International Journal of
Sensor Networks and Data Communications

Darwish and Elqafas, Int J Sens Netw Data Commun 2016, 6:1
DOI: 10.4172/2090-4886.1000150

Research Article Open Access

Enhanced Algorithms for Fault Nodes Recovery in Wireless Sensors Network

Darwish IM* and Elqafas SM

[1]Institute of Postgraduate Studies and Research, Selangor, Malaysia
[2]Arab Academy for Science, Technology and Maritime Transport, Giza Governorate, Egypt

Abstract

An integration of sensing environment with the numerous deployments of sensor nodes in Wireless Sensor Network (WSN) causes the severe security threats and hence the trust assurance mechanisms are required. For the large scale WSN, the existence of a number of intermediate nodes is responsible for the data forwarding to the sink node. Due to the battery operated sensors, the recharge and replace mechanisms suffer from the energy conservation and minimum network lifetime. The identification of fault nodes on the transmission path plays the major role in energy conservation. With the dense deployment of sensor nodes, the failures in node and link are high that disrupts the entire communication. This paper proposes the suitable alternative fault-free path prediction model to perform the communication among the nodes. Initially, the sensor nodes are deployed in the WSN environment. Once the initialization of source and destination nodes are over, the path between them is predicted through the Hamiltonian path prediction model. During the failure, scenario, this paper estimates the node and link parameters such as Received Signal Strength Indicator (RSSI), queue size, response time, and bandwidth are individually estimated and group them into the Quality Factor (QF). Based on the QF, the proposed work predicts the fault-free link to alleviate the unnecessary transmissions to the fault node and reduces the energy consumption. The comparison between the proposed Hamiltonian Path-based Hyper Cube (HPHC) network with the existing fault detection mechanisms regarding the performance measures such as Packet Delivery Ratio (PDR), fault node detection rate, throughput and end-to-end delay assures the effectiveness of HPHC in WSN communication.

Keywords: Link failure handling; Link quality factor; Reliable data delivery; Routing protocol; Stable routing

Introduction

Large scale sensing technologies are integrated with the several wireless communication links open up the various research issues regarding the minimum energy and network lifetime in Wireless Sensor Networks (WSN) [1]. The existence of shared unreliable transmission medium among the nodes induces the security threats during the communication. There are numerous schemes are developed to address the security issue in which they are limited by four factors as follows: architectural differences, limitations of sensor nodes, network density and size. Besides, the high computation, overhead, energy and memory requirement are high for the necessary solutions of WSN. For large scale WSN, the intermediate nodes perform the routing of data packets towards the sink with the following characteristics:

- Due to the limited resource availability and the large size nodes deployment induces the difficulties in the trust-based scheme.
- Traffic routed from base station to all nodes is high.
- Effective resource utilization against the number of constraints is essential.

The organization of routing is split-up into two stages such as single path routing and multi-path routing [2].

Single path routing

The simple and scalable routing established between the source and destination nodes for the specific period. The selection of an intermediate node by the source node is the repetitive task which increases the power depletion and minimizes the network lifetime. Besides, the data manipulation is corrupted with the presence of malicious node on the routing path and the lack of fault tolerant mechanism.

Multi-path routing

In this routing, a multiple number of paths are extracted to deliver the data from source to destination. Due to the intensive number of multiple paths, the assurance of reliability, integrity and load balancing is the major requirement alternative to the single path routing.

The maintenance of powerfully connected topology at all the times is the major requirement for an effective communication. The generation of faults induces the failures in WSN due to the following major issues [3]:

- Problems in fabrication process.
- Environmental factors.
- Battery power depletion
- Enemy attacks.

The failure in node causes the partition of the whole network into disjoint blocks and breaks the network connectivity adversely. The Quality of Services (QoS) also affected by such type of failure nodes. The deviations from the normal behavior of nodes due to the random faults disrupt the network functions. The unaware of structure and

***Corresponding author:** Darwish IM, Researcher, Institute of Postgraduate Studies and Research, Arab Academic of Science and Technology, Selangor, Malaysia, Tel: +203 5622366; E-mail: imsaad73@gmail.com

Received April 25, 2017; **Accepted** May 12, 2017; **Published** May 18, 2017

Citation: Darwish IM, Elqafas SM (2016) Enhanced Algorithms for Fault Nodes Recovery in Wireless Sensors Network. Int J Sens Netw Data Commun 6: 150. doi: 10.4172/2090-4886.1000150

state of WSN by the faulty nodes leads to the ignorance of other faults generated in a network. Besides, the misbehaving nodes have the capability to collide with another node with the required knowledge about structure. In both cases, the structural knowledge is the major requirement to identify the faulty nodes in WSN. Recently, the evolution of linear consensus algorithms considered the misbehaving or faulty nodes and sends the information to the neighbors. The characterization of resilience properties [4] of linear consensus strategies also required analyzing the connectivity among the nodes.

The route establishment comprises two steps transmission of Routing Request (RREQ) and replies (RREP) among the neighbors which lead to the power consumption. Due to the extensive power consumption, the battery life is degraded and the nodes in the network will become no longer available. Hence, the evolution of directed diffusion algorithms alleviates the power consumption problem by transmitting the neighbors to the first set. The nodes available in network elect the neighbor based on the hop count or rules with the exchange of request and replies [5]. The number of diffuser tower is increased drastically for large size WSN. The evolution of clustering approaches [6] addresses the issues in energy/power consumption minimization. The communication among the head branches reduce the diffusion tower that leads to reduction of power consumption effectively.

