computational Intelligence and Security, Suzhou, China, 2008, pp. 427-431, doi: 10.1109/CIS.2008.133.

[5] Y. Gu and T. He, "Dynamic Switching-Based Data Forwarding for Low-Duty-Cycle Wireless Sensor Networks," in IEEE Transactions on Mobile Computing, vol. 10, no. 12, pp. 1741-1754, Dec. 2011, doi: 10.1109/TMC.2010.266.

[6] Venkatesha, &Ashwini, T.N. &Tejaswi, V. & K R, Venugopal&Iyengar, Sundararaj&Patnaik, Lalit&Achar, Akshay. (2015). RPRDC: Reliable Proliferation Routing with low Duty-cycle in Wireless Sensor Networks. Procedia Computer Science. 54. 37-46. 10.1016/j.procs.2015.06.005.

[7] Yan, Hai& Shi, Zhijie& Cui, Jiawen. (2008). DBR: Depth-Based Routing for Underwater Sensor Networks. Lect. Notes Comput.Sci.. 4982. 72-86. 10.1007/978-3-540-79549-0_7.

[8] Wang, Na &Zeng, Jiwen. (2017). All-Direction Random Routing for Source-Location Privacy Protecting against Parasitic Sensor Networks.Sensors. 17. 614. 10.3390/s17030614.

[9] K. Gerrigagoitia, R. Uribeetxeberria, U. Zurutuza and I. Arenaza, "Reputation-based Intrusion Detection System for wireless sensor networks," 2012 Complexity in Engineering (COMPENG). Proceedings, Aachen, Germany, 2012, pp. 1-5, doi: 10.1109/CompEng.2012.6242969.

[10] H. Chen, H. Wu, X. Zhou and C. Gao, "Reputation-based Trust in Wireless Sensor Networks," 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07), Seoul, Korea (South), 2007, pp. 603-607, doi: 10.1109/MUE.2007.181.

[11] T. Ho et al., "A clinical decision and support system with automatically ECG classification in telehealthcare," 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom), Natal, Brazil, 2014, pp. 293-297, doi: 10.1109/HealthCom.2014.7001857.

[12] X. Wang, L. Ding and Sheng Wang, "Reputation-based sensing reliability assurance in wireless sensor networks," 2009 IEEE Instrumentation and Measurement Technology Conference, Singapore, 2009, pp. 40-45, doi: 10.1109/IMTC.2009.5168413.

[13] T. A. Zia, "Reputation-based trust management in wireless sensor networks," 2008 International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Sydney, NSW, Australia, 2008, pp. 163-166, doi: 10.1109/ISSNIP.2008.4761980.

[14] Yekkala, Indu& Dixit, Sunanda. (2018). Prediction of Heart Disease Using Random Forest and Rough Set Based Feature Selection. International Journal of Big Data and Analytics in Healthcare. 3. 1-12. 10.4018/IJBDAH.2018010101.

[15] Ganeriwal, Saurabh&Balzano, Laura &Srivastava, Mani. (2003). Reputation-based framework for high integrity sensor networks.TOSN.4. 10.1145/1029102.1029115.

[16] H. A. Esfahani and M. Ghazanfari, "Cardiovascular disease detection using a new ensemble classifier," 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, Iran, 2017, pp. 1011-1014, doi: 10.1109/KBEI.2017.8324946.

[17] X. Yang, D. Liu, L. Cong and L. Liang, "Shortest path algorithm based on distance comparison," 2014 IEEE Geoscience and Remote Sensing Symposium, Quebec City, QC, Canada, 2014, pp. 3137-3139, doi: 10.1109/IGARSS.2014.6947142.

[18] Jinhao Lu and Chi Dong, "Research of shortest path algorithm based on the data structure," 2012 IEEE International Conference on Computer Science and Automation Engineering, Beijing, China, 2012, pp. 108-110, doi: 10.1109/ICSESS.2012.6269416.

[19] M. Gandhi and S. N. Singh, "Predictions in heart disease using techniques of data mining," 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Greater Noida, India, 2015, pp. 520-525, doi: 10.1109/ABLAZE.2015.7154917.

[20] T. Rajesh Kumar, G.R.Suresh, S. KanagaSubaRaja, C.Karthikeyan, “Taylor-AMS Features and Deep Convolutional Neural Network for Converting Non-Audible Murmur To Normal Speech”, Computational Intelligence, Wiley Publishers, 0824-7935 , Feb-2020 (SCIE) DOI: 10.1111/coin.12281.

[21] J. P. Kelwade and S. S. Salankar, "Radial basis function neural network for prediction of cardiac arrhythmias based on heart rate time series," 2016 IEEE First International Conference on Control, Measurement and Instrumentation (CMI), Kolkata, India, 2016, pp. 454-458, doi: 10.1109/CMI.2016.7413789.

[22] V. T. Chakaravarthy, F. Checconi, F. Petrini and Y. Sabharwal, "Scalable Single Source Shortest Path Algorithms for Massively Parallel Systems," 2014 IEEE 28th International Parallel and Distributed Processing Symposium, Phoenix, AZ, USA, 2014, pp. 889-901, doi: 10.1109/IPDPS.2014.96.

[23] T. Ho et al., "A clinical decision and support system with automatically ECG classification in telehealthcare," 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom), Natal, Brazil, 2014, pp. 293-297, doi: 10.1109/HealthCom.2014.7001857.

[24] T. Rajesh Kumar, V.LakshmiSarvani, S.Siva Kumar, Asalg.G.Gupta, D.Haritha, “Murmured Speech Reorganization using Hidden Markov Model”, Proceeding of ICSSS-2020,IEEE Explorer, July-2020.

[25] P. R. Katre and A. Thakare, "A survey on shortest path algorithm for road network in emergency services," 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, India, 2017, pp. 393-396, doi: 10.1109/I2CT.2017.8226158.

[26] N. A. Khalid, Q. Bai and A. Al-Anbuky, "Adaptive Trust-Based Routing Protocol for Large Scale WSNs," in IEEE Access, vol. 7, pp. 143539-143549, 2019, doi: 10.1109/ACCESS.2019.2944648.

[27] S. Madden, R. Szewczyk, M. J. Franklin and D. Culler, "Supporting aggregate queries over ad-hoc wireless sensor networks," Proceedings Fourth IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, USA, 2002, pp. 49-58, doi: 10.1109/MCSA.2002.1017485.

[28] H. Yan, N. Al-Hoqani and S. Yang, "In-network multi-sensors query aggregation algorithm for wireless sensor networks database," 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), Zhuhai, China, 2018, pp. 1-8, doi: 10.1109/ICNSC.2018.8361280.

[29] R. Ennaji and M. Boulmalf, "Routing in wireless sensor networks," 2009 International Conference on Multimedia Computing and Systems, Ouarzazate, Morocco, 2009, pp. 495-500, doi: 10.1109/MMCS.2009.5256646.

[30] N. Nasser, A. Al-Yatama and K. Saleh, "Mobility and routing in Wireless Sensor Networks," 2011 24th Canadian Conference on Electrical and Computer Engineering(CCECE), Niagara Falls, ON, Canada, 2011, pp. 000573-000578, doi: 10.1109/CCECE.2011.6030516