© 2016 IJSRSET | Volume 2 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Literature Review of MANET's Routing Protocols Along With Security Issues

Anil Lamba[1], Sohan Garg[2], Rajeev Kumar[3]

[1]Research Scholar, Sri Venkteshwara University Gajraula, Amroha, Uttar Pradesh, India
[2]SCRIET- CCS University, Meerut, Uttar Pradesh, India
[3]Sri Venkteshwara University Gajraula, Uttar Pradesh, India

ABSTRACT

In infrastructure based networks, in ad hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. Ad hoc networks are very useful in emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrain [1]. This article discusses proposed routing protocols for these ad hoc networks. These routing protocols can be divided into two categories: table-driven and on-demand routing based on when and how the routes are discovered. In table driven routing protocols consistent and up-to-date routing information to all nodes is maintained at each node whereas in on-demand routing the routes are created only when desired by the source host. We are also discussing here the security issues related to routing protocols.

Keywords: AODV, DSDV, WRP, GSR

I. INTRODUCTION

Wireless networks is an emerging new technology that will allow users to access information and services electronically, regardless of their geographic position. Wireless networks can be classified in two types:- infrastructured network and infrastructureless (ad hoc) networks. Infrastructured network consists of a network with fixed and wired gateways. A mobile host communicates with a bridge in the network (called base station) within its communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This is called handoff. In this approach the base stations are fixed.

II. METHODS AND MATERIAL

2. Table Driven Routing Protocols

In Table-driven routing protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables so as to maintain a consistent and up-to-date view of the network. When the network topology changes the nodes propagate update messages throughout the network in order to maintain a consistent and up-to-date routing information about the whole network. These routing protocols differ in the method by which the topology change information is distributed across the network and the number of necessary routing-related tables. The following sections discuss some of the existing table-driven ad hoc routing protocols.

2.1 Dynamic Destination-Sequenced Distance-Vector Routing Protocol

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm [2] is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements.

Every mobile station maintains a routing table that lists all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination node. The sequence number is used to

distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven. The routing table updates can be sent in two ways:- a "full dump" or an incremental update. A full dump sends the full routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. If there is space in the incremental update packet then those entries may be included whose sequence number has changed.

2.2 The Wireless Routing Protocol (WRP)

The Wireless Routing Protocol (WRP) [3]is a table-based distance-vector routing protocol. Each node in the network maintains a Distance table, a Routing table, a Link-Cost table and a Message Retransmission list.

The Distance table of a node x contains the distance of each destination node y via each neighbor z of x. It also contains the downstream neighbor of z through which this path is realized. The Routing table of node x contains the distance of each destination node y from node x, the predecessor and the successor of node x on this path. It also contains a tag to identify if the entry is a simple path, a loop or invalid. Storing predecessor and successor in the table is beneficial in detecting loops and avoiding counting-to-infinity problems. The Link-Cost table contains cost of link to each neighbor of the node and the number of timeouts since an error-free message was received from that neighbor. The Message Retransmission list (MRL) contains information to let a node know which of its neighbor has not acknowledged its update message and to retransmit update message to that neighbor.

Node exchange routing tables with their neighbors using update messages periodically as well as on link changes. The nodes present on the response list of update message (formed using MRL) are required to acknowledge the receipt of update message. If there is no change in routing table since last update, the node is required to send an idle Hello message to ensure connectivity. On receiving an update message, the node modifies its distance table and looks for better paths using new information. Any new path so found is relayed back to the original nodes so that they can update their tables. The node also updates its routing table if the new path is better than the existing path. On receiving an ACK, the mode updates its MRL. A unique feature of this algorithm is that it checks the consistency of all its neighbors every time it detects a change in link of any of its neighbors. Consistency check in this manner helps eliminate looping situations in a better way and also has fast convergence.

2.3 Global State Routing

Global State Routing (GSR) [3]is similar to DSDV described in section 2.1. It takes the idea of link state routing but improves it by avoiding flooding of routing messages.

