A Review and Comparison of Reliable Unicast Routing Protocols For Mobile Ad Hoc Networks

Hadi Sargolzaey†, Ayyoub Akbari Moghanjoughi†† and Sabira Khatun†††

Wireless Routing Research Group, Department of Computer and Communication Systems Engineering
Faculty of Engineering, University Putra Malaysia, 43400 Serdang, Selangor, Malaysia

Summary
An important and essential issue for mobile ad hoc networks is routing protocol design that is a major technical challenge due to the dynamism of the network. Node failures and arbitrary movement of nodes break the routes and lead the frequent operation of rebuilding routes that consume lots of the network resources and the energy of nodes. Many efforts have been made to design reliable routing protocols that enhance network stability. This paper review and compare some recently published reliable unicast routing protocols, that can be used for selecting appropriate routing protocols, which are suitable for a particular application. Also it will maximize the reliability of the deployed network. Furthermore the proposed methods used in the reviewed protocols, can help designers and researchers for enhancing the reliability of their new routing protocols.

Key words:
Reliable routing protocols, Unicast routing, Mobile Ad-hoc Networks.

1. Introduction

The mobile ad hoc network (MANET) allows a more flexible communication model than traditional wire line networks since the user is not limited to a fixed physical location [1]. It is a new special network that does not have any fixed wired communication infrastructure or other network equipments. With no pre-existing fixed infrastructure, MANETs are gaining increasing popularity because of their ease of deployment and usability anytime and anywhere. So they are viewed as suitable systems which can support some specific applications as virtual classrooms, military communications, emergency search and rescue operations, data acquisition in hostile environments, communications set up in Exhibitions, conferences and meetings, in battle field among soldiers to coordinate defence or attack, at airport terminals for workers to share files etc.
Host mobility can cause unpredictable network topology changes in MANETs. Hence, a highly adaptive routing scheme to deal with the dynamic topology is required. Many unicast routing protocols have been proposed for MANETs to achieve efficient routing [2].

Classification of unicast routing protocols in MANETs can be done in many ways, but most of them are depending on routing strategy and network structure. According to the routing strategy, the routing protocols can be categorized as proactive and reactive routing (see Fig. 1), while depending on the network structure these are classified as flat, hierarchical and position based routing. Both the proactive and reactive protocols come under the flat routing.

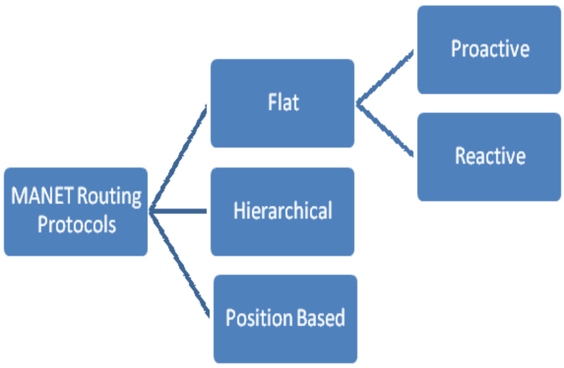

Fig. 1 Classification of MANET routing protocols

Proactive Routing Protocols: A proactive routing protocol is also called "table-driven" routing protocol. Using a proactive routing protocol, nodes in a mobile ad hoc network continuously evaluate routes to all reachable nodes and attempt to maintain consistent, up-to-date routing information. Therefore, a source node can get a routing path immediately if it needs one. When a network topology change occurs, respective updates must be propagated throughout the network to notify the change. So if we noted to network topology changes in MANETs, the control overhead to maintain up-to-date network topology information is relatively high. Wireless Routing Protocol (WRP) [3], the Destination Sequence Distance Vector (DSDV) [4] and the Fisheye State Routing (FSR) [5] are all proactive routing protocols.
Reactive Routing Protocols: Reactive routing protocols for mobile ad hoc networks are also called "on-demand" routing protocols. In a reactive routing protocol, routing paths are searched only when needed. When a source node wants to send packets to the destination but no route is

Manuscript received January 5, 2009
Manuscript revised January 20, 2009

available, it initiates a route discovery operation. In the route discovery operation, the source broadcasts route request (RREQ) packet. When the destination or a node that has a route to the destination receives the RREQ packet, a route reply (RREP) packet is created and forwarded back to the source. Each node usually uses hello messages to notify its existence to its neighbours. Therefore, the link status to the next hop in an active route can be monitored. When a node discovers a link disconnection, it broadcasts a route error (RERR) packet to its neighbours, which in turn propagates the RERR packet towards nodes whose routes may be affected by the disconnected link. Then, the affected source can re-initiate a route discovery operation if the route is still needed. Compared to the proactive routing protocols, less control overhead is a distinct advantage of the reactive routing protocols. Thus, reactive routing protocols have better scalability than proactive routing protocols. However, when using reactive routing protocols, source nodes may suffer from long delays for route searching before they can forward data packets. Hence these protocols are not suitable for real –time applications. The Dynamic Source Routing (DSR) [6] and Ad hoc On-demand Distance Vector routing (AODV) [7] are examples for reactive routing protocols.

Hierarchical Routing Protocols: Typically, when wireless network size increase (beyond certain thresholds), current “flat” routing schemes become infeasible because of link and processing overhead. One way to solve this problem and to produce scalable and efficient solutions is hierarchical routing. Wireless hierarchical routing is based on the idea of organizing nodes in groups and then assigning nodes different functionalities inside and outside of a group. The Zone Routing Protocol (ZRP) [8], Zone-based Hierarchical Link State routing (ZHLS) [9] and Hybrid Ad hoc Routing Protocol (HARP) [10] are examples for hybrid routing protocols.