The fault detection approaches [7,8] are categorized into two as follows: architectural and methodological dimensions. On the basis of the architectural view, the detection approaches are classified into centralized and distributed. In centralized approaches, the fusion center is responsible for the collection of all the sensor measurements and selects the reliable subset which eventually sent to the base station. In distributed approaches, the exchange of sensor measurements with nearby nodes without any fusion center. The majority voting scheme, threshold scheme and Bayesian methods are available for methodological point of view. Among them, the Bayesian formulation considers the background information like sensor fault to classify the measurement as corrupted or not. The major deficiency of Bayesian formulation is the exponential growth of computational complexities and energy consumption. Hence, the suitable framework is needed to provide the trade-off between the effective communication and minimum energy consumption in WSN. This paper proposes the suitable fault-free path selection to achieve the effective communication with minimum computational resources. The technical contributions of proposed work are listed as follows:

- Hamiltonian-hyper cube construction predicts the necessary fault-free path on the basis of the link quality measures. The quality factor estimation depends on the three major parameters such as Received Signal Strength Indicator (RSSI), bandwidth and queue size.
- The simultaneous inclusion of node and link failures in link quality factor estimation validates the link and switch over to the adjacent link if it is unstable.
- The integration of Hamiltonian Path with the Hyper Cube (HPHC) enables the self-configuration of WSN environment with the best link information and the immediate update of the link failure to the nodes.
- The table maintenance is associated with all the nodes is responsible for the faulty node detection.

The paper organized as follows: The detailed description about the related works on fault-free path selection mechanism is discussed in section 4. The implementation process of Hamiltonian Path-based Hyper Cube (HPHC) is described in detail in section 5. The comparative analysis of proposed approach with existing fault detection framework is provided in section 6. Finally, the conclusions about the application of cube-extension of path prediction presented in section 7.

Related Work

This section discusses the traditional fault-discovery schemes to achieve among the WSN sensor nodes under failure conditions. Due to the powering of sensor nodes by the battery, the replacement and recharge of them are difficult to issue and hence the energy-efficient routing is the major concern in WSN applications. Jain [9] presented the brief review of the flat and data centric routing techniques with the necessary comparison. The brief survey concluded that more efficient, scalable and robust routing schemes are to be required to reduce the energy consumption and improves the battery lifetime effectively. The proper functioning of network is the necessary task under failure conditions observed in some components. Chouikhi et al. [10] presented the overview of mechanisms that improved the fault tolerance property. The solutions highlighted in this survey focused on detection and prevention of fault occurrence in energy aware routing and data aggregation mechanisms. The occurrence of selfish or malicious nodes disrupts the communication among the nodes by considering the multi-dimensional trust attributes. Bao et al. [11] proposed the highly scalable cluster-based hierarchical trust management protocol for WSN. The utility of hierarchical trust management protocol was demonstrated by applying the trust-based geographic routing and intrusion detection approaches. The existence of optimal trust threshold value effectively minimized the false positives and false negatives. The maintenance of high-quality WSN dependent on the delay requirement. Duche and Sarwade presented the new method to detect the sensor node failure or malfunctioning in the WSN environment. The utilization of Round Trip Delay (RTD) provided the accurate measure of confidence factor of RTD path. On the basis of confidence factor, the faulty nodes were detected [12,13].

Lee and Choi [14] presented the distributed fault detection algorithm that identified the faulty sensor nodes on the basis of the comparisons between the neighboring nodes and decision. During the sensing of the communication process, the time redundancy was used to tolerate the transient faults in the system. The employment of sliding window eliminated the delay in redundancy measurement. The extension of sensor nodes and their operation caused the inactive nodes were unaware of communication strategy. Hence, the split-up of the network (normal and inactive) was the difficult stage during the communication. To avoid this issue, Akbari et al. [15] designed the suitable techniques to maintain the cluster structure during the two scenarios such as faulty condition and energy drained cases. On the basis of the residual energy, the Cluster Head (CH) and secondary CH were selected. The energy consumption and the remaining energy available during the cluster formation were measured effectively. The lifetime improvement, fault discovery and recovery were the major constraints in effective communication. Paradkar et al. [16] applied the grad diffusion and genetic algorithms to find the lost node information and the recover the routing path effectively. The time-out mechanism was used to detect the hard faults effectively. The dissemination of all diagnostic information was the major requirement to assure the global view of fault status of WSN. Mahapatro and Khilar [17] assumed the cluster-based routing mechanism where the nodes were organized into one-hop clusters. The spanning tree construction spanned all the CHs

disseminated the local diagnostics effectively. The binary variable was employed for distributed fault detection. When the event was detected, the binary variable assigned to be 1 and it was 0 for the undetected events. Ould-Ahmed-Vall et al. [18] proposed the new approach which considered the different failure probabilities, drift overtimes, and calibration related failures in different accuracy levels. High spatial correlation was the major requirement to analyze the failure conditions. With the increase in number of sensors, the failure in sensor nodes also increased drastically. Lo et al. [19] presented the distributed, reference free fault detection mechanism on the basis of the local pair-wise verification between the sensors. Based on the relationship, the faulty nodes were detected. The decentralized fashion based fault detection mechanism ensured the energy saving capability effectively. Research studies turned their works into energy-aware distributed fault tolerant topology control algorithm namely Adaptive Disjoint Path Vector (ADPV). Deniz et al. [20] ensured the secure super connectivity among the nodes through the ADPV algorithm. The ADPV comprised the two phases such as single initialization and restoration. They obtained the two-fold increase of super connectivity among the nodes compared to the conventional DPV algorithm. Ding et al. [21] proposed the Multi-Particle Swarm Immune Cooperative Algorithm (MPSICA) to provide the intelligent route discovery and improve the fault tolerant capability. Lau et al. [22] proposed the Centralized Naïve Bayes Detector (CNBD) that analyzed the end-to-end transmission time and collected the necessary information. The minimum power burden to the battery of each sensor nodes was achieved. Chanak and Banerjee [23] performed Fuzzy-rule formation for the fault detection and uncertainties prediction that provided high effectiveness in fault recovery.