In this algorithm, each node maintains a Neighbor list, a Topology table, a Next Hop table and a Distance table. Neighbor list of a node contains the list of its neighbors (here all nodes that can be heard by a node are assumed to be its neighbors.). For each destination node, the Topology table contains the link state information as reported by the destination and the timestamp of the information. For each destination, the Next Hop table contains the next hop to which the packets for this destination must be forwarded. The Distance table contains the shortest distance to each destination node.

The routing messages are generated on a link change as in link state protocols. On receiving a routing message, the node updates its Topology table if the sequence number of the message is newer than the sequence number stored in the table. After this the node reconstructs its routing table and broadcasts the information to its neighbors.

2.4 Fisheye State Routing

Fisheye State Routing (FSR) [4]is an improvement of GSR. The large size of update messages in GSR wastes a considerable amount of network bandwidth. In FSR, each update message does not contain information about all nodes. Instead, it exchanges information about closer nodes more frequently than it does about farther nodes thus reducing the update message size. So each node gets accurate information about neighbors and the detail and accuracy of information decreases as the distance from node increases. Figure 1 defines the scope of

fisheye for the center (red) node. The scope is defined in terms of the nodes that can be reached in a certain number of hops. The center node has most accurate information about all nodes in the white circle and so on. Even though a node does not have accurate information about distant nodes, the packets are routed correctly because the route information becomes more and more accurate as the packet moves closer to the destination. FSR scales well to large networks as the overhead is controlled in this scheme.

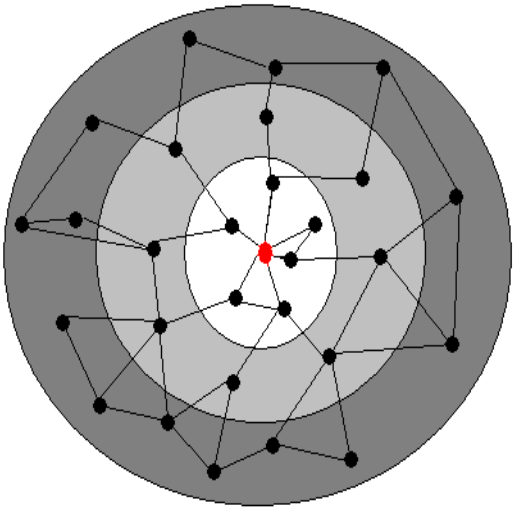


Figure 1. Accuracy of information in FSR

2.5 Hierarchical State Routing

The characteristic feature of Hierarchical State Routing (HSR) [5]is multilevel clustering and logical partitioning of mobile nodes. The network is partitioned into clusters and a cluster-head elected as in a cluster-based algorithm. In HSR, the cluster-heads again organize themselves into clusters and so on. The nodes of a physical cluster broadcast their link information to each other. The cluster-head summarizes its cluster's information and sends it to neighboring cluster-heads via gateway (section 2.2). As shown in the figure 2, these cluster-heads are member of the cluster on a level higher and they exchange their link information as well as the summarized lower-level information among each other and so on. A node at each level floods to its lower level the information that it obtains after the algorithm has run at that level. So the lower level has a hierarchical topology information. Each node has a hierarchical address. One way to assign hierarchical address is the cluster numbers on the way from root to the node as shown in figure 2. A gateway can be reached from the root via more than one path, so gateway can have more than one hierarchical address. A hierarchical address is enough to ensure delivery from anywhere in the network to the host.

