STUDY OF ALGORITHM FOR VOID FREE ROUTING IN WIRELESS SENSOR NETWORKS

Laxmikant J. Goud[1], Dr. Neeraj Sharma[2]

[1]Laxmikant J. Goud, Research Scholar, Computer Science Engineering, SSSUTMS.
Dr. Neeraj Sharma[2], Professor, Computer Science Engineering, SSSUTMS.

ABSTRACT

In existing systems, energy holes are identified and removed from the network. A void node is referred to as a routing hole. Voids are identified in two steps in existing systems: a neighbor creation and a data routing phase. Existing systems detect voids based on the position of nodes. In our proposed approach, we identify voids, as well as clusters that expect voids. Void-free routing in WSNs has applications in health, defense and the IoT. Eliminating voids and improving the energy efficiency of the sensor is key to increasing the lifetime of the network. Sensor data in the cloud, as they relate to applications, are complex and call for enhanced security. Data retrieval from the cloud with less response time needs to be made.

Keyword: Downtime, Data Link Layer, Client, Transport Layer, Ethernet Network.

1. OVERVIEW

A wireless networking system would rid of the downtime you would normally have in a wired network due to cable problems. It would also save time and money due to the fact that you would spare the expense of installing a lot of cables. Also, if a client computer needs to relocate to another part of the office then all you need to do is move the machine with the wireless network card.

Wireless networking can prove to be very useful in public places – libraries, guest houses, hotels, cafeterias, and schools are all places where one might find wireless access to the Internet. From a financial point of view, this is beneficial to both the provider and the client. The provider would offer the service for a charge – probably on a pay per use system, and the client would be able to take advantage of this service in a convenient location; away from the office or home.

A drawback of wireless Internet is that the QoS (Quality of Service) is not guaranteed and if there is any interference with the link then the connection may be dropped.

1.1Task of different layer in wireless network

The physical layer must tackle the path loss, fading, and multi-user interference to maintain stable communication links between peers. The data link layer (DLL) must make the physical link reliable and resolve contention among unsynchronized users transmitting packets on shared channel. The latter task is performed by the medium access control (MAC) sub layer in the DLL. The network layer must track changes in the network topology and appropriately determine the best route to any desired destination. The transport layer must match the delay and packet loss characteristics specific to such a dynamic wireless network. Even the application layer needs to handle frequent disconnections.

1.2 Media access control

The media access control (MAC) data communication protocol sub-layer, also known as the medium access control, is a sub layer of the data link layer specified in the seven-layer OSI model. It provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. The hardware that implements the MAC is referred to as a medium access controller.

The MAC sub-layer acts as an interface between the logical link control (LLC) sub layer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

In 100Mbps and faster MACs, the MAC address is not actually handled in the MAC layer. Doing so would make it impossible to implement IP because the ARP layer of IP-Ethernet needs access to the MAC address.

Addressing mechanism.

In 100Mbps and faster Ethernet MACs, there is no required addressing mechanism. However, the MAC address inherited from the original MAC layer specification is used in many higher level protocols such as Internet Protocol (IP) over Ethernet.

The local network address used in IP-Ethernet is called MAC address because it historically was part of the MAC layer in early Ethernet implementations. The MAC layer's addressing mechanism is called physical address or MAC address. A MAC address is a unique serial number. Once a MAC address has been assigned to a particular network interface (typically at time of manufacture), that device should be uniquely identifiable amongst all other network devices in the world. This guarantees that each device in a network will have a different MAC address (analogous to a street address). This makes it possible for data packets to be delivered to a destination within a sub network, i.e. hosts interconnected by some combination of repeaters, hubs, bridges and switches, but not by IP routers. Thus, when an IP packet reaches its destination (sub) network, the destination IP address (a layer 3 or network layer concept) is resolved with the Address Resolution Protocol for IPv4 or by Neighbor Discovery Protocol (IPv6) into the MAC address (a layer 2 concept) of the destination host.

An example of a physical network is an Ethernet network, perhaps extended by wireless local area network (WLAN) access points and WLAN network adapters, since these share the same 48-bit MAC address hierarchy as Ethernet. A MAC layer is not required in full-duplex point-to-point communication, but address fields are included in some point-to-point protocols for compatibility reasons.