Position Based Routing Protocols : The advances in the development of Global Positioning System (GPS) nowadays make it possible to provide location information with a precision in the order of a few meters. They also provide universal timing. While location information can be used for directional routing in distributed ad hoc systems, the universal clock can provide global synchronizing among GPS equipped nodes. In position based routing protocols, instead of using routing tables and network addresses, the routing decisions are made on the basis of the current position of the source and the destination nodes. Location Aided Routing (LAR) [11] and Distance Routing Effect Algorithm for Mobility (DREAM) [12] are typical position based routing protocols proposed for mobile ad hoc networks. According to several experimental works, routing schemes that use positional information scale well [13].

In all of the unicast routing protocols, the robustness of the route is generally not involved as a requirement for its selection. Consequently, route breakups will frequently occur, induced by nodal mobility and/ or nodal and link failures as well as by fluctuations in the communications transport quality experienced across the network’s communications links. The latter are caused by signal interferences, fading and multi-path phenomena and other causes producing ambient and environmental noise and signal interference processes. On the other hands, route breakups lead the frequent operation of rebuilding routes that consume lots of the network resources and the energy of nodes.

Many efforts have been made to design reliable routing protocols that enhance network stability. In this paper, we review and compare some recent published reliable unicast routing protocols. This paper has organized as following; in section 2, some reliable routing protocols are described briefly. Section 3 presents the comparisons on the reviewed protocols, and finally conclusion of paper comes in section 4 as well.

2. MANET Reliable unicast routing protocols

2.1 Energy Aware Reliable Routing (EARR)

EARR is a cross-layer reactive routing protocol that reduces the route-reconstructions due to residual energy shortages [14].

It is assumed that all nodes in EARR are equipped with a residual energy detection device and some energy consumption model is offered for each node to estimate whether its remaining battery capacity is sufficient to relay the traffic. Also the traffic load from application layer is carried in the RREQ packet. In this protocol, only nodes with sufficient residual energy to complete the task will take part in the propagation of RREQ packet.

Finally after all RREP packets received, source node pick the optimum path with maximal bottleneck energy to route data packets. (Bottleneck energy refers to the minimal residual energy of all nodes along one path)

In EARR, when a source node wants to send packets, if it has already kept at least one route to the destination, then for each path it will check whether each node on the path has sufficient residual energy to complete the forwarding task. Only when all nodes on the path have enough battery the path can be thought as valid one. Like the previous state, if several paths are valid, the one with maximal bottleneck energy is chosen to transmit data packets.

Both periodical information exchange and error report are used in EARR to maintain routes, as in many conventional reactive routing protocols. The only difference lies in that when nodes exchange information with neighbours, not only address information but also current residual energy info are carried by hello messages, so that each node is able to obtain the most up-to-date energy information of neighbours.

2.2 Stable Weight-based On-demand Routing Protocol (SWORP)

SWORP is a reactive routing protocol that uses the weight-based route strategy to select a stable route in order to improve routing quality in MANETs. The basic idea is to select a stable routing path to reduce the routing overhead and packet loss [15].

The weight of a route is decided by three factors: the Route Expiration Time (RET), the Error Count (EC), and the Hop Count (HC).

The RET is the minimum Link Expiration Time (LET) for a feasible path. The LET can be obtained by using the principle that two neighbours in motion will be able to predict future disconnection time. Such a prediction can be accomplished by the following method.

The motion parameters of two neighbouring nodes can be obtained by using the Global Positioning System (GPS). A free space propagation model is assumed which signal strength solely depends on the distance to the transmitter. Also it is considered that all nodes have their clocks synchronized using the GPS clock. On the other hand, by considering the motion parameters of two nodes, the duration of time which these two nodes remain connected can be calculated. The speed and heading of a mobile node can be obtained from the mobile node's own instruments and sensors (e.g., compass, odometer, speed sensors).

When each node sends a RREQ packet, the packet appends its location, direction, and speed. So, the next hop of the node that receives the RREQ packet can predict the link expiration time between itself and the previous node.

The EC is the maximum node error count for a feasible path. The error count is used to indicate the number of link failures caused by a mobile node.

The SWORP effectively combines all the three parameters in a weight function with weighing factors C1, C2, and C3, the values of which can be chosen according to the system requirements. As an illustration, route expiration time is very important in MANETs. Thus, the weight of that factor can be made larger. The flexibility of changing the factors helps in using this algorithm to select a optimum routing path. A larger route expiration time represents higher reliability, as do a lower error count and lower hop count.

In the route discovery process source node S broadcasts a RREQ packet to its neighbouring nodes. If the node is within the transmission radius, it forwards the RREQ packet to its own neighbouring nodes and adds its ID, the route expiration time, the error count, and the hop count of the RREQ packet to the packet entry. When destination node D receives a RREQ packet, it waits for a certain amount of time to receive other RREQ packets. Then node D computes the weight value using the weight function. Afterwards, node D selects the path with the maximum weight value as the primary routing path among all feasible paths. Finally, node D sends a RREP packet to source node S along the primary routing path.

Another form of this protocol (SWORP-BR) also is proposed for selecting alternative paths. When a link failure occurs, the alternative path selection algorithm is triggered. The method is to overhear RREP packets transmitted by a neighbouring node. It records this neighbouring node as a next hop to the destination node in its alternate route table. For example, Figure 2 shows the process of constructing the primary and alternate routes.