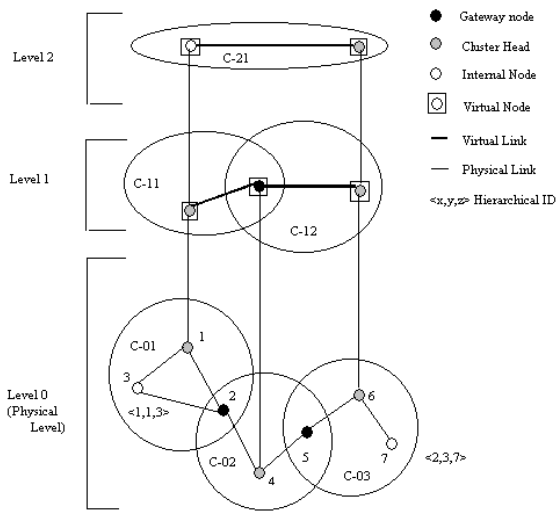


Figure 2. An example of clustering in HSR

In addition, nodes are also partitioned into logical subnetworks and each node is assigned a logical address <subnet, host>. Each subnetwork has a location management server (LMS). All the nodes of that subnet register their logical address with the LMS. The LMS advertise their hierarchical address to the top levels and the information is sent down to all LMS too. The transport layer sends a packet to the network layer with the logical address of the destination. The network layer finds the hierarchical address of the hierarchical address of the destinationÆs LMS from its LMS and then sends the packet to it. The destinationÆs LMS forwards the packet to the destination. Once the source and destination know each otherÆs hierarchical addresses, they can bypass the LMS and communicate directly. Since logical address/hierarchical address is used for routing, it is adaptable to network changes.

2.6 Zone-based Hierarchical Link State Routing Protocol

In Zone-based Hierarchical Link State Routing Protocol (ZHLS) [5], the network is divided into non-overlapping zones. Unlike other hierarchical protocols, there is no zone-head. ZHLS defines two levels of topologies - node level and zone level. A node level topology tells how nodes of a zone are connected to each other physically. A virtual link between two zones exists if at least one node of a zone is physically connected to some

node of the other zone. Zone level topology tells how zones are connected together. There are two types of Link State Packets (LSP) as well - node LSP and zone LSP. A node LSP of a node contains its neighbor node information and is propagated with the zone where as a zone LSP contains the zone information and is propagated globally. So each node has full node connectivity knowledge about the nodes in its zone and only zone connectivity information about other zones in the network. So given the zone id and the node id of a destination, the packet is routed based on the zone id till it reaches the correct zone. Then in that zone, it is routed based on node id. A <zone id, node id@gt; of the destination is sufficient for routing so it is adaptable to changing topologies.

2.7 Clusterhead Gateway Switch Routing Protocol

Clusterhead Gateway Switch Routing (CGSR) [6]uses as basis the DSDV Routing algorithm described in the previous section.

The mobile nodes are aggregated into clusters and a cluster-head is elected. All nodes that are in the communication range of the cluster-head belong to its cluster. A gateway node is a node that is in the communication range of two or more cluster-heads. In a dynamic network cluster head scheme can cause performance degradation due to frequent cluster-head elections, so CGSR uses a Least Cluster Change (LCC) algorithm. In LCC, cluster-head change occurs only if a change in network causes two cluster-heads to come into one cluster or one of the nodes moves out of the range of all the cluster-heads.

The general algorithm works in the following manner. The source of the packet transmits the packet to its cluster-head. From this cluster-head, the packet is sent to the gateway node that connects this cluster-head and the next cluster-head along the route to the destination. The gateway sends it to that cluster-head and so on till the destination cluster-head is reached in this way. The destination cluster-head then transmits the packet to the destination. Figure 3 shows an example of CGSR routing scheme.

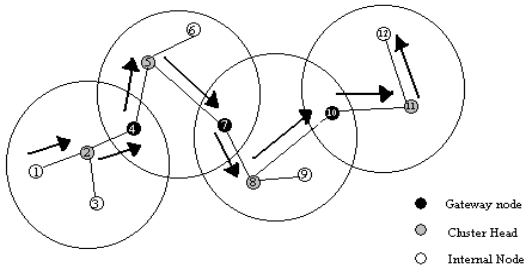


Figure 3. Example of CGSR routing from node 1 to node 12

Each node maintains a cluster member table that has mapping from each node to its respective cluster-head. Each node broadcasts its cluster member table periodically and updates its table after receiving other nodeÆs broadcasts using the DSDV algorithm. In addition, each node also maintains a routing table that determines the next hop to reach the destination cluster.

On receiving a packet, a node finds the nearest cluster-head along the route to the destination according to the cluster member table and the routing table. Then it consults its routing table to find the next hop in order to reach the cluster-head selected in step one and transmits the packet to that node.

3. On-Demand Routing Protocols

These protocols take a lazy approach to routing. In contrast to table-driven routing protocols all up-to-date routes are not maintained at every node, instead the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid till the destination is reachable or until the route is no longer needed. This section discusses a few on-demand routing protocols.