Hamiltonian Path Based Hyper Cube for Route Discovery

This section discusses the implementation of proposed Hamiltonian Path based Hyper Cube (HPHC) for the routing path estimation to deliver the data to the sink node by avoiding the node and link failures. The routing path comprises the set of tiny immediate sensor nodes to accept the data from the source node and forward them to sink node through the number of neighbor nodes. The failures in node and link level cause the disruption in communication. The failure report to the base station creates as many as routing requests and retransmissions that cause the overhead and time complexity. Besides, the energy consumed by the sensor nodes is increased due to the following factors:

- Communication in failure path.
- No. of retransmissions due to the node/link failures.

To alleviate these issues, this paper focuses on the fault-free communication among the nodes under node and link failures. The proposed work namely HPHC constructs the hyper cube structure on the basis of the Hamiltonian path with the Harmony search algorithm. Figure 1 shows the workflow of proposed HPHC in WSN applications. Initially, the WSN environment is constructed with the number of sensor nodes and base station on the suitable locations. The presence of faulty nodes violates the link and affects the communication adversely. The failures observed during the data transmission are observed in node and link levels. In node level, the sequential measurements such as Received Signal Strength Indicator (RSSI), velocity and relative velocity are performed.

Background: Ad-hoc on demand vector

With the infrastructure less and the existence of unreliable links, the routing of data to the sink node induces the energy saving requirements. The scarcity in energy consumption and the kept of sensors in operational stages throughout the simulation period are the major issues to be considered during the development of routing protocols. The manual assignment of unique identifiers unique identifiers is infeasible. The utilization of potentially unique identifier through the MAC address and GPS coordinates increase the payload in the messages. To alleviate these issues, the Ad-hoc On Demand Vector (AODV) [16] is used as the background framework for the proposed cube structure.

The set of tables is maintained in the AODV is used to find the information regarding the paths available, position, energy and speed. When a node wishes to transmit the message (source node) to the other node, it initiates the route discovery process to identify the location of destination node. The source node floods the query packet to all the nodes in the network. The acknowledgement reply from the node to the source node is responsible for the creation of route between them. Once the route request (RREQ) is initiated, the intermediate nodes update their routing table during forward and reverse route. Figure 2 shows the AODV workflow among the source (S) and destination (D) nodes.

Initially, the AODV utilizes the sequence numbers to determine

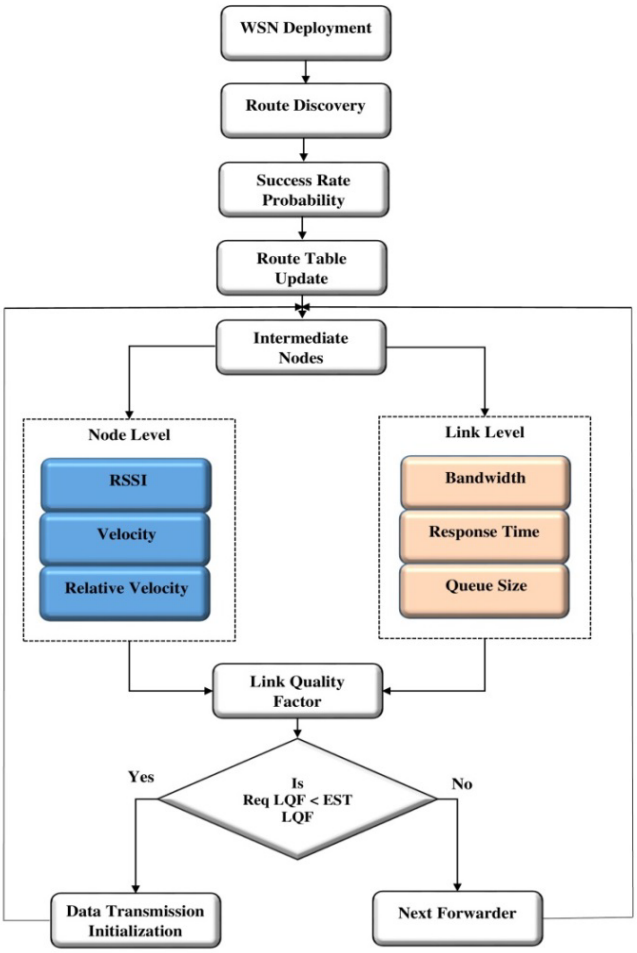


Figure 1: Workflow of HPHC scheme for faults tolerant WSN. In the link level, the bandwidth, response time and the queue size are computed. Based on these measurements, the Link Quality Factor (LQF) is computed. If the estimated LQF is less than the actual LQF, then the data transmission is initiated. Otherwise, the next forwarder is selected and the controller is transferred to the intermediate nodes.

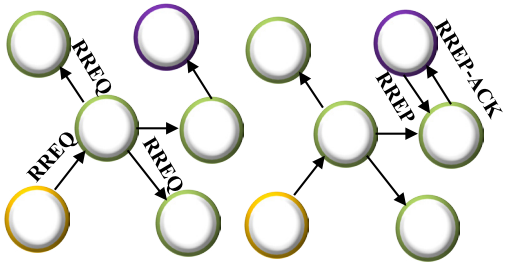


Figure 2: AODV implementation.

the timeliness of each packet with the avoidance of loops. The kept of all the routes is fresh with the help of expiry timers. The maintenance of advantages of fundamental distance vector routing components with the evaluation philosophy to check the operation. The addition of malicious node to the AODV will induce the fault model (failure scenario) in WSN formation. The node which is declared as malicious node drop out the packets during the communication. The steps modified in the AODV protocol in this paper are listed as follows:

1. Initialize the malicious variable with the value 'false' and this declaration inside the constructor is listed as follows:

AODV::AODV(nsadrr_t id):Agent(PT_AODV)…

{

…..