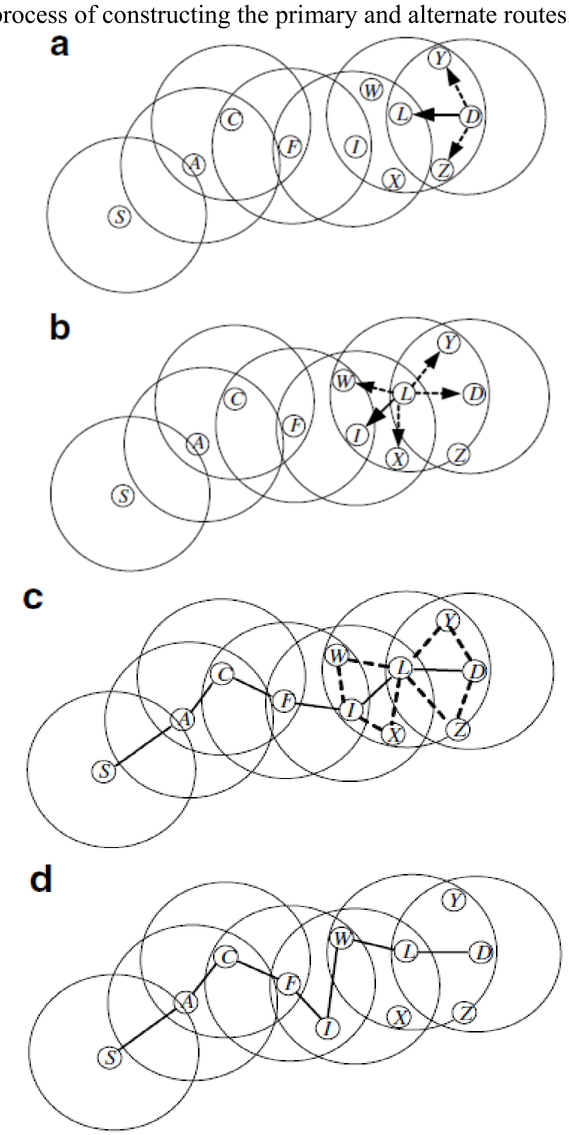

Fig. 2 Multiple route construction of stable weight-based on-demand routing protocol with backup routes (SWORP-BR): (a) destination node D sends a route reply (RREP), (b) node L forwards the RREP, (c) the primary route and alternate routes are established and (d) the data packet is transmitted via an alternate route when the primary route is disconnected.

With the proposed method, when the RREQ packet reaches the destination node D, the primary route (S, A, C, F, I, L, D) is selected. Then destination node D sends a RREP to node L. At this time, nodes Y and Z that are within the transmission range of node D overhear the RREP packet and insert an entry into their alternate route table. This process is shown in Figure 2.a. Similar processes are executed at the next hops backwards until the RREP packet reaches the source node S. Figure 2.c shows the state when the RREP reaches the source node S. The protocol then builds the primary and the alternate routes. Figure 2.d illustrates the use of an alternate path when the primary route gets disconnected. Node *i* move out of the transmission range of its neighbouring node L. It cannot transmit data from node F to node L. Therefore, node I must broadcast the packet to its neighbouring nodes to salvage the data. When node W receives the packet, it looks up its alternative route table and finds node L as its next hop toward the destination node D. Then node W unicast the packet to node L and builds the new connection.

2.3 Mobility Sensitive Approach (MSA)

MSA is a protocol framework that is implemented on top of the network layer that tries to adapt to the diverse mobility rates of the nodes as exhibited in real networks [16]. Instead of providing a single routing strategy, this framework uses a suite of complementary protocols that are suitable for different types of mobile networks.

In this work, a metric is proposed, named stability, which is used for characterizing the relative mobility of the nodes. The metric uses the notion of associativity, which is the time (in beacons) that nodes are associated (i.e., they retain a connection). According to its stability, every node is classified to a mobility class. Based on these mobility classes, a novel protocol framework is designed that operates on top of the network layer and, for any pair of origin and destination nodes, determines the routing technique (among those available to the nodes) that best corresponds to their mobility properties.

It is assumed that every node has access to a beaconing mechanism, which is either provided by the data link layer or can be easily implemented using the reactive protocol. (e.g., the hello messages)

This framework can be divided into three services (i.e., software agents). The first service is concerned with the calculation of the associativity of the links and the classification of the nodes into mobility classes. It is called the mobility classification service (MCS). The second service determines how routing between two nodes of the network is performed, based on the information provided by the first service (MCS) and the software components of the available routing protocols. It is called the strategy selection service (SSS). The third service is the actual routing service offered to the other software agents running in the mobile node, and ‘‘looks’’ like a routing protocol. It is called the routing service (RS).

For a graphical representation of the interconnection of the three services (MCS, SSS, and RS) with the lower (MAC) and higher (Network) layers, as well as the routing protocols (see Fig. 3).

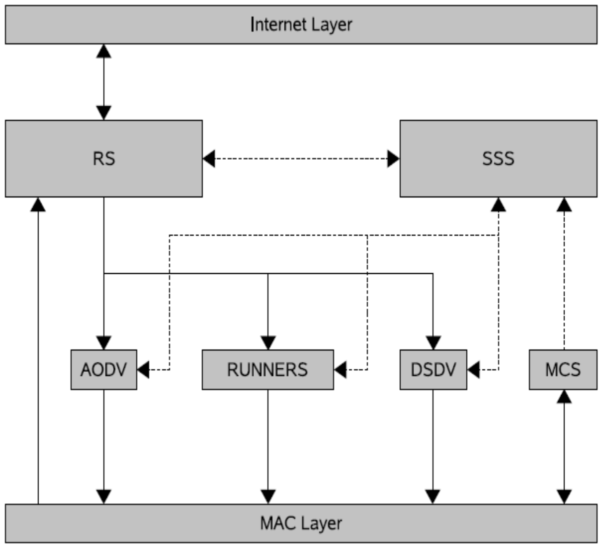

Fig. 3 Architecture of the framework – dotted lines represent inter-process communication, continuous lines represent packet flow. (AODV, RUNNERS and DSDV is routing protocol examples)

The main idea is to allow each node to execute different routing protocols concurrently and let the mobility-sensitive framework control their operation (by activating/deactivating them) and reroute the offered services through RS. This framework can be extended to make this choice based on other network conditions, such as available energy, geo-location, QoS guarantees, etc.