3.1 Cluster based Routing Protocols

In Cluster Based Routing protocol (CBRP) [6], the nodes are divided into clusters. To form the cluster the following algorithm is used. When a node comes up, it enters the "undecided" state, starts a timer and broadcasts a Hello message. When a cluster-head gets this hello message it responds with a triggered hello message immediately. When the undecided node gets this message it sets its state to "member". If the undecided node times out, then it makes itself the cluster-head if it has bi-directional link to some neighbor

otherwise it remains in undecided state and repeats the procedure again. Clusterheads are changed as infrequently as possible.

Each node maintains a neighbor table. For each neighbor, the neighbor table of a node contains the status of the link (uni- or bi-directional) and the state of the neighbor (cluster-head or member). A cluster-head keeps information about the members of its cluster and also maintains a cluster adjacency table that contains information about the neighboring clusters. For each neighbor cluster, the table has entry that contains the gateway through which the cluster can be reached and the cluster-head of the cluster.

When a source has to send data to destination, it floods route request packets (but only to the neighboring cluster-heads). On receiving the request a cluster-head checks to see if the destination is in its cluster. If yes, then it sends the request directly to the destination else it sends it to all its adjacent cluster-heads. The cluster-heads address is recorded in the packet so a cluster-head discards a request packet that it has already seen. When the destination receives the request packet, it replies back with the route that had been recorded in the request packet. If the source does not receive a reply within a time period, it backs off exponentially before trying to send route request again.

In CBRP, routing is done using source routing. It also uses route shortening that is on receiving a source route packet, the node tries to find the farthest node in the route that is its neighbor (this could have happened due to a topology change) and sends the packet to that node thus reducing the route. While forwarding the packet if a node detects a broken link it sends back an error message to the source and then uses local repair mechanism. In local repair mechanism, when a node finds the next hop is unreachable, it checks to see if the next hop can be reached through any of its neighbor or if hop after next hop can be reached through any other neighbor. If any of the two works, the packet can be sent out over the repaired path.

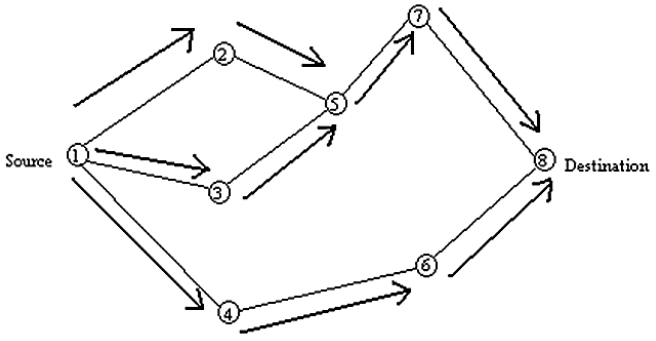
3.2 Ad hoc On-demand Distance Vector Routing

Ad hoc On-demand Distance Vector Routing (AODV) [7]is an improvement on the DSDV algorithm discussed in section 2.1. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes.

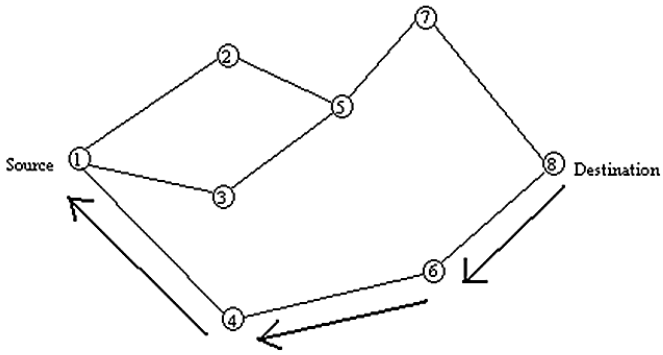
To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has a recent route information about the destination or till it reaches the destination (Figure 4a). A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only.

When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source (Figure 4b), the nodes along the path enter the forward route into their tables.

