Efficient Packet Delivery for Reliable Multi-Path Routing

R.P.Mahesh[1],Dr. S.Chidambaranathan[2]
[1] Research Scholar, Manonmaniam Sundaranar University, Abishekapatti,Tirunelveli,Tamilnadu,India
[2] Department of MCA, St.Xavier College,Palayankottai ,Tamilnadu , India
Corresponding author: R.P.Mahesh

Abstract: The modern research has discovered a assortment of applications and systems with tremendously shifting requirements and characteristics in Wireless Networks (WNs). WNs are an accumulation of nodes imparting through wireless channels without any existing network infrastructure or centralized administration. The high versatility of nodes in WNs makes it hard to keep up a deterministic route. It is discovered that link insecurity can be a major issue for unreliable data delivery. The quality of the path and link quality of the node are the significant reasons for unintentional node failure in WN. The aim of this paper is to propose a novel routing protocol for WN communication which decreases the route failure during transmission. So the proposed routing protocol considers these two parameters to choose the best deliverer node in the path. The reliable data communication is accomplished by transmitting information via the path selected by the proposed routing scheme.

Keywords*:* Reliable Routing, Wireless Network, Efficient Packet Delivery, Path Selection

I. Introduction

Now-a-days, wireless communication is one of the key technologies for empowering the typical activity of a Wireless Network (WN). It has been extensively contemplated for conventional wireless networks in the last couple of decades and significant advances have been gained in various parts of wireless communication.

At the physical layer, an assortment of regulation, synchronization, and antenna techniques have been intended for different network scenarios and applications. Whereas, at higher layers, efficient communication protocols have been created to address various networking issues, for example medium access control, routing QoS, and security. These correspondence techniques and protocols provide a rich innovative foundation for the design of wireless communication in WNs.

WN can be recognized from conventional wireless communication networks, for instance, cellular systems and mobile ad-hoc networks (MANET) have unique characteristics such as densely deployment of node, higher unreliability of sensor nodes, severe energy, computation, and storage constraints, which exhibit many new difficulties in the development and applications of WNs. Today, research has been carried out by the researchers and the research institutions to examine and beat the limitations of WNs and to solve the difficulties in the design and application issues.

In many wireless scenarios, however, the metric of genuine interest is not the transmission energy of individual packets, however the total operational dependability of the network. To dodge the annihilation of nodes due to exhaustion of their unreliable routing algorithms, they try to guarantee an equitable distribution of the transmission costs among the constituent nodes. It is anything but difficult to see that the two routing objectives can be mutually conflicting. The fundamental commitment of this paper is in demonstrating how unreliable routing protocols must not only be based on node specific parameters, but must also consider the link specific parameters (e.g. channel characteristics of the link) too, to build the operational reliability of the network.

The challenge in making a routing protocol for WNs is to design a single protocol that can adapt to the wide assortment of conditions that can be present in any WNs over time. The routing protocol must perform efficiently in unreliable environments in which nodes are stationary and bandwidth is not a limiting factor. However, the same protocol must still function efficiently

when the bandwidth available between nodes is low and the level of mobility and topology change is high. Most routing protocols incorporate at least some periodic behaviors, meaning that there are protocol operations that are performed regularly at some interval regardless of outside events. These periodic behaviors typically limit the ability of the protocols to adjust to unreliable environments.

In this section, a brief introduction among the WNs and its challenges are discussed. The section 2 examined about the literature review for the reliable environment routing in wireless networks. The WNs issues and difficulties in routing with reliable environment is portrayed in section 3. The section 4 depicts the proposed conspire for efficient unreliable environment routing. Then the paper concludes with the aspects of unreliable environment routing.

II Related Review

The network reliability problem has been widely studied for wired networks. For example, in [1] the author deals with the problem of measuring the reliability and availability of a wired network assuming hardware and software failures. The author gives an important insight about the state-space enumeration and the topology adaptation strategy when failures occur. The main difference between the reliability analysis of wired and wireless networks is related to the dynamics of the network. In a wireless networks, the dynamics of the network is greater since links fail more often and also due to the mobility of some of the devices. An early work about the reliability evaluation for a radio-broadcast network was conducted by [2]. In that work, the authors considered unreliable devices and reliable links and showed that the two-terminal reliability problem for radio broadcast networks is computationally difficult.