2.4 Distributed Long Lifetime Route (DLLR)

DLLR is a reactive routing protocol that discovers two of the most desirable Long Lifetime Routes (LLRs) through one best-effort route discovery procedure [17]. If two LLRs can be provided at a time, the routing protocol can save the longer LRR as a backup and use the shorter LRR, which usually has a shorter route length and is thus more energy-efficient, as the primary route for transmissions. The routing protocol can switch to the longer LRR to maintain the flow of traffic when the shorter LLR breaks. Meanwhile, a new route discovery procedure can be initiated, and when the newly discovered LLRs are returned, the old LLRs can be replaced.

Link lifetime can be estimated through the link break probability (probability that a link is broken at time t) given an estimation rule, such as from now to when the link break probability is higher than a certain threshold. The quality of a link can be thus quantified using this estimated link lifetime. Using this quantified link lifetime estimations, the route lifetime is simply the minimum lifetime of the *n* links.

The main procedure of DLLR is similar to a typical reactive on-demand routing protocol. The difference lies in the implementation details such as RREQ packet format, routing update rules and RREQ forwarding delay rules.

In DLLR, RREQ packet contains a primary route that expands while the RREQ propagates throughout the network. In addition, it contains an auxiliary route (backup route) which does not have any effect on RREQ forwarding decisions. Also, included in the RREQ are the primary and auxiliary route lifetimes. These route lifetimes are calculated at each intermediate node by choosing the minimum from the composed estimated link lifetimes. The source node broadcasts this RREQ packet, which initially, the two routes only contain the source node and their lifetimes are set as 0.

When an intermediate node receives an RREQ for the first time, it appends itself into the prim/aux routes in the packet and records the request locally. Then it adjusts the lifetimes by choosing the minimum of the previous route lifetime and its link lifetime with the previous node. Next, it schedules a local delay time for forwarding this modified RREQ. When the delay time is up, it forwards this RREQ packet. If the intermediate node receives a duplicate RREQ, it will update the prim/aux routes in its recorded RREQ based on the LLR update rule (the node picks the one with the longest lifetime from the shortest routes as the primary route, and it picks the one with the longest lifetime from the second shortest routes as the auxiliary route).

When destination node receives RREQ, it waits enough time for receiving other RREQs and then it will unicast an RREP packet to the source node using the primary route with the auxiliary route attached, just as in the normal reactive procedure.

2.5 Reliable Source Routing (RSR)

RAS is a reactive routing protocol that achieves increased reliability through the maintenance of a reliability factor by the nodes in the network [18].

During the route discovery process, the request messages are only propagated to nodes with a reliability factor that is above a threshold value specified by the application. Selection among multiple possible discovered routes is done through the use of a normalized cumulative path reliability factor that is calculated by the destination.

In this protocol, the source node sends the RREQ packet which is similar to other reactive routing protocols but contains the following different fields: (1) RMIN: The minimum value for the reliability factor required in the path from source to destination. (2) RCUM: The cumulative reliability factor of the path that is being discovered. (3) NH: It contains a list of the next hop host candidates that satisfy the reliability requirements for the path that is being discovered. (4) MAX NH: Maximum number of nodes in the NH list. This parameter is intended to control the flooding of the RREQ packet during route discovery. (5) BACKUP PATHS: This is the maximum number of backup paths that can be included in the routing table of the source node.

When an intermediate node receives a RREQ packet from another node, it builds the NH list with all of the neighbours whose reliability factor is above RMIN. It then adds its reliability factor to the cumulative path reliability factor RCUM and propagates the RREQ packet to its neighbours. Each of the neighbours whose ID is in the NH list will further propagate the RREQ packet according to the same algorithm.

When and if the destination receives the RREQ packets, it selects the path with the highest normalized path reliability factor *PRF=RCUM/n*, where *n* is the number of intermediate nodes in the path (not including the source and destination nodes), and unicast a RREP packet back to the source. If backup paths are required then the paths with the highest reliability factors will have their corresponding RREP packets sent to the source.

Figure 4 shows a detailed example that illustrates the route discovery process using the RAS routing protocol between the source node A and the destination node G.

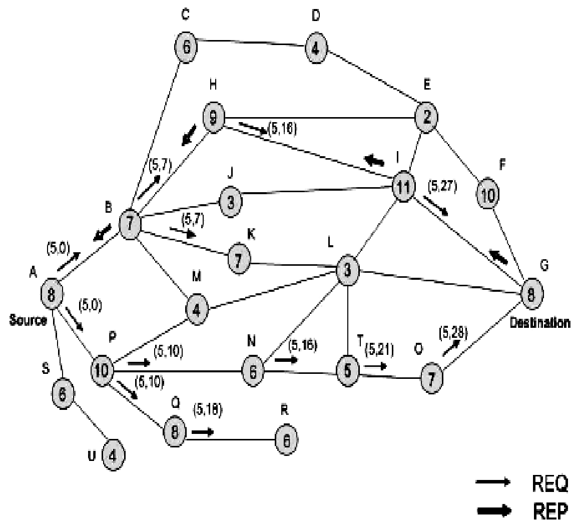

Fig. 4 An example of the route discovery process in RAS

In this case, the required path to transmit the data has a minimum reliability factor RMIN = 5, and MAX NH = 2. Node A propagates the RREQ packet to nodes B and P. In turn, each of the nodes further propagates the RREQ packet according the above algorithm and accumulates the reliability factor for each node in the path cumulative path reliability factor. Finally, the RREQ packet, arrives at the destination node G with the discovered path A − B − H − I − G and a final cumulative reliability factor of 27. Similarly, a RREQ packet is propagated through nodes A−P −N −T −O −G with a cumulative reliability factor of 28. When the destination node G receives both RREQ packets for the two discovered paths, it divides each path's final cumulative reliability factor with the number of nodes in the path to calculate the normalized path reliability factor *PRF* = *RCUM/n*. Here, the destination node G determines that the discovered paths A−B−H−I−G, and A − P − N − T − O − G have normalized reliability factors of 27/3 = 9 and 32/4 = 8 respectively. Therefore it chooses the more reliable path A − B − H − I − G with the higher normalized path reliability factor of 9. So, unicast a RREP packet back to the source node A along the discovered intermediate nodes in the path list.

