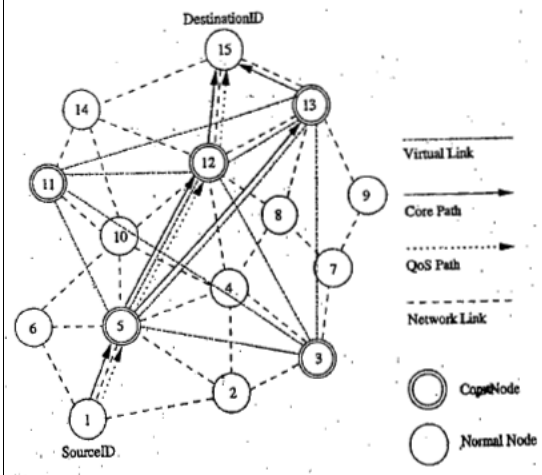
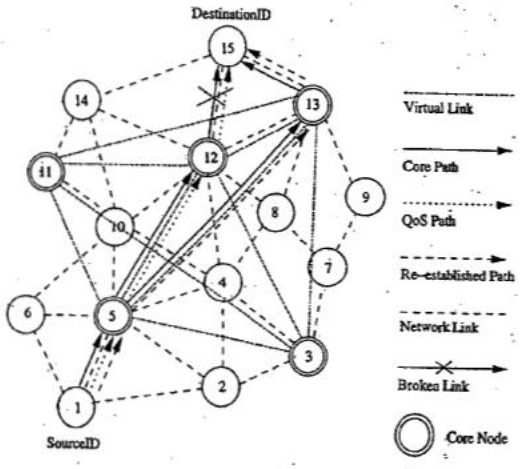
USN										

Improvement Test-May 2018

Sub:	Adhoc Networks					Sub Code:	10IS841	Branch:	ISE	
Date:		Duration:	90 min's	Max Marks:	50	Sem / Sec:	VIII A & B			OBE

	Scheme and Solution	MARKS	CO	RBT
1.	**Explain core contention based distributed adhoc routing protocol** Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR**)** ▪ CEDAR integrates routing and support for QoS. ▪ It is based on extracting core nodes (also called as Dominator nodes) in the network. ▪ Core nodes together approximate the minimum Dominating Set (DS). ▪ A DS of a graph is defined as a set of nodes such that every node in the graph is either present in the DS or is a neighbor of some node present in the DS. ▪ There exists at least one core node within every three hops. ▪ The nodes that choose a core node as their dominating node are called core member nodes of the core node concerned. ▪ The path between two core nodes is termed as virtual link. ▪ CEDAR employs a distributed Algorithm to select core nodes. ▪ The selection of core nodes represents the core extraction phase. ▪ CEDAR uses the core broadcast mechanism to transmit any packet throughout the network in the unicast mode, involving as minimum number of nodes as possible. ▪ Route Establishment in CEDAR: It is carried out in two phase. ▪ The first phase finds a core path from source to destination. The core path is defined as the path from dominator of the source node (source core) to the dominator of the destination node (destination core). ▪ In the second phase, a QoS feasible path is found over the core path. ▪ A node initiates a RouteRequest if the destination is not in the local topology table of its core node; otherwise the path is immediately established. ▪ For establishing a route, the source core initiates a core broadcast in which the RouteRequest is sent to all neighboring core nodes which inturn forwards it. ▪ A core node which has the destination node as its core member replies to the source core. ▪ Once the core path is established, a path with the requested QoS support is then chosen. A node after which the break occurred: o Sends a notification of failure. o Begins to find a new path from it to the destination. o Rejects every received packet till the moment it finds the new path to the destination. ▪ Meanwhile, as the source receives the notification message: o It stops to transmit. o Tries to find a new route to the destination. o If the new route is found by either of these two nodes, a new path from the source to the destination is established. **Advantages** ▪ Performs both routing and QoS path computation very efficiently with the help of core nodes. ▪ Utilization of core nodes reduces traffic overhead. ▪ Core broadcasts provide a reliable mechanism for establishing paths with QoS support. **Disadvantages** ▪ Since route establishment is carried out at core nodes, the movement of core nodes adversely affects the performance of the protocol.	10	CO3	L2