In [3], the authors analyzed the reliability and the expected maximum delay for a distributed sensor network. The network is assumed to be densed and organized into clusters. The reliability was measured as the probability that there was at least one path between the sink device and a sensor node within a cluster. The authors assumed unreliable devices and reliable links. It was proved that the problem was, in general, NP-hard. However for a topology up to 40 devices the problem is still tractable. In [4], the network reliability was evaluated for mobile ad-hoc networks based on the 2-terminal problem. The authors assumed unreliable devices and dynamic network connectivity. The proposed algorithm, although not finding the minimal cut set for the network, can be extended for the type of static networks typically found in industrial applications. In [5], the authors analyzed the influence of adding redundant devices, in what concerns the reliability and availability of multi-hop wireless networks. This work provides an interesting discussion about the reliability and availability of a WSN, particularly if it is considered that a router node can be a redundant device.

Another coverage-oriented reliability mechanism was proposed in [6]. The authors propose a framework to evaluate the reliability of a WSN based on coverage requirements. In a given area A, the network will fail if there is no subset of fully operating nodes whose own generated traffic can reach the sink and the total area covered by this subset is greater than A. The authors used a 3-state node reliability model to represent random failures in the devices. This model has been shown to work better over the conventional 2-state (operate/fail), but it neither supports the inclusion of spare devices nor indicates the criticality of the devices. Finally, creating several coverage areas makes it difficult to specify flexible failure conditions.

Another methodology for the reliability evaluation of a WSN was proposed in [7]. The authors propose a new topology control mechanism and they used a methodology for evaluating the reliability of the network operating with this mechanism. The basic idea is to represent the network as a graph and to measure the reliability based on the number of functional spanning trees. If there is at least one functional spanning tree, then the network is considered as reliable. The proposal is simple and works very well for the analysis of the topology control mechanism. However it is not suitable to evaluate arbitrary WSN. In [8], the authors developed a modeling methodology for automatic generation of fault trees. The idea is to split a system in different components

that are represented by function tables and state transition tables. These components are connected to each other in order to describe the behavior of the whole system. After the modeling phase, a trace-back algorithm is used to create the fault tree.

III. Design Issues and Challenges in Routing

Due to various wireless network constraints, the plan of routing protocols is very exceptionally for WNs. The network design issues for WNs, are energy, bandwidth, central processing unit, and storage [13][15]. The plan challenges in sensor networks involve the main viewpoints [13][14][15]:

- *Massive and Random Node Deployment:* Node deployment in WNs is application dependent and can be either manual or arbitrary which at long last influences the performance of the routing protocol. In many applications, nodes can be scattered arbitrarily in an intended area or dropped enormously area over an inaccessible or hostile region.
- *Unreliable Environments:* A network more often than not operates in a dynamic and unreliable environment. The topology of a network, which is defined by the communication links between the nodes, changes frequently due to node addition, deletion, node failures or harms. Likewise, the sensor nodes are linked by a wireless medium, which is noisy, error prone, and time differing. Therefore, routing paths should consider network topology dynamics due to limited node mobility as well as increasing the size of the network to keep up particular application requirements in terms of coverage and connectivity.
- *Limited Hardware Resources:* Nodes have also constrained processing and capacity limits, and thus can only perform limited computational functionalities. These hardware constraints present many difficulties in software development and network protocol design for WNs.

IV. Proposed Scheme

WNs are an infrastructure less multi-hop wireless network. In wireless communication, the nodes can communicate with each other only when they are accessible inside the communication range of each other, when the receiver is far away from the transmitter (Destination is out of range of the data toward the receiver). One of the salient features of WNs is that every node can reconfigure itself as router to forward the data packets with any centralized control.

The multi-hop path is found by using routing protocols in WNs. Routing protocols available for WNs communication should guarantee QoS in the dynamic environment. But the dynamic nature of WNs makes the task of providing QoS tedious. The reliable communication is accomplished by providing high QoS. The node-to-node channel quality changes powerfully which may influence the multi-hop data flows. The link quality also severely influences the multi-hop data streams.