The reliability factor of a particular node is a measure of its past performance in being a part of successful data transmissions. There are several different algorithms that can be used to maintain the reliability factor:

Self maintenance of the reliability factor by the node: Each time a node successfully transmits a number of packets to another node along the path it increases its reliability factor.

Maintenance of the reliability factor by the acknowledgements: Using this policy, the destination sends positive acknowledgments to the source. The reliability factor is incremented when an intermediate node receives positive acknowledgements from the destination.

Maintenance of the reliability factor by 1-hop neighbours: Each node maintains a reliability factor for each of its *n* neighbours. This set of reliability factors are a measure of the reliability of each of them in its view based on their past performance in successful data transmissions.

Maintenance of the reliability factor using link-based acknowledgement: If the next hop node did follow up and forward the packet to its successor node, then it is rewarded by increasing its reliability factor in previous node. Otherwise, if that node did not forward the data, then it is penalized by not increasing its reliability factor.

2.6 Link Reliability based Hybrid Routing (LRHR)

LRHR is a hybrid routing protocol that contrary to the traditional single path routing strategy, multiple paths are established between a pair of source-destination nodes [19]. Hybrid routing protocols have to deal with the problem of how to switch between reactive on-demand and proactive table driven routing strategy. A special and natural switching mechanism is adopted in LRHR. LRHR mostly works in the table-driven state. If all the following conditions are met, LRHR will transit from table-driven state to on-demand state. In other words, the route discovery procedure will be initiated: I) Source node S has packet sending to destination node D, but S has no route to D. II) the interval between the new route discovery and the latest one is bigger than the minimum route request interval. (When there is no route to the destination node, instead of simply dropping the packet, LRHR will buffer the packet and initiates route discovery)

In LRHR, the node operates in a promiscuous receive mode. In the promiscuous mode, a node can overhear a packet that is not destined for it. Therefore, it can obtain more routes than a node that operates in the ordinary mode. LRHR mainly consists of the following modules: route discovery, route maintenance, route advertisement and edge weight management. Figure 5 shows the relationships among these modules.

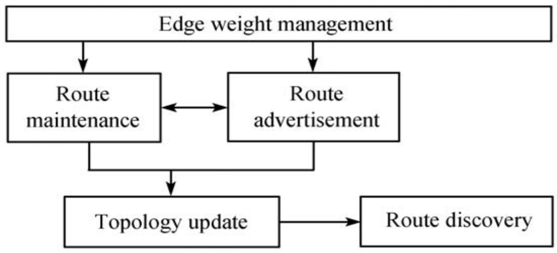

Fig. 5 Framework of LRHR

In LRHR, link reliability between nodes is quantified as an edge weight. (The link from one node to another is defined as an edge) Contrary to the well-known Dijkstra's shortest-path algorithm, LRHR selects the route that has the maximum edge weight sum as the primary route. In this way, the selected route is of the maximum reliability. In addition, unlike the traditional single path routing strategy, multiple paths are established between a pair of source-destination nodes.

In LRHR, each edge is assigned a value between 0 and 10. The value represents the reliability of the edge. (The greater the value, the higher the reliability) Edge weight management mainly consists of increasing and decreasing the edge weight. Each new established edge is assigned the weight of 10. If the edge is not used, with time elapsing, the edge reliability will be decreased gradually. So the more frequently the edge is used, the higher the reliability.

In the hybrid routing protocol LRHR, the link status database is periodically broadcasted to the neighbour nodes in route advertisement by one node. To reduce route advertisement overhead, LRHR divides route advertisement into full route advertisement and partial route advertisement. The full route advertisement includes the entire link status database, whereas, the partial route advertisement only advertises the new edges. The period of partial route advertisement is comparably short. It is triggered on-demand in some sense. If no route advertisement is received in the predefined time interval from a certain node X, node X is considered to be in the inactive state.

When each node forwards a packet (the packet may be the data packet, route request or route reply), it can obtain routing information from the source route list or route reply list carried by the packet. Then the route table can be updated. This is an active learning procedure. Also, because the node operates in the promiscuous receive mode, a node can overhear a packet that is not destined for it. In this way, the node can obtain route information from the overheard packet. This is a passive learning procedure.

As wireless networks are inherently less reliable than wired networks, LRHR utilizes a hop-by-hop acknowledgment to provide detection and retransmission of lost or corrupted packets. After sending a packet to the next hop node, the sender may be able to hear that node transmitting the packet again, on its way further along the path, if it operates in promiscuous receive mode. For example, in Fig.6, node X may be able to hear Y's transmission of the packet to Z. This type of acknowledgment is known as implicit acknowledgment.

In the route table, there exists more than one path from a source to a destination. In general, two packets generated for a common destination by a source may be routed through different paths. After arranging these paths according to the edge weight sum along the path in descending order, the path along which the edge weight sum is the maximum, called primary path. The other paths are called backup paths.

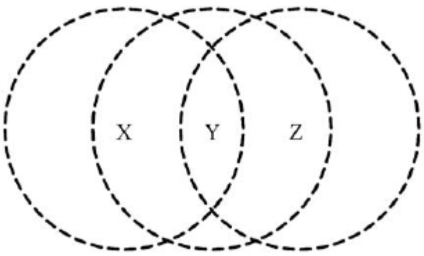

Fig. 6 Implicit acknowledgment

2.7 Stable and Energy efficient Routing (SBNRP)

SBNRP is a reactive on demand routing protocol that uses a new concept of backbone nodes with power factor [20].

In this protocol two different concepts have been joined together to make an efficient protocol. (Stability and Energy Efficiency) The scheme uses backbone nodes for stable routes and uses power factor to determine active nodes to participate in routing.