	▪ Core node update information causes control overhead.  Figure 7.24. Route establishment in CEDAR.  Figure 7.25. Route maintenance in CEDAR.			
2.	**Describe any two hierarchical routing protocols** Hierarchical State Routing (HSR) protocol ▪ It is a distributed multi-level hierarchical routing protocol that employs clustering at different levels with efficient membership management at every level of clustering. ▪ Each cluster has its leader. ▪ Clustering is organized in levels: o **Physical**: between nodes that have physical wireless one-hop links between them. o **Logical**: based on certain relations. ▪ Fig 7.31 shows an ex for multilevel clustering **Advantages** ▪ Reduces routing table size storage required is O (n x m). ▪ For flat topology, it is O (nm) o n→ no. of nodes o m→ no. of levels **Disadvantage** ▪ Process of exchanging information concerned all the levels of the hierarchy as well as the process of leader election in every cluster makes it quite problematic for adhoc networks.	10	CO3	L3

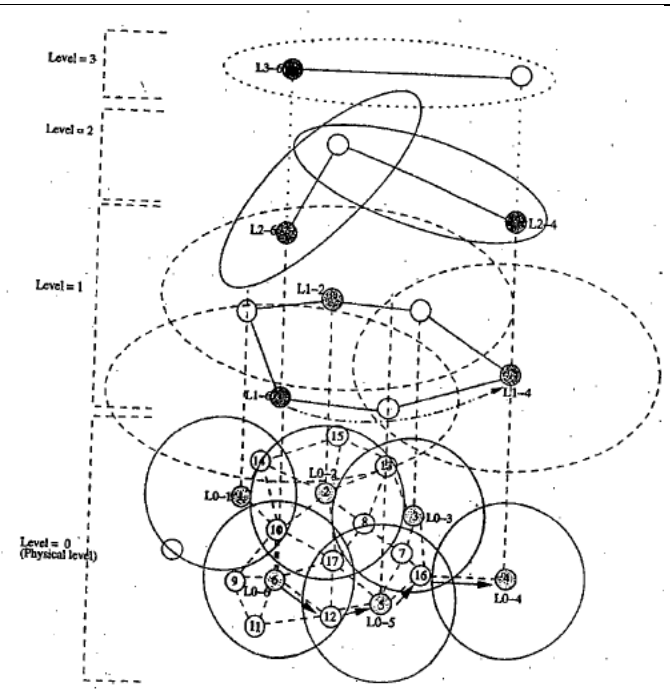
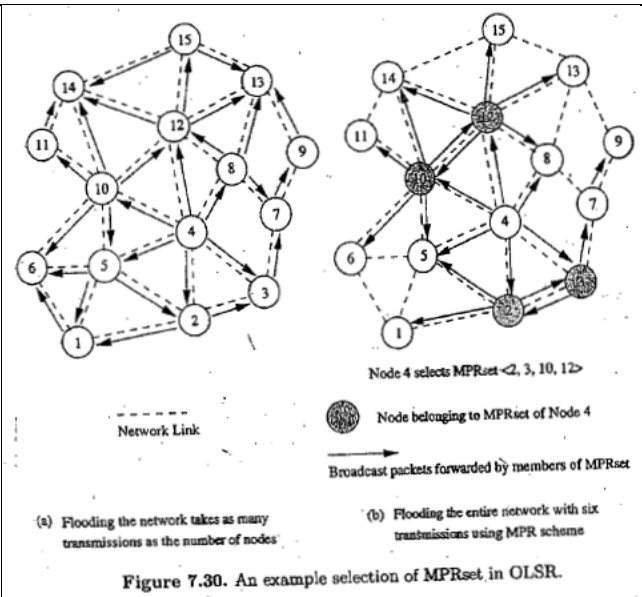


Figure 7.31. Example of HSR multi-level clustering.

3	**Explain the "optimal link state routing" with diagram** It is a proactive routing protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying (MPR). ▪ This protocol optimizes the pure link state routing protocol. ▪ Optimizations are done in two ways: o By reducing the size of control packets. o By reducing the no. of links that are used for forwarding the link state packets. ▪ The subset of links or neighbors that are designated for link state updates and are assigned the responsibility of packet forwarding are called multipoint relays. ▪ The set consisting of nodes that are multipoint relays is referred to as MPRset. ▪ Each node(say, P) in the n/w selects an MPRset that processes and forwards every link state packet that node P originates. ▪ The neighbor nodes that do not belong to the MPRset process the link state packets originated by node P but do not forward them. ▪ Similarly, each node maintains a subset of neighbors called MPR selectors, which is nothing but the set of neighbors that have selected the node as a multipoint relay. ▪ In order to decide on the membership of the nodes in the MPRset, a node periodically sends Hello messages that contain o List of neighbors with which the node has bidirectional links o List of neighbors whose transmission was received in the recent past but with whom bidirectional links have not yet been confirmed. ▪ The nodes that receive this Hello packet update their own two-hop topology tables. ▪ The selection of multipoint relays is also indicated in the Hello packet. ▪ The Data structure called neighbor table is used to store the list of neighbors, the two-hop neighbors, and the status of neighbor nodes. ▪ The neighbor nodes can be in one of the three possible link status states, i.e o Unidirectional o Bidirectional	10	CO3	L2