In wireless communication, a node has the link with all the nodes accessible inside its communication range. When a node moves away from the communication range, the link between the two nodes will be terminated or broken. This may cause packet drop during transmission. The dynamic (mobility) nature of MANET causes link failure habitually. When a specific mobile node leaves the communication range of the existing node and at the same time it might create the link with a new node. This behavior of mobile node makes the way toward finding a reliable route monotonous task.

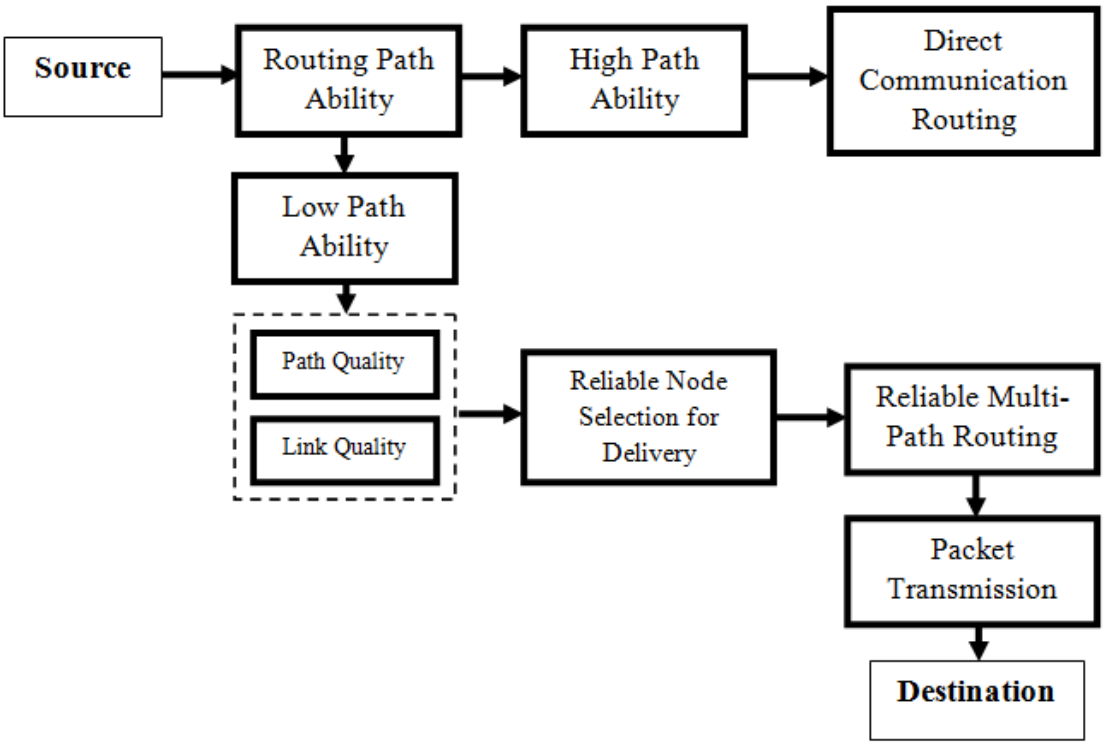

Figure 1: Architectural Design for Proposed Reliable Routing Scheme

In this paper, we propose a reliable routing scheme which selects the forwarder nodes between source and destination based on following two aspects is shown in Figure 1.

(a) Path Quality

In a communications path, an analysis that (a) incorporates the general assessment of the component quality measures, the individual link quality measures, and the aggregate path quality measures, and (b) is performed by assessing communications parameters, such as bit error ratio and packet delivery ratio.

(b) Link Quality

Link quality is assessed from the quality of the received signal. In this paper, another new link quality metric is presented. The time during which the link exists between the nodes (link remaining life) is taken to gauge the link quality. In the proposed scheme, the link quality measurement is used to diminish the route failure in the highly dynamic environment. As the exact depiction of wireless links in WNs is a monotonous task, a new metric link residual life can easily be estimated based on the communication range and the relative velocity between the nodes.