Selection of backbone nodes is made upon availability of nodes and battery status and each route table has an entry for number of backbone nodes attached to it and their battery status.

The proposed scheme is explained with the help of an example shown in Figure 7.

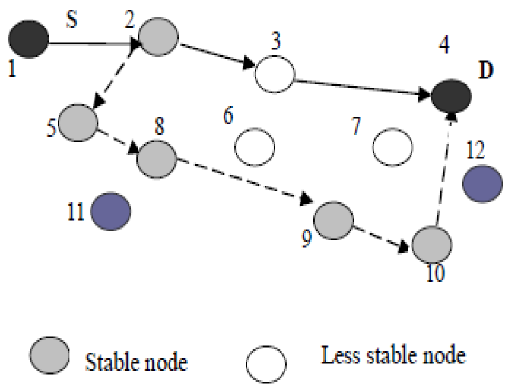

Fig. 7 An Example of routing with SBNRP

Assume that the node with index 1 is the source while destination is the node with index 4. If the node with index 3 is having power status in critical or danger zone, then though the shortest path is 1—2—3—4 but the more stable path 1—2—5—8—9—10—4 in terms of active power status is chosen. This may lead to slight delay but improves overall efficiency of the protocol by sending more packets without link break than the state when some node is unable to process route due to inadequate battery power.

The process also helps when some intermediate node moves out of the range and link break occurs, in that case backbone nodes take care of the process and the route is established again without much overhead. In Figure7 if the node with index 8 moves out, the new established route will be 1—2—5—11—9—10— 4. Here the node with index 11 is acting as backbone node (BN) for the node with index 5 and the node with index 8. Similarly the node with index 12 can be BN for the nodes with indices 7, 10 and 4. BN has been selected at one hop distance from the said node.

The protocol is divided into three phases. Route Request (REQ), Route Repair (REP) and Error Phase (ERR).

REQ phase is like route discovery operation of reactive routing protocols. (Query and Reply procedure)

An Intermediate node with an active route (in terms of power and Backbone Nodes), upon receiving a new RREQ packet, records the previous hop and the source node information in its route table i.e. backward learning. It then broadcasts the packet or sends back a RREP packet to the

source if it has an active route to the destination.
The destination node sends a RREP packet via the selected route when it receives the first RREQ or subsequent RREQ packets that traversed a more stable route. Stability of route depends upon two major aspects as: Lifetime and Power status.
Taking advantage of the broadcast nature of wireless communications, a node promiscuously overhears packets that are transmitted by their neighbouring nodes. When a node that is not part of the route overhears a RREP packet not directed to itself transmit by a neighbour (on the primary route), it records that neighbour as the next hop to the destination in its alternate route table. From these packets, a node obtains alternate path information and makes entries of these backbone nodes (BN) in its route table.
When a node detects a link break, it performs a one hop data broadcast to its immediate neighbours. The node specifies in the data header that the link is disconnected and thus the packet is candidate for alternate routing.
Upon receiving this packet route maintenance phase starts by selecting alternate path and checking power status. During local repair data packets will be buffered at local originator.
If, at the end of the discovery period, the repairing node has not received a reply message REP it proceeds in by transmitting a route error ERR to the originating node.

2.8 Cross-Layer Reliable Routing (CLRR)

CLRR is a cross-layer reactive routing protocol that used received signal strength information to choose reliable links to form stable routes [21].
In this cross-layer design, the received signal strength is measured at physical layer and transferred to the top layers.
In CLRR, each node stored/ updated the received signal strength (RSS) of RREQ packet in Neighbour Table (NT) of routing protocol, against the address of the neighbouring node from which the RREQ is received.
Hence, whenever a node receives RREQ packet, by using the current received signal strength and the previous value that is available in neighbour table, the moving direction of sending and receiving nodes can be found. That is, if current value is greater than previous one, the nodes are approaching; else they are moving apart.
The RREQ packet forwarding decision is based on whether the sending and receiving nodes are approaching or moving away, in addition to having an adaptive signal strength threshold with reference to moving speed of the nodes.

2.9 Robust Flow Admission and Routing (RFAR)

RFAR is a reactive on-demand robust routing protocol selectively discovers routes that are probabilistically assured to survive for the duration of the underlying sessions or file transfers [22].
Under the RFAR scheme, the concept is to select a route that will stay intact (with sufficiently high probability) for a certain period of time. This time duration represents the time it takes to transport across the network the data associated with a transaction that is executed by an underlying time critical application.
For the calculation of the robustness indices along a route the RREQ packet of RFAR contains in its header Route Vulnerability Index (RVI) and underlying session holding time H. At source node s, RVI set to 0.In each node the value of RVI updated according to the speeds of that node and the previous node and the effective communications range(at an acceptable bit-error –rate level).
In this protocol, a node receiving such a RREQ packet will proceed to forward (flood) it to its neighbours (if it has not yet forwarded such a RREQ packet) only if:

a) Robustness control: it is desired for the selected route to exhibit a lifetime longer than the expected session holding time.
b) Capacity control: The link capacity (or delay, or queue-size) level that it can offer to packets to be generated by this flow, if admitted, is acceptable.

Upon receipt of RREQ packets, the intermediate or the destination node waits for a prescribed period of time in collecting several, if any, RREQ packets. It then proceeds to examine the cumulative robustness status indices carried in the header of these packets (indicating the corresponding expected lifetime of the route travelled by each RREQ packet), as well as other indices, such as the hop-length of the travelled route.
The destination node then, for example, selects an RREQ packet that provides acceptable robustness level while offering the shortest route among all such received RREQ packets.
In the destination node, the selected RREQ packet induces the issue of a route reply (RREP) packet that is transported towards the source node across the selected route, configuring at this phase the forwarding entries at the nodes located along the route.
In the RFAR, if no acceptable route is discovered or calculated, the admission of the flow is rejected or blocked by the source node.
So if a route is selected in this protocol, the route lifetime is sufficiently long to carry, with high probability, the flow’s transaction without early interruption.
In addition, the selected route should offer the admitted flow packets with sufficient capacity resources so that prescribed (per application type) end-to-end packet delay (mean and jitter) levels are met.