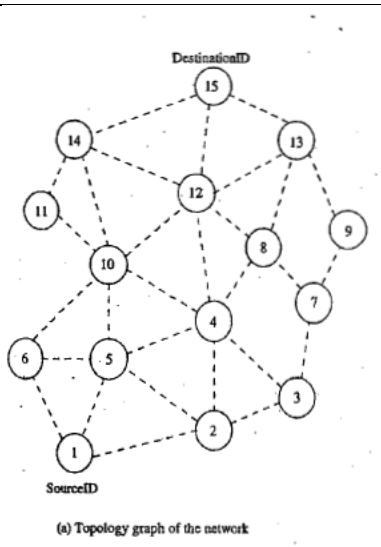
	 **Figure 7.30.** An example selection of MPRset in OLSR.			
4	**Explain the following proper aware routing metrics:** ***Minimal energy consumption per packet*** o This metric aims at minimizing the power consumed by a packet in traversing from source node to the destination node. o The energy consumed by a packet when traversing through a path is the sum of the energies required at every intermediate hop in that path. o This metric doesn't balance the load o Disadvantages o Selection of path with large hop length o Inability to measure the power consumption in advance o Inability to prevent the fast discharging of batteries at some nodes ▪ ***Maximize network connectivity*** o This metric attempt to balance the routing load among the cut set (the subset of the nodes in the network, the removal of which results in network partitions). ▪ ***Maximum variance in Node power levels*** o This metric proposes to distribute the load among all nodes in the network so that the power consumption pattern remains uniform across them. o This problem is very complex when the rate and size of the data packets vary ▪ ***Minimum cost per packet*** o In order to maximize the life of every node in the network, this routing metric is made as a function of the state of the node's battery. o A node's cost decreases with an increase in its battery change and vice versa. o Cost of node can be easily computed o Advantage → congestion handling & cost calculation ▪ ***Minimize maximum node cost*** o This metric minimizes the maximum cost per node for a packet after routing a number of packets or after a specific period. o This delays the failure of a node, occurring due to higher discharge because of packet forwarding	10	CO3	L3
5	**Discuss the adv and disadvantage of zone routing protocol and zone based hierarchical link state routing protocol** **Zone Routing Protocol** **Advantage** Reduce the control overhead by combining the best features of Proactive and Reactive protocols. **Disadvantage** Control overhead may increase due to the large overlapping of nodes routing zones.	5+5	CO3	L2

	Zone Based Hierarchical Routing protocol **Advantages** ▪ Reduce storage requirements and common overhead. ▪ Robust and resilient to path breaks. ▪ Non overlapping zones. **Disadvantages** ▪ Additional overhead incurred in creation of zone level topology. ▪ Path to Destination is suboptimal. ▪ Geographical info may not be available in all environments.			