A. Reliable Multi-Path Routing

The source node gets the address of the destination from a location enlistment and lookup service. Then it connects destination's address to the packet header. On the off chance that the destination is within the source's transmission range, then the next hop is the destination. The packets are delivered directly and the routing process ends something else, neighbors are organized based on their link stability. The node which gains positive progress towards the destination and with the maximum power is considered as best deliverer.

Transmitted area is chosen as the overlapping area of the transmission range of the source and half of the transmission range of the best forwarder. Among the nodes inside this overlapping area zone, only those nodes which are nearer to the

destination than the source and which are more remote from the destination than the best forwarder, turn into the candidate nodes. A delivery table comprising of the source id, destination id, best deliverer id and the ids of candidate nodes is maintained by the source for a specific timeframe. The candidate list is appended to the packet header and the packet is broadcasted. The best deliverer and the candidate nodes reserve the packets.

B.Reliable Node Selection for Delivery

In WNs, the accidental route failure is due to path fading and link failure. In the node channel fading causes impedance in WNs. So the level of QoS will be decreased. The link failure in the WNs tends to reproduce the route. The continuous route reconstruction causes end-to-end delay and high routing overhead. The node turns out to be dead when the energy in the node is depleted. At the point when the node in the path is dead, the path ought to be remade. Subsequently, the proposed method diminishes route failure by considering path quality and link quality as the parameters to choose the reliable node in the path. The best deliverer with reliable routing illustrated with an example in Figure 2.

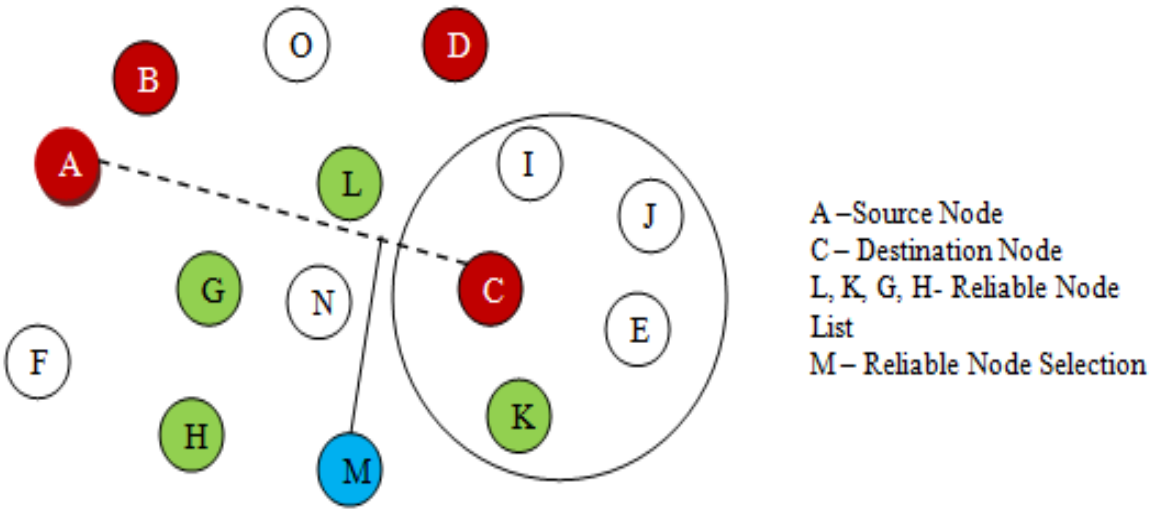

Figure 2: Best Deliverer with Reliable Node Selection for Efficient Packet Delivery

Algorithm BDRNS: Best Deliverer with Reliable Nodes Selection

{
Input: N_{Des} – Destination Node
N_{Source} – Source Node
L_{List} - Neighbour List
Output: $N_{Reliable}$ – Reliable Node
FindDes(N_{Des}) from L_{List}
If(N_{Des} == $L_{List}(N')$)
{
N_{Des} = NextHop(N_{Des})
}
Else
{
For each N' from L_{List}
{
//checking for link status for the destination