1.3 Channel access control mechanism

The channel access control mechanisms provided by the MAC layer are also known as a multiple access protocol. This makes it possible for several stations connected to the same physical medium to share it. Examples of shared physical media are bus networks, ring networks, hub networks, wireless networks and half-duplex point-to-point links. The multiple access protocol may detect or avoid data packet collisions if a packet mode contention based channel access method is used, or reserve resources to establish a logical channel if a circuit switched or channelization based channel access method is used. The channel access control mechanism relies on a physical layer multiplex scheme.

The most widespread multiple access protocol is the contention based CSMA/CD protocol used in Ethernet networks. This mechanism is only utilized within a network collision domain, for example an Ethernet bus network or a hub network. An Ethernet network may be divided into several collision domains, interconnected by bridges and switches.

A multiple access protocol is not required in a switched full-duplex network, such as today's switched Ethernet networks, but is often available in the equipment for compatibility reasons.

1.4 Geographic Position Aided Routing

The fundamental problems of routing in ad hoc networks arise due to the random movements of the nodes. Such movements make topological information stale, and hence, when an on-demand routing protocol needs to find the route, it often has to flood the entire network looking for the destination. One of the ways of reducing the wastage of bandwidth in transmitting route request packets to every node in the network is to confine the search using geographical location information. Geographical positioning systems (GPS) can detect the physical location of a terminal using universal satellite-transmitted wireless signals [24, 25, and 26]. In recent times, GPS have become smaller, more versatile, and more cost- effective. Hence, several protocols have been proposed that assume the presence of a GPS receiver in each node and utilize the location information in routing one of the approaches for utilizing geographic location information in routing is to forward data packets in the direction of the location of the destination node, as proposed in various references. It may be required to define geographic location–specific addresses instead of logical node addresses to do that.

An alternative concept is proposed in the Location Aided Routing (LAR) protocol, which uses location information in on-demand routing to limit the spread of request packets for route discoveries. LAR uses information such as the last known location and speed of movements of a destination to determine a REQUEST ZONE, which is defined as a restricted area within which the REQUEST packets are forwarded in order to find the destination. Two different ways of defining REQUEST ZONES have been proposed. The idea is to allow route request packets to be forwarded by only those nodes that lie within the REQUEST ZONE, specified by the source. This limits the overhead of routing packets for route discovery, which would normally be flooded over the whole network.

A related protocol that uses spatial locality based on hop counts to confine the spread of request packets was proposed by Castaneda and Das. This protocol uses the concept that once an existing route is broken, a new route can be determined within a certain distance (measured in number of hops) from the old route. The protocol confines the spread of route request packets while searching for a new route to replace one that is freshly broken. For a new route discovery where no earlier routes were on record, the protocol still uses traditional flooding. However, this query localization technique for rediscovering routes still saves routing overhead.

1.5 Stability-Based Routing

A different approach to improve the performance of routing in mobile ad hoc networks is based on using routes that are selected on the basis of their stability. The Associativity-Based Routing (ABR) [27] protocol maintains association stability metric that measures the duration of time for which a link has been stable. While discovering a new route, the protocol selects paths that have high aggregate-association stability. This is done with the idea that a long-lived link is likely to be stable for a longer interval than a link that has been relatively short-lived Signal Stability-Based Routing (SSR)[28] uses signal strengths to determine stable links. It allows the discrimination between “strong” and “weak” links when a route request packet is received by a node. The request packet is forwarded by the node if it has been received over a strong link. This allows the selection of routes that are expected to be stable for a longer time.

1.6 Multipath Routing

On-demand or reactive routing protocols suffer from the disadvantage that data packets cannot be transmitted until the route discovery is completed. This delay can be significant under heavy traffic conditions when the REQUEST or the REPLY packet may take a considerable amount of time in traversing its path. This characteristic, along with the fact that each route discovery process consumes additional bandwidth for the transmission of REQUEST and REPLY packets, motivates us to find ways to reduce the frequency of route discoveries in on-demand protocols. One way of doing that is to maintain multiple alternate routes between the same source-destination pair such that when the primary route breaks, the transmission of data packets can be switched over to the next available path in the memory. Under the assumption that multiple paths do not break at the same time, which is most often true if the paths are sufficiently disjoint, the source may delay a fresh route discovery if the alternate paths are usable. As a result, many routing protocols have been designed to maintain multiple paths or routes for each pair of source and destination nodes.