6	E**xplain the key management in adhoc wireless n/w** Adhoc wireless networks pose certain specific challenges in key management, due to the lack of infrastructure in such networks. □ 3 types of infrastructure have been identified, which are absent in adhoc wireless networks: o The first is the network infrastructure, such as dedicated routers & stable links, which ensure communication with all nodes. o The second missing infrastructure is services, such as name resolution, directory & TTP's. o The third missing infrastructure in adhoc wireless network is the administrative support of certifying authorities. ***Password-Based Group Systems:*** □ A password-based system has been explored where, in the simplest case, a long string is given as the password for users for one session. □ However, human beings tend to favour natural language phrases as passwords, over randomly generated strings. □ Such passwords, if used as keys directly during a session, are very week & open to attack directly during a high redundancy, & the possibility of reuse over different sessions. □ Hence, protocols have been proposed to derive a strong key (not vulnerable to attacks). □ This password-based system could be two-party, with a separate exchange between any 2 participants, or it could be for the whole group, ***Threshold Cryptography:*** □ Public Key Infrastructure (PKI) enables the easy distribution of keys & is a scalable method. □ Each node has a public/private key pair,& a certifying authority (CA) can bind the keys to a particular node. But CA has to be present at all times, which may not be feasible in Adhoc wireless networks. □ A scheme based on threshold cryptography has been proposed by which n servers exist in an adhoc wireless network, out of which any (t+1) servers can jointly perform arbitration or authorization successfully, but t servers cannot perform the same. This is called an (n, t+1) configuration, where n >= 3t +1. □ To sign a certificate, each server generates a partial signature using its private key & submits it to a combiner. The combiner can be any one of the servers. o In order to ensure that the key is combined correctly, t+1 combiners can be used to account for at most t malicious servers. o Using t+1 partial signatures, the combiner computes a signature & verifies its validity using a public key.	10	CO4	L2

	○ If verification fails, it means that at least one of the t+1 keys is not valid, so another subset of t+1 partial signature is tried. If combiner itself is malicious, it cannot get a valid key, because partial key itself is always invalid. ***Self-Organised Public Key Management for Mobile Adhoc Networks:*** □ Self-organised public key system makes use of absolutely no infrastructure. □ The users in the adhoc wireless network issue certificates to each other based on personal acquaintance. □ A certificate is binding between a node & its public key. These certificates are stored & distributed by the users themselves. Certificates are issued only for specific period of time, before it expires; the certificate is updated by the user who had issued the certificate. □ Each certificate is initially stored twice, by the issuer & by the person for whom it is issued. □ If any of the certificates are conflicting (e.g: the same public key to different users, or the same user having different pubic keys), it is possible that a malicious node has issued a false certificate. □ A node then enables such certificates as conflicting & tries to resolve the conflict. □ If the certificates issued by some node are found to be wrong, then that node may be assumed to be malicious. □ A certificate graph is a graph whose vertices are public keys of some nodes and whose edges are public key certificates issued by users.			
7a	**Explain authenticated routing in adhoc wireless networks.** ARAN is a secure routing protocol which successfully defeats all identified attacks in the network layer ▪ It takes care of authentication, message integrity and non-repudiation ▪ During the route discovery process of ARAN, the source node broadcasts RouteRequest packets ▪ Destination packets responds by unicasting back a reply packet on the selected path ▪ The ARAN protocol uses a preliminary cryptographic certification process, followed by an end-to-end route authentication process, which ensures secure route establishment **ISSUE OF CERTIFICATES** ▪ There exists an authenticated trusted server whose public key is known to all legal nodes in the network ▪ The ARAN protocol assumes that keys are generated a priori by the server and distributed to all nodes in the network ▪ On joining the network, each node receives a certificate from the trusted server ▪ The certificate received by a node A from the trusted server T looks like the following: $T \rightarrow A: \ cert_A = [IP_A, K_{A+}, t, e]K_{T-}$ (9.12.1) Here, IP_A, K_{A+}, t, e, and K_{T-} represent the IP address of node A, the public key of node A, the time of creation of the certificate, the time of expiry of the certificate, and the private key of the server, respectively. **END-TO-END ROUTE AUTHENTICATION** ▪ The main goal of this end-to-end route authentication process is to ensure that the correct intended destination is reached by the packets sent from the source node ▪ The source node *S* broadcasts a *RouteRequest/RouteDiscovery* packet destined to destination node *D.* $S \rightarrow broadcasts := [RDP, IP_D, Cert_S, N_S, t]K_{S-}$ $A \rightarrow broadcasts := [[RDP, IP_D, Cert_S, N_S, t]K_{S-}]K_{A-}, Cert_A$ $D \rightarrow X := [REP, IP_S, Cert_D, N_S, t]K_{D-}$	05	CO4	L2