Malicious=false;

}

2. The TCL script is updated as follows

If (strcmp(argv (1) "malicious")==0)

{

Malicious-true;

Return TCL-OK

}

3. Then, implement the behavior of node on the basis of the rt_ resolve function used in AODv protocol.

If (malicious==true)

{

drop (p_DROP_RTR_ROUTE Loop)

}

With these modifications, the AODV is selected in this paper and integrate with the Hamiltonian path to estimate the relevant path for data transmission and minimum energy communications.

Hamiltonian path estimation

The number of tiny sensor nodes deployed in WSN environment has the capability to collect the information about the zone of interest and track the target over the specific region to deliver the services. The major tasks performed in WSN are sensing and transmission. The fault node present in the network affects the sensing and transmission tasks. The failures observed in WSN model are categorized into two levels as follows:

Node Level: The failures occurred in node level are caused either by hardware (sensing unit, CPU, memory, network interface and battery etc.) or software (routing, MAC and application) malfunctioning. If the battery energy falls below the level, the sensing unit provides the incorrect reading that leads to improper data acquisition. The major fault tolerance solution is to implement the any mechanism that minimizes the energy consumption and improves the network lifetime. During the node failure conditions, the RSSI, velocity and relative velocity are measured respectively.

Link level: The interferences between the WSN nodes and the packet collisions lead to loss of transmitted data. The paths built by the routing protocol lead to the dropping and loss in transmission data. During the selection of routes, the routing protocol considers the requirements of applications. During the link failure conditions, the bandwidth, queue size and response time are estimated accordingly.

In both cases, the occupation of data packets in the queue within the frame length limits the link capacity. Then, the time required for the data forwarding and the acknowledgement is more. The existence of obstacles among the sender and receiver nodes makes the RSSI as unsuitable for link formation. The ratio of difference between the total queue size and occupied queue size to the frame length is referred as queue size (Qs) and it is formulated as follows:

$$Qs = \frac{Total\ \text{Queue size - Occupied Queue size}}{Frame\ \text{length}} \quad (1)$$

Then, the mathematical formulation of response time is expressed as follows:

$$Rt_i = \left(T_{DR} - T_{DDT}\right) + \left(T_{ACKT} - T_{ACKDR}\right) \quad (2)$$

Where, T_{DR}–Time of data packet accumulated in queue of received port.

T_{DDT}–Time of data removed from the queue of transmission port.

T_{ACKT}–Time of acknowledgement packet accumulated in transmission port.

T_{ACKDR}–Time of acknowledgement packet removed from receiver port.

In the minimal energy consumption mode, the RSSI value is estimated in this paper. The distance between the nodes is calculated using a constant value 'k' and power required for transmission/ reception (Pt, Pr) as follows:

$$d = \sqrt[4]{k.Pt/\Pr} \quad (3)$$

Relative velocity is calculated by:

$$\overline{v} = \Delta d/\Delta t \quad (4)$$

Finally, the LQF is estimated with the above formulations as follows:

$$LQF\left(S,D\right) = \sum_{i=0}^{n}\left(QS_i + Rt_i + BW_i\right) \quad (5)$$

With the above formulation, the quality factor of each link is estimated. If the estimated value is less than the required value, then the transmission is initiated. Otherwise the next forwarder is selected on the basis of Hamiltonian fault-free path estimation [24]. The algorithm used to estimate the path between the nodes is described as follows:

Hamiltonian path

Input: Number of nodes (n), Location n(x, y), Node Failure Rate (NFR) (Z)
Output: Fault free path

Step 1: Deployment of sensor nodes in field of in range 1000 X 1000
Step 2: Placing the Base Station in Center of Region (Mid (Rx, Ry))
Step 3: Calculate distance between the neighbor nodes to reach the base station

$$D=\sqrt{\left(X_i-X_j\right)^2+\left(Y_i-Y_j\right)^2}$$

Step 4: if (D < TxRange200) Then ALM (i, j) =1 //Adjacency Link Matrix (ALM)
Step 5: Calculate the Node Failure Rate *NFR(i, j)=((Z$_i$)+(Z$_j$))/2*
Step 6: Find the intermediate hop by hop node estimation (Xi, NFR(i, j))
// To Choose hop by hop high reliable node in path
Step 7: Create Graph using the Node as edges and calculated NFR value as vertices
Step 8: Use Hamiltonian Path A utility function to check if the vertex v can be added at index 'pos' in the Hamiltonian Cycle constructed so far (stored in 'path[]')

The interconnection among the nodes in WSN is modelled as the simple graph [25] called G=(V, E) which contains set of edges (E) and nodes (V). The travelling cycle in which each node in the graph G traverses exactly once refers the Hamiltonian cycle and such type of graph refers Hamiltonian. The faulty nodes (f_v) and edges (f_e) are referred as the faulty set (f). Then, the graph is said to be fault-free only if the set f is not equal to 0. The Hyper cube (HQ) construction through the Hamiltonian formulation isolates the faulty set from the normal set effectively. The node is labeled with the unique n-bit string as its address and is adjacent to the n distinct nodes. The adjacency or neighbor nodes modeling are performed by n-dimensional HQ with the complementary in bits. Let us consider the two four dimensional HQs namely 0-HQ$_n$ and 1-HQ$_n$ as shown in Figure 3.

The set of crossing edges in the hyper cube is described as:

$$E^c=\left\{(x,y)\middle|(x,y)\in E\left(HQ_{n+1}\right),x\in HQ_n^0\ and\ y\in HQ_n^1\right\} \quad (6)$$

Where, x, y–Arbitrary nodes in hyper cube.

If the arbitrary nodes are located in the same hyper cube, then the first Hamiltonian path (p) and cycle (c) are constructed. By merging of path and cycle, the fault-free Hamiltonian path is constructed. The major characteristics of the fault free Hamiltonian path are described as follows:

- Hamiltonian path is present in HQ1.
- Fault free Hamiltonian path is described as HQ$_2$-f, where, *F* defines only one faulty node and edge.
- Fault-free Hamiltonian path in HQ_3-*f, Where* $f \le 2$.
- Fault-free Hamiltonian path HQ_{n+1} *with* $f_v+f_c \le n$.