If the source moves then it can reinitiate route discovery to the destination. If one of the intermediate nodes move then the moved nodes neighbor realizes the link failure and sends a link failure notification to its upstream neighbors and so on till it reaches the source upon which the source can reinitiate route discovery if needed.



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

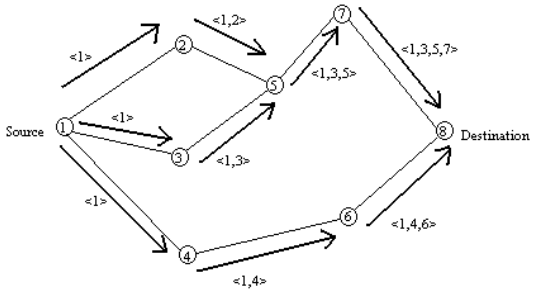
Figure 4. Route discovery in AODV

3.3 Dynamic Source Routing Protocol

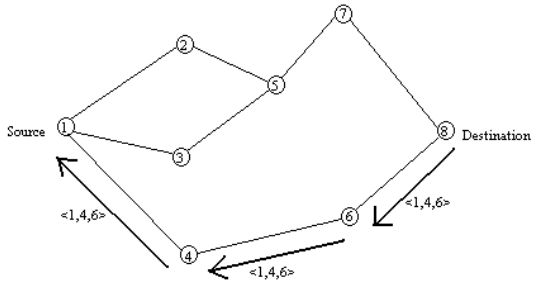
The Dynamic Source Routing Protocol [8]is a source-routed on-demand routing protocol. A node maintains route caches containing the source routes that it is aware of. The node updates entries in the route cache as and when it learns about new routes.

The two major phases of the protocol are: route discovery and route maintenance. When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a route request packet. The route request packet contains the address of the source and the destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors. To limit the number of route requests propagated, a node processes the route request packet only if it has not already seen the packet and it's address is not present in the route record of the packet.

A route reply is generated when either the destination or an intermediate node with current information about the destination receives the route request packet [8]. A route request packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node.



(a) Building Record Route during Route Discovery



(b) Propogation of Route Reply with the Route Record

Figure 5. Creation of record route in DSRP

As the route request packet propagates through the network, the route record is formed as shown in figure 5a. If the route reply is generated by the destination then it places the route record from route request packet into the route reply packet. On the other hand, if the node generating the route reply is an intermediate node then it appends its cached route to destination to the route record of route request packet and puts that into the route reply packet. Figure 5b shows the route reply packet being sent by the destination itself. To send the route reply packet, the responding node must have a route to the source. If it has a route to the source in its route cache, it can use that route. The reverse of route record can be used if symmetric links are supported. In case symmetric links are not supported, the node can initiate route discovery to source and piggyback the route reply on this new route request.

DSRP uses two types of packets for route maintenance:- Route Error packet and Acknowledgements. When a node encounters a fatal transmission problem at its data link layer, it generates a Route Error packet. When a node receives a route error packet, it removes the hop in error from it's route cache. All routes that contain the hop in error are are truncated at that point. Acknowledgment packets are used to verify the correct operation of the route links. This also includes passive

acknowledgments in which a node hears the next hop forwarding the packet along the route.

3.4 Temporally Ordered Routing Algorithm

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal [8]. TORA is proposed for highly dynamic mobile, multihop wireless networks. It is a source-initiated on-demand routing protocol. It finds multiple routes from a source node to a destination node. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. To achieve this, the nodes maintain routing information about adjacent nodes. The protocol has three basic functions: Route creation, Route maintenance, and Route erasure.

Each node has a quintuple associated with it -

- Logical time of a link failure
- The unique ID of the node that defined the new reference level
- A reflection indicator bit
- A propagation ordering parameter
- The unique ID of the node

The first three elements collectively represent the reference level. A new reference level is defined each time a node loses its last downstream link due to a link failure. The last two values define a delta with respect to the reference level [8].