	K_{A+} Public key of node A. K_{A-} Private key of node A. K_{AB} Symmetric key shared by nodes A and B. $\{d\}K_{A+}$ Encryption of data d with key K_{A+}. $[d]K_{A-}$ Data d digitally signed by node A. cert_A Certificate belonging to node A. e Certificate expiration time. N_A Nonce issued by node A. IP_A IP address of node A. RDP Route Discovery Packet identifier. REP REPly packet identifier. t timestamp.			
7b.	**Explain Route Establishment in DSDV**. It is an enhanced version of the distributed Bellman-Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network. ▪ It incorporates table updates with increasing sequence number tags to prevent loops, to counter the count-to-infinity problem, and for faster convergence. ▪ As it is a table-driven routing protocol, routes to all destinations are readily available at every node at all times. ▪ The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology. ▪ The table updates are of two types: ○ ***Incremental updates:*** Takes a single network data packet unit (NDPU). These are used when a node does not observe significant changes in the local topology. ○ ***Full dumps:*** Takes multiple NDPUs. It is done either when the local topology changes significantly or when an incremental update requires more than a single NDPU. ▪ Table updates are initiated by a destination with a new sequence number which is always greater than the previous one. ▪ Consider the example as shown in figure (a). Here node 1 is the source node and node 15 is the destination. As all the nodes maintain global topology information, the route is already available as shown in figure (b). ▪ Here the routing table node 1 indicates that the shortest route to the destination node is available through node 5 and the distance to it is 4 hops, as depicted in figure (b) ▪ The reconfiguration of a path used by an on-going data transfer session is handled by the protocol in the following way. ▪ The end node of the broken link initiates a table update message with the broken link's weight assigned to infinity (∞) and with a sequence number greater than the stored sequence number for that destination. ▪ Each node upon receiving an update with weight ∞, quickly disseminates it to its neighbors in order to propagate the broken-link information to the whole network. ▪ A node always assign an odd number to the link break update to differentiate it from the even sequence number generated by the destination. ▪ Figure 7.6 shows the case when node 11 moves from its current position.	05	CO4	L2

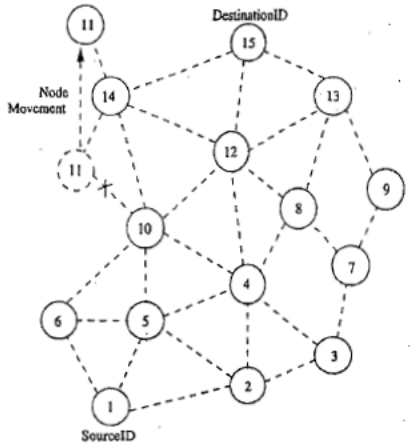


(a) Topology graph of the network

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b) Routing table for Node 1

Figure 7.5. Route establishment in DSDV.



Routing Table for Node 1

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

Figure 7.6. Route maintenance in DSDV.

8a **Explain Fisheye State Routing in detail.** 05 CO4 L2

FishEye State Routing Protocol (FSR)

- It is a generalization of the GSR protocol.
- It uses Fisheye technique to reduce the routing overhead.
- Principle: Property of a fish's eye that can capture pixel information with greater accuracy near its eye's focal point.
- This accuracy decreases with an increase in the distance from the center of the focal point
- This property is translated to routing in adhoc wireless networks by a node
- Each node maintains accurate information about near nodes.
- Nodes exchange topology information only with their neighbors.
- A sequence numbering scheme is used to identify the recent topology changes
- This constitutes a link-level information exchange of distance vector protocols and complete topology information exchange of link state protocols.
- FSR defines routing scope, which is the set of nodes that are reachable in a specific no. of hops.
- The scope of a node at two hops is the set of nodes that can be reached in two hops fig 7.32 shows scope of node 5 with one hop and two hops.
- The routing overhead is significantly reduced

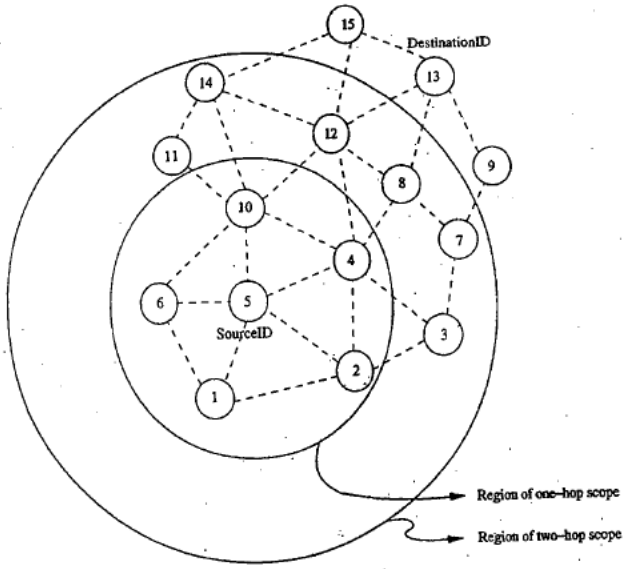


Figure 7.32. Fisheye state routing.