With the above characteristics, the fault-free path is selected to provide the effective communication among the nodes in WSN.

Recursive hyper cube network

The popular technology in nowadays is the interconnection of the nodes in communication is hypercube network. The one-dimensional hypercube network is modeled as the graph with two vertices (v_0, v_1) with the following conditions [26]:

- Vertex set $V=v_0 U v_1$.
- The matched edge set M ⊏ E(G).

The hypercube network is initialized with the vertices and matched edges as follows:

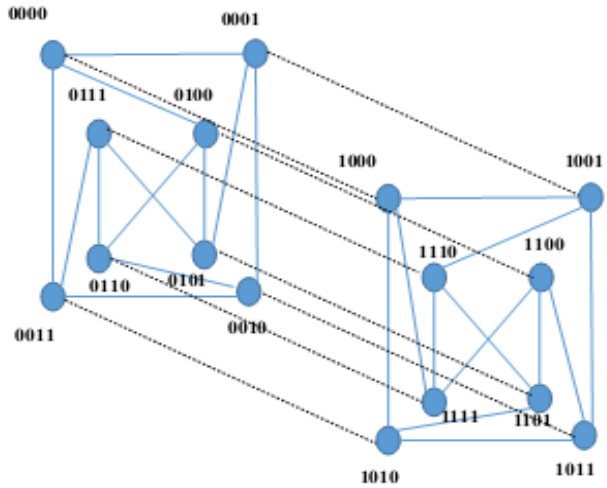
$$HQ_n=(v_0 \cup v_1, E_0 \cup E_1 \cup M) \quad (7)$$

The position of the network is extracted with the place including high LQF. The additional vertex added to the Hamiltonian cycle by using the following algorithm.

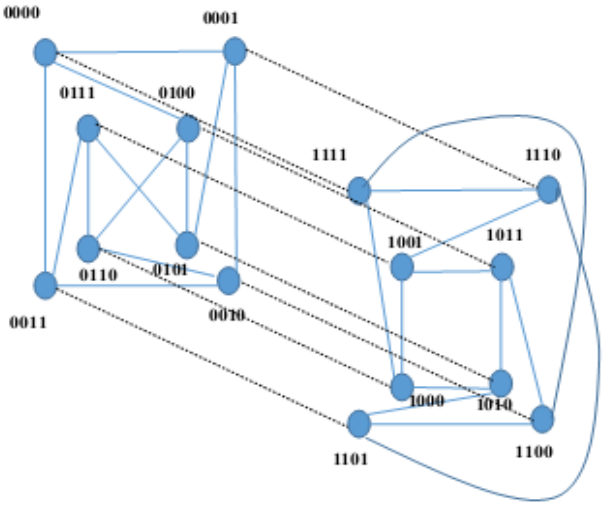
Addition of vertex to Hamiltonian cycle

For each vertex
If (safe(v, G, P, pos)
Path[pos]=v; // Recursive process to construct the fault-free path
If(HamcycleUtil((G, P, pos+1)==true)
Return true;
If(added v does not lead to the solution)
P(pos)=-1;
Endif
End For

During the demanding conditions, the Hamiltonian path is formed on the basis of hypercube network construction in the previous section. During the communication, some of the nodes or links underwent the failure that leads to the disruption in communication. The node



(a)



(b)

Figure 3: Four dimensional HQs (a) 0 – HQ_n and (b) 1 – HQ_n.

failure rate estimation through the adjacency link matrix provides the necessary background information. Initially, the set of neighbor nodes is initialized with zero. The availability of elements (channels) for the transmission node during the run time defines the cardinality. The algorithm to compute the matched edge is expressed as follows:

Cardinality-based Matched Edge set prediction

For each secondary node (N_i) //i=1, 2, …n

Set the neighbor set as null Ni={0}

For each cardinal value (N_j) //j=1,2, …, Nn)

Send(Hello, Sj) //Sj–Neighbor of Si

If Si receives (RREP, Sj)

Ni=Ni$\cup${Sj}

End For

End For

For k=1, 2, …, Nn

For l=1, 2, …, Ch // Ch-Channels

Sense (ch_k, l)

If (ch_k, l==True)

Add the channel to ALM

End If

End For

End For

For each node, the number of secondary nodes on the path (P) is extracted. For each secondary node, the routing request (RREQ) and the reply (RREP) are communicated in between the source and destination nodes as per AODV. Then, the cardinality values for the particular node are estimated. The channels available at the time are selected for transmission.

Performance Analysis

This section presents the performance analysis of the proposed HPHC-based fault-free path prediction for an efficient WSN communication. We utilize the Network Simulator-2 (NS-2) and MATLAB to model the fault model and the cardinality-based fault-free path estimation respectively. Besides, the performance of proposed HPHC is compared with the existing works such as FDWSN, PFDWSN and FNCM [23] regarding the various parameters such as throughput, faulty node detection accuracy, Packet Delivery ratio (PDR) and end-to-end delay. The message overhead, end-to-end delay and the PDR values are estimated with the variations of faulty nodes and no fault condition. The simulation configuration parameters for proposed work implementation are listed in Table 1.

Packet delivery ratio

The measure of the sum of packets received by the destination to the sum of packets generated is referred as packet delivery ratio.

$$PDR = \frac{\text{Sum of packets received by the destination}}{\text{Sum of packets generarted in the source}} \quad (8)$$

This section investigates the effect of proposed HPHC on PDR values with respect to minimum and maximum simulation periods.