Route Creation is done using QRY and UPD packets. The route creation algorithm starts with the height (propagation ordering parameter in the quintuple) of destination set to 0 and all other node's height set to NULL (i.e. undefined). The source broadcasts a QRY packet with the destination node's id in it. A node with a non-NULL height responds with a UPD packet that has its height in it. A node receiving a UPD packet sets its height to one more than that of the node that generated the UPD. A node with higher height is considered upstream and a node with lower height downstream. In this way a directed acyclic graph is constructed from source to the destination. Figure 6 illustrates a route creation process in TORA. As shown in figure 6a, node 5 does not propagate QRY from node 3 as it has already seen and propagated QRY message from node 2. In figure 6b, the source (i.e. node 1) may have received a UPD each from node 2 or node 3 but since node 4 gives it lesser height, it retains that height.

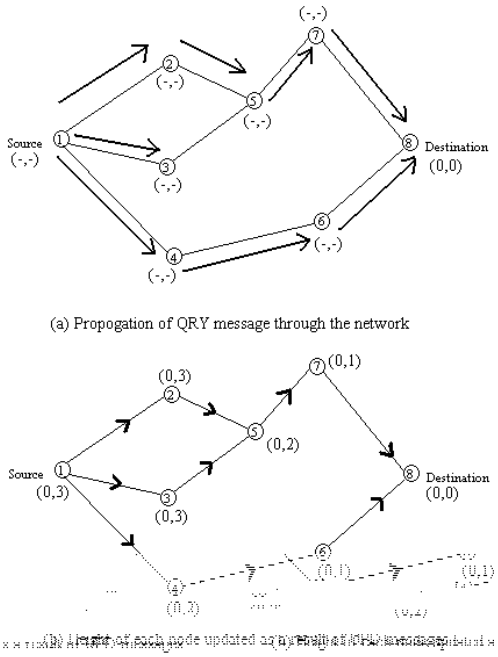


Figure 6. Route creation in TORA. (Numbers in braces are reference level, height of each node)

When a node moves the DAG route is broken, and route maintenance is needed to reestablish a DAG for the same destination. When the last downstream link of a node fails, it generates a new reference level. This results in the propagation of that reference level by neighboring nodes as shown in figure 7. Links are reversed to reflect the change in adapting to the new reference level. This has the same effect as reversing the direction of one or more links when a node has no downstream links.

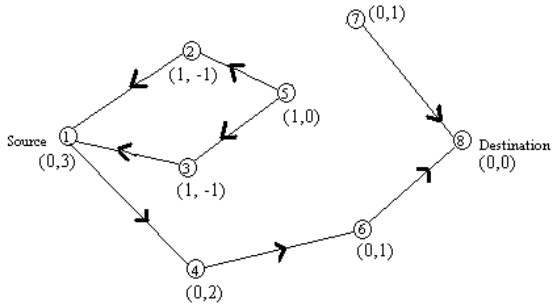


Figure 7. Re-establishing route on failure of link 5-7. The new reference level is node 5.

In the route erasure phase, TORA floods a broadcast clear packet (CLR) throughout the network to erase invalid routes.

In TORA there is a potential for oscillations to occur, especially when multiple sets of coordinating nodes are concurrently detecting partitions, erasing routes, and building new routes based on each other. Because TORA uses internodal coordination, its instability problem is similar to the "count-to-infinity" problem in distance-vector routing protocols, except that such oscillations are temporary and route convergence will ultimately occur.

III. RESULTS AND DISCUSSION

Security Issues In Routing Protocols

MANET's unique characteristics make it affected by several types of attacks. Since they are used in an open environment where all nodes can change their position at any time to some other place, all the nodes should co-operate to forward the packets in the network. So detecting the malicious nodes is also a difficult task in MANET. Hence, it is relatively difficult to design a secure protocol for MANET, when compared to wired or infrastructure–based wireless networks. This section discusses the security goals for an ad hoc network. Also it discusses the various layer attacks in MANET.

To secure the routing protocols in MANETs, researchers have considered the following security services specified by Bing Wu, et al. : Availability, confidentiality, integrity, authentication and non-repudiation.

[a] Availability guarantees the survivability of the network services despite attacks. A DoS (Denial-of-Service) is a potential threat at any layer of an ad hoc network. On the Media Access Control (MAC) layer, an adversary could jam the physical communication channels. On the network layer disruption of the routing operation may result in a partition of the network, rendering certain nodes inaccessible. On higher levels, an attacker could bring down high-level services like key management service.