The Temporally Ordered Routing Algorithm (TORA) [29] provides multiple alternate paths by maintaining a “destination oriented” directed acyclic graph from the source. The DSR protocol also has an option of maintaining multiple routes for each destination in the route cache, so that an alternate route can be used upon failure of the primary route. Two multipath extensions of DSR were proposed by Nasipuri, Castaneda, and Das that aggressively determine multiple disjoint paths for each destination. Here, two different schemes for selecting alternative routes were considered, both benefiting from reducing the frequency of route discoveries caused by link breakages. Several other multipath routing protocols that derive benefits using the same principle have also been proposed.

1.7 Pre-emptive Routing

A purely reactive routing protocol typically does not avoid a multihop communication from being interrupted before the route breaks due to a link failure. Most reactive routing protocols initiate a fresh route discovery when an ERROR packet is received at the source due to a link breakage. This introduces a pause in the communication until a new route is found. The goal of pre-emptive routing protocols is to avoid such pauses by triggering a route discovery and switching to a new (and, it is hoped, better) route before the existing route breaks. Such protocols can be viewed as a combination of proactive and reactive routing, where the route maintenance is performed proactively but the basic routing framework is reactive. The crucial design issue in such protocols is to detect when to initiate a pre-emptive route discovery to find a “better” route. The protocol proposed by Goff and colleagues uses the technique of determining this by observing when the signal strength falls below a predetermined threshold. If the wireless channel is relatively static, then this correctly detects the initiation of link failure due to increasing distance between the two nodes in the link.

However, multipath fading and shadowing effects might lead to false alarms while using this technique. Alternatively, using a time-to-live parameter was proposed by Nasipuri [26] and colleagues. In this protocol, a pre-emptive route discovery is initiated when a route has been in use for a predetermined threshold of time. The pre-emption obviously makes the route discoveries more frequent than what would be observed in a purely reactive scheme. To keep the routing overhead low, the pre-emptive routing protocol use of query localization in the pre-emptive searches.

2. The Routing Protocols

The routing protocols are responsible for all aspects of end-to-end packet delivery, including logical message addressing and routing packets between different networks. The main goal of a routing technique is to efficiently deliver data from the source to the destination. Although all routing protocols share this goal, each protocol adopts a different approach to achieve it.

Routing paths for transmission of data packets from one node to another can be established in one of three ways, namely proactive, reactive or hybrid. In proactive routing [35], all the routes are computed in advance and maintain consistent up-to-date routing information from each node to every other node in the network. Every node in the network maintains one or more routing tables that store the routing information. This is also called table driven routing and is preferably used in the application where the sensor nodes are static. Proactive routing protocols periodically monitor the changes in the topology to ensure the ready availability of any path amongst active nodes. When a topology changes due to the failure of nodes, the change has to be propagated throughout the network as updates so that the network view remains consistent. The protocols vary in the number of routing tables maintained and the method by which the routing updates are propagated.

In reactive routing, routes are discovered only when desired. This means that protocols don't make the nodes initiate a route discovery process until a route to a destination is required. Route discovery can be initiated either by source or destination. Source-initiated routing means that it is the source node that begins the discovery process, while destination-initiated is the opposite. Once a route has been established, the route discovery process ends and a maintenance procedure preserve it until the route breaks down or is no longer desired. The main disadvantage of reactive protocol is that, significant amount of energy is expended in route discovery and setup. Hybrid routing combines characteristics of both reactive and proactive routing protocols to make routing more scalable and efficient.