Figure 4 graphically illustrates the PDR variations with respect to the simulation period values. For minimum simulation period (10 ms), the PDR value of HPHC is 90.58% for the absence of fault and 58.9% for 50 faulty nodes. Similarly, the PDR values are 94.96 and 66.60% for maximum simulation period (100 ms). The utilization Hamiltonian formulation and hypercube network maintained the PDR value in stable level.

Figure 5 shows the PDR variations corresponding to the linear increase of number of nodes from 25 to 200. In existing methods, the FDWSN offers 89.89 and 91.12% PDR which are more compared to the existing PFDWSN for 25 and 200 nodes respectively. But, the cube structure extension increases the PDR values to 92.715% for maximum nodes (200). The comparative analysis of proposed HPHC with the PFDWSN shows that the HPHC offers 1.72% improvement due to the cube extension.

End-to-end delay

The end-to-end delay of the packet is the time it takes to reach the destination and it depends on the number of components as follows:

$$delay_{E\text{-}E}=N_L(delay_{TX}+delay_{prop}+delay_{process}+delay_{queue}) \quad (9)$$

Parameters	Values
Number of nodes	200
Topology size	1000 × 1000 m^2
Data packet size	800 bits
Data aggregation energy	5 nJ/bit/signal
BS location	x=150, y=160
Duration of round	20 s
Initial energy	0.5 J
Sensing range	10 m
Frame/second	5 frame
Threshold transmission range	200 m
Control packet size	80 bits
TTL control packet	3
Stand-by node energy consumption	15 mW
Round time	20 s
MAC header	68 bits

Table 1: Simulation parameters.

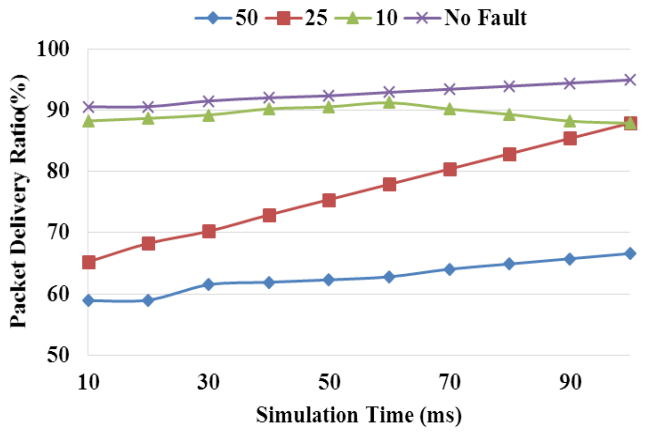


Figure 4: Packet delivery ratio under faulty nodes.

Where, N_L–Number of links;

$delay_{TX}$–Transmission delay (BW/L);

$delay_{prop-}$Propagation delay;

$delay_{process}$–Processing delay;

$delay_{queue}$–Queuing delay.

The parameters that affect the end-to-end delay are bandwidth and packet length (bits). Besides, the parameters that affect the propagation delay are congestion level, physical link length and speed respectively. Hence, the preservation of link is the major requirement to reduce the end-to-end delay.

Figure 6 graphically illustrates the end-to-end delay variations with the linear increase of number of nodes from 25 to 200 nodes. For 25 nodes, the end-to-end delay value for PFDWSN is minimum like 25 ms and it is 37.02 ms for 200 nodes. The delay values for proposed HPHC are 25.18 and 28.28 ms for 25 and 200 nodes respectively. The comparative analysis between the proposed HPHC with the PFDWSN shows the 23.61% reduction in end-to-end delay values.

Figure 7 shows the end-to-end delay variations with respect to the absence and presence of faulty nodes respectively. For minimum simulation period (10 ms), the end-to-end delay value of HPHC is 0.0263 ms for the absence of fault and 0.0496 ms for 50 faulty nodes. Similarly, the delay values are 0.06096 and 0.10275 ms for maximum simulation period (100 ms). The utilization Hamiltonian formulation and hypercube network linearly increases the time consumption.

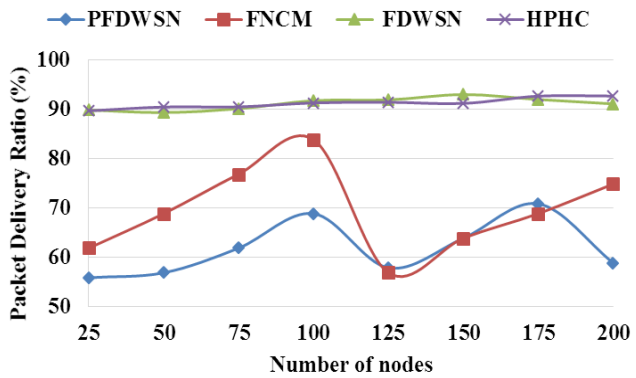


Figure 5: Packet delivery ratio analysis.

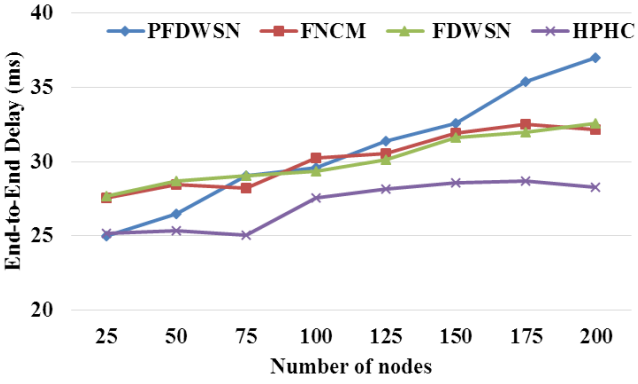


Figure 6: End-to-end delay analysis.