CheckLink($N^{'}$)
If(LinkStatus($N^{'}$) ==”active”
{
CheckDistance(N_{Des})
// verifying distance from destination to current node
If (Distance (N_{Des}) >= Distance ($N^{'}$))
{
Break the Chosen path
}
Else
{
A [] =AddNode($N^{'}$)
}
For each node n_1 from A[n]
{
If (Distance (n_1) <= Distance (N_{Des}, N_{Source}))
//Reliable Node Selection
$N_{Reliable}$= ReliableNode(n_1)
Else
ChooseNext(A[n])
}
}
Else // if the link status is passive
{
ChooseNextNode($N^{'}$, L_{List})
}
}
}
Return $N_{Reliable}$
}

The algorithmic representation of the proposed flow is depicted in the above algorithm. If no transmission is caught during this period, the candidate node understands that the best forwarder has failed. The forwarding task is then controlled by the candidate node. Every node that is a sender or a relay node maintains a forwarding table for the packets of each stream. The table entry has an expiry time within which a required transmission is to be finished. Consequently the overhead in developing and keeping up the forwarding table is significantly lesser compared with that of a traditional routing table shown in Table 1.

Source/Destination	Next Link Route	Reliable Node
A,C	K	L,M
B,D	C	G,H

Table 1: Reliable Routing Table

Communication holes may exist since nodes are not consistently conveyed. At this point, when the best forwarder looks for the following hop node and discovers none, a correspondence void is said to be experienced. The protocol at that point changes to a routing hole handling mechanism. When the excellent forwarder encounters a communication hole, it throws a void flag to the previous link. The past forwarder turns the trigger node and the best deliverer becomes the void node.

V. Performance Metrics

To describe the essential performance of the protocols, utilize a set of high-level summary metrics that are of important to network users. To comprehend the internal functioning of the protocols, different sets of metrics are utilized: some of which are

particular and depicted as required in the content, and some of which are general to all on-demand routing protocols and portrayed underneath. The accompanying three metrics capture the most basic overall performance and the other protocols to be actualized in this paper.

(a) Packet Delivery Ratio

The ratio between the number of packets originated by the application layer at the sources and the number of packets received by the node at the final destination.

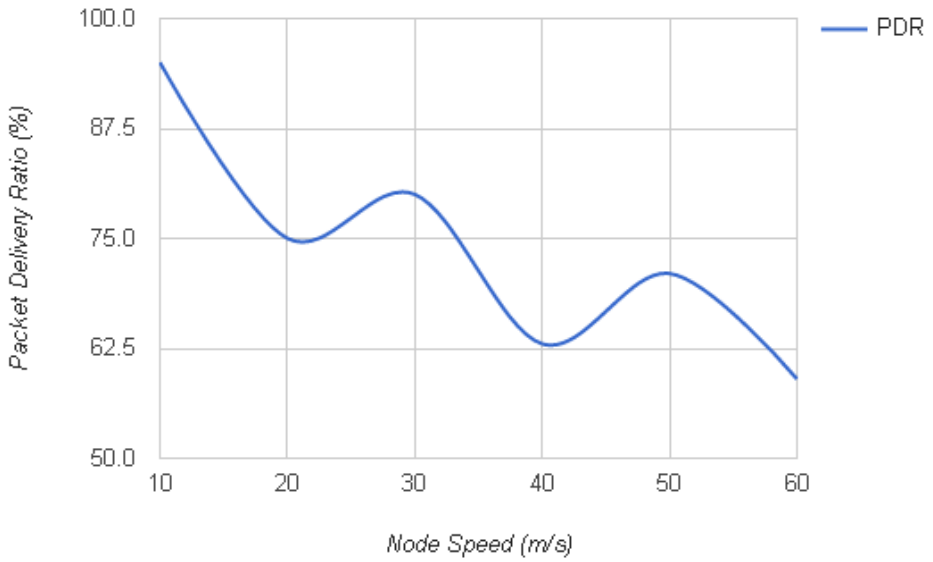

Figure 3: Packet Delivery Ratio Evaluation

The performance metrics of Packet Delivery Ratio (PDR) is evaluated and illustrated in Figure 3. The figure depicts that the system provides high PDR that assures reliable packet delivery.