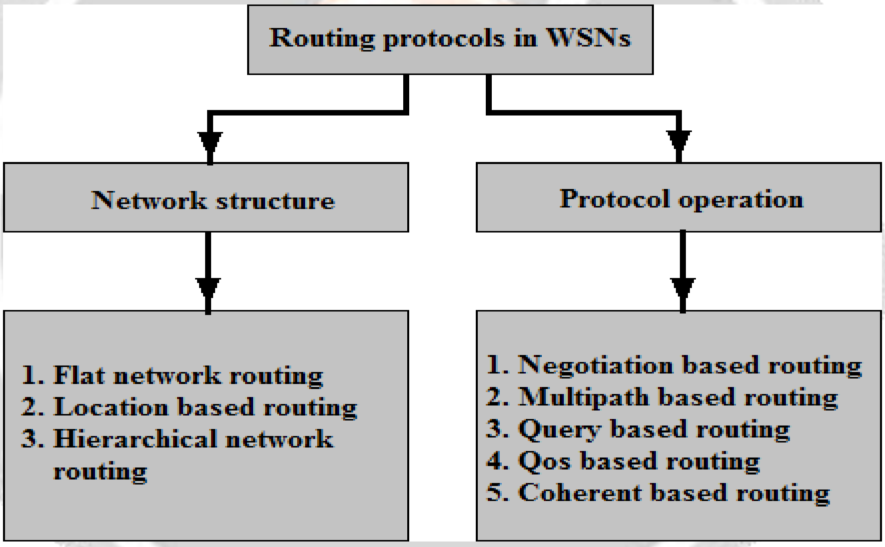
Routing protocols in WSNs
Network structure
Protocol operation
1. Flat network routing
2. Location based routing
3. Hierarchical network routing
1. Negotiation based routing
2. Multipath based routing
3. Query based routing
4. Qos based routing
5. Coherent based routing

Fig.1: Classification of Routing Protocols in Wireless Sensor Network

based on network structure (i.e. network architecture) and protocol operation (i.e. application) [36]. The Figure 3.1 shows the classification of routing protocols in WSNs. Depending on the network structure, the routing protocols are divided into flat-based routing, hierarchical based routing, and localization-based routing. Generally, in flat-based routing, the same functionality is assigned to every node in the network. However, in hierarchical-based routing, the nodes play different roles in the network. In localization-based routing, the location information is used to adequately route the data.

A routing protocol will be considered adaptive if it can adapt to the current network conditions and available energy levels. Depending on the protocol functioning, these can be classified as multi-path based routing, query based, negotiation based, quality of service based or coherent based.

2.1 Network-Structure based protocols

The network structure can play significant role in routing the data from the nodes to the base station. Depending on the network structure, routing in WSNs can be classified [36] as mentioned below.

2.2 Flat based routing

In a flat network topology, each node plays the same role and has the same functionality as other sensor nodes in the network. When a sensor node needs to send data, a flat network routing protocols attempt to find a route to the sink hop by hop using some form of flooding. Since the sensor networks com- posed of large number of sensor nodes, it is not feasible to assign a global identifier to each node in the network. The most popular flat-based routing in WSN are data-centric protocols, where the base station collects the data from the selected regions by sending queries. Most of the protocols use at- tribute based naming to specify the characteristics of data. The advantage of data-centric protocols is that these save energy through data negotiation and elimination of redundant data and also, that all the nodes can reach the BS irrespective of their position. The following paragraphs describe some of the flat network routing protocols.

3. CONCLUSION

Routing paths for transmission of data packets from one node to another can be established in one of three ways, namely proactive, reactive or hybrid. In proactive routing all the routes are computed in advance and maintain consistent up-to-date routing information from each node to every other node in the network. Every node in the network maintains one or more routing tables that store the routing information. This is also called table driven routing and is preferably used in the application where the sensor nodes are static. Proactive routing protocols periodically monitor the changes in the topology to ensure the ready availability of any path amongst active nodes. When a topology changes due to the failure of nodes, the change has to be propagated throughout the network as updates so that the network view remains consistent. A Dynamic Election of Cluster Head sensor and Void Removal mechanism (DECHVR) to save energy through eliminating void sensors at all nodes and replacing a boundary relay void sensor with a dynamic sensor mobile node. A Relative Record Index method (RRI) for WSNs to store data with an encrypted security mechanism in the cloud and facilitate rapid data retrieval from the cloud. To store sensor data in the cloud using a B+ tree index and facilitate a fastest retrieval from the cloud.