Faulty node detection rate

The faulty node detection rate is defined as the ratio of the number of faulty sensor nodes detected to the total number of faulty nodes available in the network. Figure 8 graphically presents the faulty node detection rate variations with respect to the minimum and maximum number of nodes like 10 and 100 nodes. For minimum number of nodes (10), the faulty node detection rate for proposed HPHC is 1 and it is linearly decreased to 0.51 ms for 100 nodes. The existing FNCM offers 0.2655 and 0.12 ms for 10 and 100 nodes respectively. The comparative analysis between the proposed HPHC with the existing FNCM shows that the HPHC offers 73.45 and 76.47% reduction in end-to-end delay values respectively compared to the existing FNCM method.

Throughput

The number of data packets sent over the total simulation period refers throughput. The mathematical formulation for throughput is expressed as:

$$\text{Throughput} = \frac{\text{Number of data packets sent (bits)}}{\text{Time period (secs)}} \quad (10)$$

In this section, the percentage of throughput is investigated corresponding to the number of nodes variation. Figure 9 shows the graphical variations of throughput with respect to the variation in simulation period from 10 to 100 ms. The percentage throughput values corresponding to HPHC are 96.63 and 98.62% for 10 and 100 ms respectively. Similarly, the percentage values corresponding to FDWSN are 93.61 and 93.14% respectively. The comparative analysis between the proposed HPHC with the existing FDWSN shows that

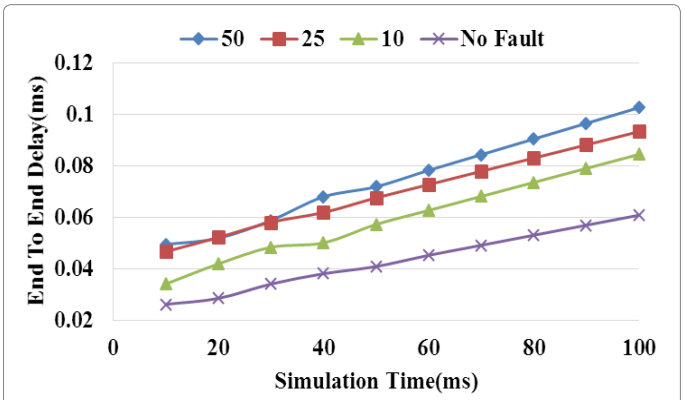


Figure 7: End-to-end delay analysis under faulty nodes.

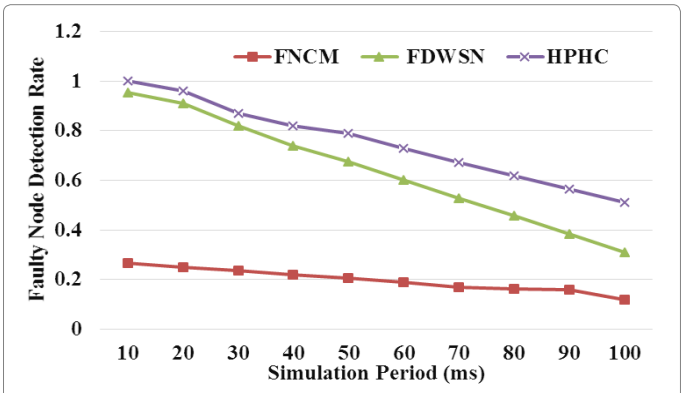


Figure 8: Fault node detection rate analysis.

the HPHC offers 3.13 and 5.56% improvement with respect to the simulation time values.

Average message overhead

Under the delay constraint, the ratio of the size of control packets to the total number of data packets successfully transmitted to the destination refers routing overhead. The analysis of control packet flow for minimum and maximum simulation periods of 10 and 100 ms.

The average message overhead for minimum (10) and maximum simulation period values (100 ms) are 0.57 and 1 under the absence of fault nodes.

The link preservation and the quality factor update through Hamiltonian cube formulation increase the overhead values to 2.3659 and 3.2189 respectively which are the acceptable levels. The cube extension-based link preservation in proposed work efficiently overcomes the fault scenario.

Conclusion and Future Work

Due to the battery-operated sensors, the recharge and replace mechanisms, the WSN suffered from the energy conservation and minimum network lifetime. The identification of fault nodes on the transmission path played the major role in energy conservation. With the dense deployment of sensor nodes, the failures in node and link are high that disrupted the entire communication. This paper proposed the suitable alternative fault-free path prediction model to perform the communication among the nodes. Initially, the sensor nodes are deployed in the WSN environment. Once the initialization of source and destination nodes are over, the path between them is predicted through the Hamiltonian path prediction model. During the failure scenario, this paper estimated the node and link parameters such as RSSI, queue size, response time, and bandwidth are individually estimated and group them into the QF. Based on the QF, the proposed work predicts the fault-free link to alleviate the unnecessary transmissions to the fault node and reduced the energy consumption. The comparison between the proposed HPHC network with the existing fault detection mechanisms regarding the performance measures such as Packet Delivery ratio (PDR), fault node detection rate, throughput and end-to-end delay assured the effectiveness of HPHC in WSN communication. The major focus of this paper to identify the fault-free path after the faults occurred (Figure 10). The occurrence of faults lies in two ways such as self and external. The prevention of external faults and the spreading of internal faults to other node will be considered as the future work to improve the communication performance.

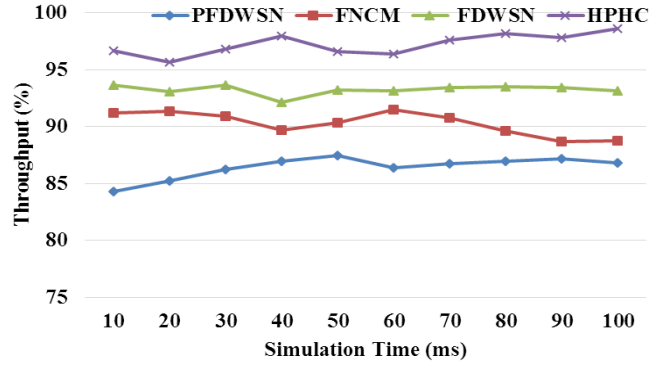


Figure 9: Throughput analysis.