3. Protocols Comparison

Table 1 summarizes the major features of the aforementioned reliable unicast routing protocols. Here the protocols are discussed and compared according to their features.

In the table, the first column shows the type of each protocol. As it can be seen, most of the protocols are reactive on-demand protocols.

Simple implementation and low control overhead are important advantage of reactive type. But as it is mentioned in the introduction, when wireless network size increases, flat routing schemes (like reactive protocols) become infeasible.

LRHR is the only hybrid method that can be used for large scale networks. Also MSA is a protocol framework that can be used by all types of protocols, so it can be applied with all kind of networks.

The second column of the table shows the most important information about the protocols. The reliability metric determines how the protocols select a route from the existing routes between source and destination node. This is the main difference between protocols and each protocol usually uses different metric.

Network size, density of nodes, mobility level and the type of nodes and applications must be considered when the suitable metric for a network is selected.

The protocols select single path or multipath? It is shown in the third column.

If notice to more storage, that is used in multipath for routing table, these protocols are better choices for reliability. The routing protocol can switch to the backup routes to maintain the flow of traffic when the main primary route breaks. So, the delay reduces very well.

In the fourth column, assumptions or requirements of each protocol is showed.

Before implementing the protocols this items must be prepared. As it can be seen, some of the protocols have no assumption or requirement that means it can be used directly.

Next column of the table, determine the network operation enhancements for each protocols.

The information showed in this column is obtained from the paper related to each protocol and verified by using a simulator and comparison with other routing protocols.

Although the main goal of all protocols is increasing the reliability of the network, some of them have other enhancement too.

Higher packet delivery ratio is the main reliability enhancement of almost all of the protocols. Packet delivery ratio is the ratio between the number of packets received by the destination node and the number of packets originated by the source node. The packet delivery ratio is important as it describes the packet delivery efficiency of the routing protocol.

Less time for route discovery, reduced no. of packets dropped and lower route breakup rates are considered reliability enhancements too.

On the other hands, reduced routing load, less control overhead, reduced path discovery overhead and Reduced routing overhead are all about the reduction of the network overhead of the protocols.

Balanced energy consumption is the only different enhancement that exists in EARR. The good result of this enhancement is prolonging the network lifetime.

Finally in the last column, it is shown that which protocols is cross-layer.

Basically, the cross-layer design enables the network protocols and the applications to observe and respond to the changing network and channel conditions. So, in order to meet the changes in mobile ad hoc networks topology, the various layers can be considered together, which leads to cross-layer designs.

4. Conclusion

This paper review and compare some recent published reliable unicast routing protocols for mobile ad hoc networks, that can be used for selecting appropriate routing protocols which are suitable for a particular application. Furthermore it maximizes the reliability of the deployed network. As a conclusion, a perfect reliable unicast routing protocol for mobile ad hoc networks is difficulty of design. Each protocol has its own advantages and disadvantages. A suitable reliable unicast routing protocol should be chosen based on network conditions and application demands. The protocols comparison table provides a guide line for such choice. Also the proposed methods used in the reviewed protocols, can help designers and researchers for enhancing the reliability of their new routing protocols.

Table 1: Reliable unicast routing protocols features

Protocol	*Type*	*Reliability Metric*	*Single path or Multipath*	*Assumptions and Requirements*	*Network Operation Enhancements*	*Cross-Layer Design*
EARR	Reactive	Node residual energy	Single path	Residual energy detection device, Energy consumption model	Less time for route discovery, Reduced routing load, Balanced energy consumption	Yes
SWORP	Reactive	Link expiration time, Link failures caused by a node	Single path	Global Positioning System(GPS)	Less control overhead, Reduced no. of packets dropped, Higher packet delivery ratio	No
MSA	Can be used with all types	Stability of nodes	Single path	Beaconing mechanism	Higher packet delivery ratio	No
DLLR	Reactive	Probabilistic link lifetime estimation	Double path (primary and backup)	---------------	Higher packet delivery ratio	No
RAS	Reactive	Node successful data transmissions	Multipath	---------------	Reduced path discovery overhead	No
LRHR	Hybrid	Link usages	Multipath	---------------	Higher packet delivery ratio	No
SBNRP	Reactive	Probabilistic link lifetime, Node power status	Single path	Node battery power detection	Higher packet delivery ratio	Yes
CLRR	Reactive	Received signal strength	Single path	Receiver signal strength measurement	Higher packet delivery ratio, Reduced routing overhead	Yes
RFAR	Reactive	Probabilistic link lifetime, Link capacity	Single path	---------------	Lower route breakup rates	No

References

[1] J. P. Macker and M. S. Corson, "Mobile Ad Hoc Networking and the IETF", ACM SIGMOBILE Mobile Computing and Communications Reviews, Vol. 2, No. 2, pp. 9-14, January 1998.

[2] Changling Liu, Jörg Kaiser , "A Survey of Mobile Ad Hoc network Routing Protocols", the University of Magdeburg , October 2005 .

[3] Murthy, S. and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks" , ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97.

[4] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers", ACM Computer Communication Review, Vol. 24, No.4, (ACM SIGCOMM'94) Oct. 1994, pp.234-244.

[5] G. Pei, M. Gerla and T.-W. Chen, "Fisheye State Routing in Mobile Ad Hoc Networks", In Proceedings of the 2000 ICDCS Workshops, Taipei, Taiwan, Apr. 2000, pp. D71-D78.

[6] D. Johnson, D. A. Maltz, "Dynamic source routing in ad hoc wireless networks", in Mobile Computing (T. Imielinski and H. Korth, eds.), Kluwer Acad. Publ., 1996.