REFERENCES

[1] P.T Sivasankar and M. Rama and G. krishnan, An Energy-Efficient Based on Heterogeneous Cluster Head Selection Algorithm for Wireless Sensor Networks , Journal of Computational and Theoretical Nano science, 14,(9), (2017), 4520-4527.

[2] A. Suhar , J.Jono, and G. Hendrantoro, Hop Distances Optimization for Balancing the Energy Consumption of Multi-Hop Clustered Wireless Sensor Networks, Proceedings of the International Conference on Computer, Control, Informatics and Its Applications (IC3INA), (2013), 49-52.

[3] Alghamdi and Turki, Secure And Energy Efficient Path Optimization Technique in Wireless Sensor Networks using DH Method , IEEE Access ,6(2018) , 53576-53582.

[4] T. Behera, U. Samal and S. Mohapatra, Energy-Efficient Modified LEACH Protocol for IoT Application, IET Wireless Sensor Systems, 8,(5), (2018), 223-228.

[5] K. Li, H. Luan and C.C. Shenqi-Ferry: Energy-Constrained Wireless Charging in Wireless Sensor Networks (WSN), Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), (2012), 2515-2520.

[6] S. Kim, T. Yang, C. Kim, H. Cho, and S.H. Kim, Dynamic Anchors Based Void Avoidance Scheme for Real-Time Application in WSN, Proceedings of the 86th Vehicular Technology Conference (VTC-Fall),(2017),1-5.

[7] D. Zhang, D. Khang and E. Dong, A Bypassing Void Routing Combining of Geographic and Virtual Coordinate Information for WSN , Proceedings of the 22nd International Conference on Telecommunications (ICT),(2015),118-122.

[8] S. Mitra and A. Roy, Communication Void Free Routing Protocol in Wireless Sensor Network, Wireless Personal Communication, 123, (2015), 2567-2580.

[9] N. Javaid, T. Hafeez, Z. Wadud and N. Guizani, , Establishing A Cooperation-Based and Void Node Avoiding Energy-Efficient Underwater WSN for a Cloud , IEEE Access, 5,(2017),11582-11593.

[10] Javaid k Latif, N. Saqib, M. N., Khan, Z. A., Qasim, U., Mahmood, B., and Ilahi, M, Energy hole minimization with field division for energy efficient routing in WSNs. International Journal of Distributed Sensor Networks, 11(10), (2015), 953134.

[11] Pathak, A. and Tiwari, M. K. ,Minimizing the Energy Hole Problem in Wireless Sensor Networks by Normal Distribution of Nodes and Relaying Range Regulation ,Fourth International Conference on Computational Intelligence and Communication Networks, IEEE,(2012) ,154-157.

[12] Xue, Y., Chang, X., Zhong, S. and Zhuang, Y, An efficient energy hole alleviating algorithm for wireless sensor networks, IEEE Transactions on Consumer Electronics, 60(3), (2014),347-355.

[13] Watfa, M. K., Al-Hassanieh, H., & Salmen, S , A novel solution to the energy hole problem in sensor networks, Journal of network and computer applications, 36(2), (2013), 949-958.

[14] Ren, J., Zhang, Y., Zhang, K., Liu, A., Chen, J., & Shen, X. S , Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks , IEEE transactions on industrial informatics, 12(2), (2016), 788-800.

[15] A.Sher, A. Khan, N. Javaid, S. Ahmed, M. Aalsalem, and W. Khan, Void Hole Avoidance for Reliable Data Delivery in IoT Enabled Underwater Wireless Sensor Networks, Sensors, 18, (10), (2018), 3271.

[16] W. Ghoreyshi, Md. Seyed, S. Alireza, and B. Tuleen, A Stateless Opportunistic Routing Protocol for Underwater Sensor Networks, Wireless Communications and Mobile Computing, (2018).

[17] A. Ahmed, V. Kangwar and A.R Bhan, WPTE: Weight-Based Probabilistic Trust Evaluation Scheme for WSN , Proceedings of the 5th International Conference on Future Internet of Things and Cloud Workshops (Ficloudw) , (2017), 108-113.

[18] H.Y Lao and Fong ,D. Yi, Coverage Hole Detection Algorithm Based on HPNS in WSN, Proceedings of the IEEE 18th International Conference on Communication Technology (ICCT),2018, 896-900.