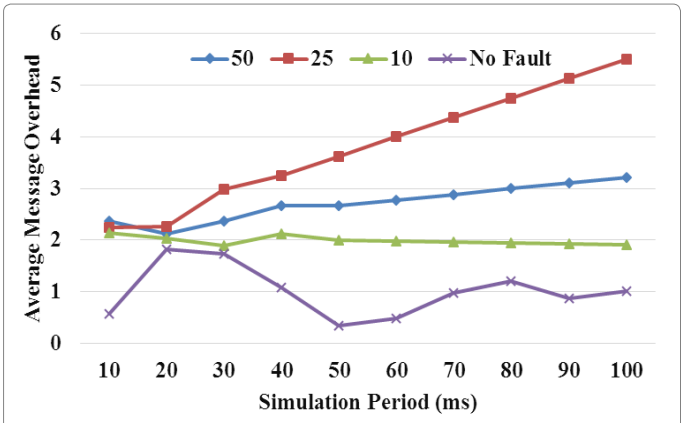


Figure 10: Control packet overflow analysis.

References

1. Halim T, Islam MR (2012) A study on the security issues in WSN. Int J Comput Appl T 53.
2. Sha K, Gehlot J, Greve R (2013) Multipath routing techniques in wireless sensor networks: A survey. Wireless Pers Commun pp: 1-23.
3. Sathish S, Ramesh L, Kumar SG (2014) A survey on node recovery from a failure in wireless sensor networks. Int J Adv Res Comp Sci Technol 2: 158-161.
4. Pasqualetti F, Bicchi A, Bullo F (2012) Consensus computation in unreliable networks: A system theoretic approach. IEEE Transactions on Automatic Control 57: 90-104.
5. Sharanapriya RP (2014) Design and implementation of dead nodes recovery algorithm to improve the life time of a wireless sensor network. Int J Sci Res 3: 1419-1422.
6. Hashemi SE, Motameni H, Ghaleh MR, Esmaeili S (2013) Clustering and routing wireless sensor network based on the parameters of distance, density, energy and traffic with the help of fuzzy logic. Int J Comput Sci Issues 10: 9-14.
7. Bianchin G, Cenedese A, Luvisotto M, Michieletto G (2015) Distributed fault detection in sensor networks via clustering and consensus: In Decision and Control (CDC). IEEE 54th Annual Conference pp: 3828-3833.
8. Re GL, Milazzo F, Ortolani M (2012) A distributed Bayesian approach to fault detection in sensor networks via Global Communications Conference (GLOBECOM). IEEE pp: 634-639.
9. Jain AGS (2014) Routing Techniques in wireless sensor networks. Int J Comput Appl 94: 15-20.
10. Chouikhi S, El Korbi I, Ghamri-Doudane Y, Saidane LA (2015) A survey on fault tolerance in small and large scale wireless sensor networks. Comput Commun 69: 22-37.
11. Bao F, Chen R, Chang M, Cho JH (2012) Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Transactions on Network and Service Management 9: 169-183.
12. Duche RN, Sarwade NP (2012) Sensor node failure or malfunctioning detection in wireless sensor network. ACEEE Int J Commun 3: 57-61.
13. Duche RN, Sarwade NP (2014) Sensor node failure detection based on round trip delay and paths in WSNs. IEEE Sensors J 14: 455-464.
14. Lee MH, Choi YH (2008) Fault detection of wireless sensor networks. Comput Commun 31: 3469-3475.
15. Akbari A, Dana A, Khademzadeh A, Beikmahdavi N (2011) Fault detection and recovery in wireless sensor network using clustering. IJWMN 3: 130-138.
16. Paradkar V, Chandel GS, Patidar K (2015) Fault Node Discovery and Efficient Route Repairing Algorithm for Wireless Sensor Network. IJCSIT 6: 1710-1715.
17. Mahapatro A, Khilar PM (2013) Energy-efficient distributed approach for clustering-based fault detection and diagnosis in image sensor networks. IET Wireless Sensor Systems 3: 26-36.

18. Ould-Ahmed-Vall E, Ferri BH, Riley GF (2012) Distributed fault-tolerance for event detection using heterogeneous wireless sensor networks. IEEE Transactions on Mobile Computing 11: 1994-2007.

19. Lo C, Lynch JP, Liu M (2013) Distributed reference-free fault detection method for autonomous wireless sensor networks. IEEE Sensors J 13: 2009-2019.

20. Deniz F, Bagci H, Korpeoglu I, Yazıcı A (2016) An adaptive, energy-aware and distributed fault-tolerant topology-control algorithm for heterogeneous wireless sensor networks. Ad Hoc Networks 44: 104-117.

21. Ding Y, Hu Y, Hao K, Cheng L (2015) MPSICA: An intelligent routing recovery scheme for heterogeneous wireless sensor networks. Inf Sci 308: 49-60.

22. Lau Bc, Ma EW, Chow TW (2014) Probabilistic fault detector for wireless sensor network. Expert Systems with Applications 41: 3703-3711.

23. Chanak P, Banerjee I (2016) Fuzzy rule-based faulty node classification and management scheme for large scale wireless sensor networks. Expert Systems with Applications 45: 307-321.

24. Hsieh SY, Chang NW (2006) Hamiltonian path embedding and pancyclicity on the Mobius cube with faulty nodes and faulty edges. IEEE Transactions on Computers 55: 854-863.

25. Cheng CW, Hsieh SY (2016) Edge-fault-tolerant pancyclicity and bipancyclicity of Cartesian product graphs with faulty edges. J Comput Syst Sci 82: 767-781.

26. Lai PL (2012) A systematic algorithm for identifying faults on hypercube-like networks under the comparison model. IEEE Transactions on Reliability 61: 452-459.