(b) Routing Overhead

The total number of routing packets transmitted during the simulation. For packets sent over multiple hops, each transmission of the packet (each hop) is counted as one transmission. Routing packets are those that are originated by the routing protocol and do not also include user data. Protocols like DSR, incorporate both routing data and user data in the same packet. In this type of protocol, all the bytes of routing data in the packets are counted as routing overhead.

For packets sent over various hops, every transmission of the packet(each hop) is considered as one transmission. Routing packets are those that are started by the routing protocol and don't likewise incorporate user information.

(c) Path Optimality

The contrast among the quantity of hops a packet takes to achieve its destination and the length of the shortest path that physically existed via the network while the packet is begun. Packet delivery ratio is vital as it depicts the loss rate so as to be visible to transport protocols, which in turn influences the maximum throughput that the network can bolster. This metric portrays both the completeness and completeness of the routing protocol. Routing overhead is an essential metric for contrasting those

protocols, as it measures the versatility of a protocol, how much it's going to function in congested or low-transmission bandwidth environments, and its effectiveness is achieved using node battery power.

(d) Path Length

Path length describes average end-to-end number of hops for successful packet delivery.

Figure 4 illustrates that path length variation is found since the forwarder selection is not based on distance metric. Hence the hop count may not always be a minimal. This causes less end-to-end delay. The end-end delay is depicted in figure 5.

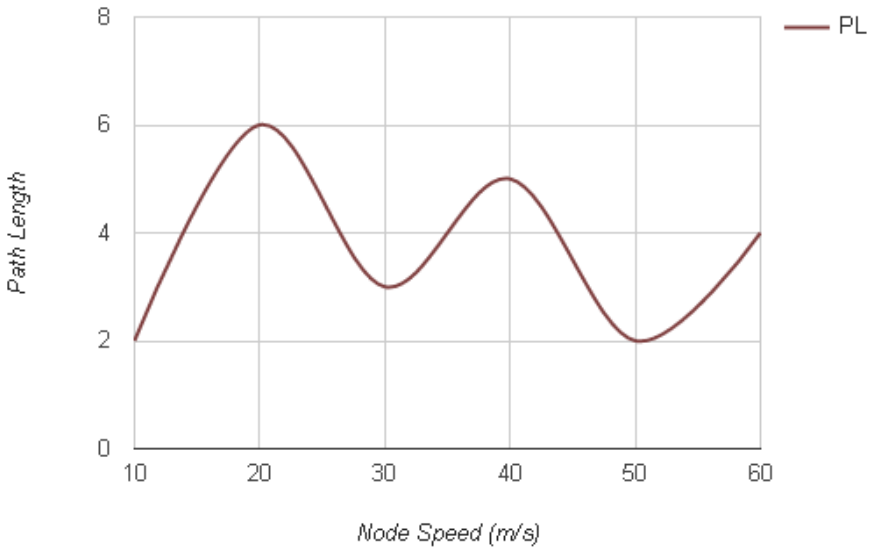

Figure 4: Path Length Evaluation

(e) End-to-end-delay

The time taken for a packet to be transmitted from the source to the destination.

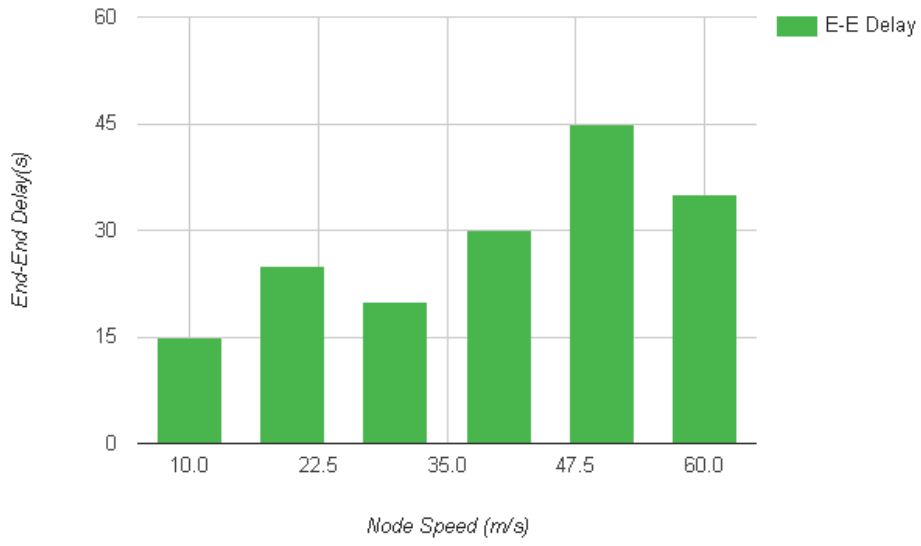

Figure 5: End-End Delay with respect to Path Length

(f) Packet forwarding times per packet (FTP)