[7] C.E. Perkins and E.M. Royer. "Ad hoc on demand Distance Vector routing", mobile computing systems and applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, 1999, p90 - p10.

[8] Z. J. Haas. "The Zone Routing Protocol (ZRP) for ad hoc networks", Internet Draft, Nov. 1997.

[9] M. Joa-Ng and I-Tai Lu, "A peer-to-peer zone-based two-level link state routing for mobile ad hoc net-works", IEEE on Selected Areas in Communications, vol. 17, no. 8, pp. 1415 1425, 1999.

[10] Navid Nikaein, Christian Bonnet and Neda Nikaein, "HARP - Hybrid Ad Hoc Routing Protocol", in proceeding of IST 2001: International Symposium on Telecommunications, Iran/Tehran 2001.

[11] Y. B. Ko and N. H. Vaidya. "Location Aid Routing (LAR) in mobile ad hoc networks", In Proc. ACM/IEEE MOBICOM, Oct. 1998.

[12] S. Basagni, I. Chlamtac, V. Syrotiuk and B. WoodWard, "A Distance Routing Effect Algorithm for Mobility (DREAM)", Proc. 4th MOBCOM, 1998.

[13] I. Broustis, G. Jakllari, T. Repantis, and M. Molle. "A Performance Comparison of Routing Protocols for Large-Scale Wireless Mobile Ad Hoc Networks", Technical Report, University of California, Riverside, 2006.

[14] Fang Xie, Lei Du, Yong Bai, Lan Chen, "Energy Aware Reliable Routing Protocol for Mobile Ad-Hoc Networks",IEEE Communication Society,WCNC 2007 proceedings.

[15] Nen-Chung Wang, Yung-Fa Huang, Jhu-Chan Chen, "A stable weight-based on-demand routing protocol for mobile ad hoc networks", Elsevier Information Sciences 177,

2007, p 5522–5537.
[16] Athanasios Bamis, Azzedine Boukerche, Ioannis Chatzigiannakis, Sotiris Nikoletseas, "A mobility aware protocol synthesis for efficient routing in ad hoc mobile networks", Elsevier Computer Networks 52, 2008 p130–154.
[17] Zhao Cheng , Wendi B. Heinzelman, "Discovering long lifetime routes in mobile ad hoc networks", Elsevier Ad Hoc Networks 6, 2008, p661–674.
[18] Imad Jawhar, Zouheir Trabelsi, and Jameela Al-Jaroodi, "Towards More Reliable Source Routing in Wireless Networks", IEEE International Conference on Networking, Architecture, and Storage, 2008.
[19] Xie Xiaochuan, Wei Gang, Wu Keping, Wang Gang, Jia Shilou, "Link reliability based hybrid routing for tactical mobile ad hoc network", Elsevier Journal of Systems Engineering and Electronics Vol. 19, No. 2, 2008, pp.259–267.
[20] Vinay Rishiwal, Ashwani Kush, Shekhar Verma, "Stable and Energy Efficient Routing for Mobile Adhoc Networks", IEEE Fifth International Conference on Information Technology: New Generations, 2008, p1028-1033.
[21] B. Ramachandran, S. Shanmugavel1, "Received Signal Strength-based Cross-layer Designs for Mobile Ad Hoc Networks", IETE technical review, vol 25, issue 4, 2008, p192-200.
[22] Izhak Rubin, Runhe Zhang, "Robust throughput and routing for mobile ad hoc wireless networks", Elsevier Ad Hoc Networks 7, 2009, p 265–280.

Hadi Sargolzaey received the B.S. in Electronic Engineering and M.S. degrees in Digital Electronic Engineering from Ferdowsi University of Mashhad and Sharif University respectively. Currently he is PhD student in Communication Network Engineering, University Putra Malaysia. He has teaching experience in data communication network for more than 13 years in Islamic Azad University of Qazvin. His research interests are mainly on wireless data communication networks and microprocessor systems.

Ayyoub Akbari Moghanjoughi received his B. Eng from IAU University (2006) in Iran and currently he doing his M.Sc. of communication network engineering in Faculty of Engineering at University Putra Malaysia. Also he is postgraduate research assistant there. He was professional inspector of ICT training Centers for state of Yazd in Iran (2004-2006). Currently he is a member of International Association of Engineers (IAEng), International Engineering Consortium (IEC) and IEEE member of Computer, Communication and Computational Intelligence societies. His research interests are mainly management aspects of high-speed and wireless Networks, including the area of topology discovering, quality of service (QoS) routing, Wireless Ad-Hoc and Wireless Mesh Networks. Also swarm Intelligence is his specially interest research area.

Associate Professor Dr. Sabira Khatun is presently working at the Department of Computer & Communication Systems Engineering, Faculty of Engineering, and University Putra Malaysia. She is head of Electronics and Communications Laboratory and Research Advisor of Networks Research Group in the department. She received her PhD in communications and Networking from University Putra Malaysia (UPM) in 2003.

She directs research activities within the Wireless Communications and Networks (WCN) group and her work in Mobile IPv6 (MIPv6) is gaining importance in Internet-based applications so as to offer secure uninterrupted on-line experience in interactive network applications such as in entertainment, games, video conferencing or video streaming while on the move and has had worldwide publicity. She currently leads a few research projects on WCN for mobile internet, medical and 3G/4G applications including UWB, Combined C-SDMA and SDR. She was the proud recipient of Best Inventor of the Asia Pacific Rim 2006, Korea Invention Promotion Association (KIPA) Special Award 2006 for commending excellent efforts to create micro-mobility related MIPv6 invention and Excellent Research Award 2006 from Ministry of Higher Research, Malaysia.

She is an active researcher of Teman project and MyREN Research Community. She is a member of IEEE and her research interest spans Broadband and Wireless Communications including Cognitive Radio, Software Defined Radio (SDR), MIMO, UWB and IPv6.