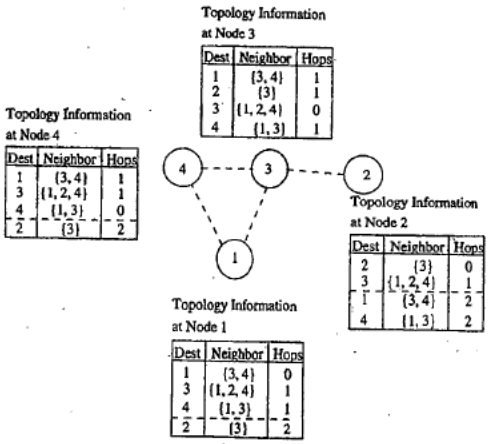


Figure 7.33. An illustration of routing tables in FSR.

The link state info for the nodes belonging to the smallest scope is exchanged at the highest frequency. Frequency of exchanges decreases with an increase in scope.

- Fig 7.33 illustrates an example depicting the n/w topology information maintained at nodes in a n/w.
- Message size for a typical topology information update packet is significantly reduced
- The routing information for the nodes that are one hop away from a node are exchanged more frequently than the routing information about nodes that are more than one hop away
- Information regarding nodes that are more than one hop away from the current node are listed below the dotted line in the topology table.

Advantages

- Reduce bandwidth consumption by link state update packets.
- Suitable for large and highly mobile adhoc wireless network.

Disadvantages

- Very poor performance in small adhoc networks

8b	**Explain TORA** Source-initiated on-demand routing protocol ▪ Uses a link reversal algorithm ▪ Provides loop free multi path routes to the destination	05	CO4	L2

- Each node maintains its one-loop local topology information
- Has capability to detect partitions
- Unique property → limiting the control packets to a small region during the reconfiguration process initiated by a path break

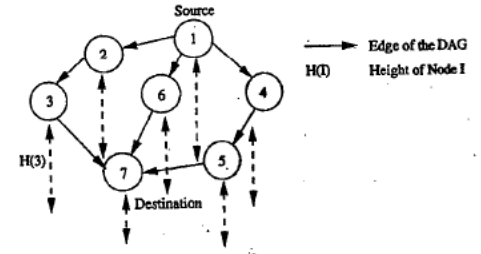


Figure 7.14. Illustration of temporal ordering in TORA.

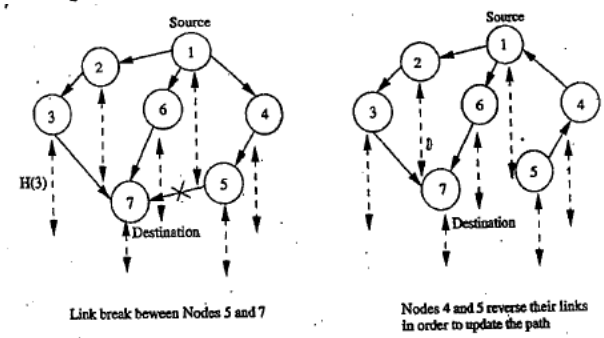


Figure 7.15. Illustration of route maintenance in TORA.

TORA has 3 main functions: establishing, maintaining and erasing routes

- The route establishment function is performed only when a node requires a path to a destination but does not have any directed link
- This process establishes a destination-oriented directed acyclic graph using a query/update mechanism
- Once the path to the destination is obtained, it is considered to exist as long as the path is available, irrespective of the path length changes due to the re-configurations that may take place during the course of data transfer session
- If the node detects a partition, it originated a clear message, which erases the existing path information in that partition related to the destination

Advantages

- Incur less control overhead
- Concurrent detection of partitions
- Subsequent deletion of routes

Disadvantages

- Temporary oscillations and transient loops

Local reconfiguration of paths result in non-optimal routes

6	Explain the key management in adhoc wireless n/w	10	CO4	L2
7a	Explain authenticated routing in adhoc wireless networks.	05	CO4	L2
7b.	Explain Route Establishment in DSDV.	05	CO4	L2
8a	Explain Fisheye State Routing in detail.	05	CO4	L2
8b	Explain TORA	05	CO4	L2