The average number of times a packet is being forwarded to deliver a packet from the source to the destination

VI. Conclusion

This work is aggravated by the need of reliable route in the dynamic WNs. To facilitate the reliable communication in the highly dynamic environment of WNs, this paper proposes a novel routing protocol named as **Efficient Packet Delivery for Reliable Multi-Path Routing.**. This protocol used two important which reduces route failure in WNs while discovering the route on demand. The two parameters include path quality and link quality. The consideration of link quality during path discovery reduces the route failure during transmission. The consideration of path quality during route discovery process increases the overall system throughput. The consideration of reliable node selection during routing process will reduce the node failure during packet delivery.

References

[1] Hou, W. Integrated Reliability and Availability Analysis of Networks with Software Failures and Hardware Failures. Ph.D. Thesis, University of South Florida, Fowler Avenue Tampa, FL, USA, 2003.

[2] AboElFotoh, H.; Colbourn, C. Computing 2-terminal reliability for radio-broadcast networks. IEEE Trans. Reliab. 1989, 38, 538–555

[3] AboElFotoh, H.; Iyengar, S.; Chakrabarty, K. Computing reliability and message delay for cooperative wireless distributed sensor networks subject to random failures. IEEE Trans. Reliab. 2005, 54, 145–155.

[4] Kharbash, S.; Wang, W. Computing two-terminal reliability in mbile ad hoc networks. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’07), Kowloon, HongKong, 11–15 March 2007; pp. 2831–2836.

[5] Egeland, G.; Engelstad, P. The availability and reliability of wireless multi-hop networks with stochastic link failures. IEEE J. Sel. Areas Commun. 2009, 27, 1132–1146.

[6] AboElFotoh, H.; Shazly, M.; Elmallah, E.; Harms, J. On area coverage reliability of wireless sensor networks. In Proceedings of the 36th Annual IEEE Conference on Local Computer Networks (LCN ’11), Bonn, Germany, 4–7 October 2011; pp. 584–592.

[7] Qureshi, H.K.; Rizvi, S.; Saleem, M.; Khayam, S.A.; Rakocevic, V.; Rajarajan, M. Poly: A reliable and energy efficient topology control protocol for wireless sensor networks. Comput. Commun. 2011, 34, 1235–1242.

[8] Majdara, A.; Wakabayashi, T. Component-based modeling of systems for automated fault tree generation. Reliab. Eng. Syst. Saf. 2009, 94, 1076–1086.

[9] A. Trivino-Cabrera, S. Canadas-Hurtado, “Survey on Opportunistic Routing in Multihop Wireless Networks”, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 3, No. 2, August 2011

[10] Dazhi Chen, Pramod K. Varshney, “A Survey of void handling techniques for geographic routing in wireless networks”, IEEE communications survey, 1st Quarter, Vol.9, No. 1, 2007

[11] Luiz Carlos P. Albini, Antonio Caruso, Stefano Chessa and Piero Maestrini, “Reliable Routing in Wireless Ad Hoc Networks: The Virtual Routing Protocol”, Journal of Network and Systems Management, Vol 14, No. 3, 2006.

[12] Shengbo Yang, Chai Kiat Yeo, and Bu Sung Lee, “Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks”, IEEE Transactions on Mobile Computing, Vol. 11, No. 1, Jan 2012.

[13] Jamal Al-Karaki, and Ahmed E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey“, IEEE Communications Magazine, vol 11, no. 6, pp. 6-28, Dec. 2004.

[14] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[15] Kemal Akkaya and Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Ad hoc Networks, vol. 3, no. 3, pp. 325-349, May 2005.