[b] Confidentiality ensures that certain information be never disclosed to unauthorized entities. It is of paramount importance to strategic or tactical military communications. Routing information must also remain confidential in some cases, because the information might be valuable for enemies to locate their targets in a battlefield.

[c] Integrity ensures that a message that is on the way to the destination is never corrupted. A message could be corrupted because of channel noise or because of malicious attacks on the network.

[d] Authentication enables a node to ensure the identity of the peer node. Without authentication, an attacker could masquerade as a normal node, thus gaining access to sensitive information.

[e] Non-repudiation ensures that the originator of a message cannot deny that it is the real originator. Non-repudiation is important for detection and isolation of compromised nodes.

The networking environment in wireless schemes makes the routing sessions vulnerable to attacks ranging from passive eavesdropping to active attacks such as impersonation, message reply, message littering, network partitioning, etc. Eavesdropping is a threat to confidentiality and active attacks are threats to availability, integrity, authentication and non-repudiation. Nodes roaming in an ad hoc environment with poor physical protection are quite vulnerable and they may be compromised. Once the nodes are compromised, they can be used as starting points to launch attacks against the routing protocols.

The MANET routing protocols are facing different routing attacks such as flooding, black hole, link withholding, link spoofing, replay, wormhole and colluding misrelay attacks. A comprehensive study of these routing attacks and countermeasures against these attacks in MANET can be found . The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications , while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are snooping , eavesdropping, traffic analysis, and traffic monitoring . Examples of active attacks include jamming,

impersonation, modification, denial of service (DoS), and message replay.

The attacks can also be classified into two categories, namely external attacks and internal attacks, according to the domain of the attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights. Bing Wu, et al. classified the attacks according to network protocol stacks . They are physical layer attacks, Link layer attacks, Network layer attacks, Transport layer attacks and Application layer attacks.

Eavesdropping is the intercepting and reading of messages and conversations by unintended receivers. The mobile hosts in mobile ad hoc networks share a wireless medium. The majority of wireless communications use the RF spectrum and broadcast by nature. Signals broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency. Thus, messages transmitted can be eavesdropped, and fake messages can be injected into network. Moreover, a radio signal can be jammed or interfered, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. The most common types of this form of signal jamming are random noise and pulse. Jamming equipment is readily available. In addition, jamming attacks can be mounted from a location remote to the target networks.

There are malicious routing attacks that target the routing discovery or maintenance phase by not following the specifications of the routing protocols. Routing message flooding attacks, such as hello flooding, RREQ flooding, acknowledgement flooding, routing table overflow, routing cache poisoning, and routing loop are simple examples of routing attacks targeting the route discovery phase.

Proactive routing algorithms, such as DSDV and OLSR, attempt to discover routing information before it is need, while reactive algorithms, such as DSR and AODV, create routes only when they are needed. Thus, proactive algorithms are more vulnerable to routing table overflow attacks. Some of these attacks are listed below.

a) Routing table overflow attack: A malicious node advertises routes that go to non-existent nodes to the authorized nodes present in the network. It usually happens in proactive routing algorithms, which update routing information periodically. The attacker tries to create enough routes to prevent new routes from being created. The proactive routing algorithms are more vulnerable to table overflow attacks because proactive routing algorithms attempt to discover routing information before it is actually needed. An attacker can simply send excessive route advertisements to overflow the victim's routing table.

b) Routing cache poisoning attack: In route cache poisoning attacks, attackers take advantage of the promiscuous mode of routing table updating, where a node overhearing any packet may add the routing information contained in that packet header to its own route cache, even if that node is not on the path. Suppose a malicious node M wants to poison routes to node X. M could broadcast spoofed packets with source route to X via M itself; thus, neighboring nodes that overhear the packet may add the route to their route caches.

There are attacks that target the route maintenance phase by broadcasting false control messages, such as link-broken error messages, which cause the invocation of the costly route maintenance or repairing operation. For example, AODV and DSR implement path maintenance procedures to recover broken paths when nodes move. If the destination node or an intermediate node along an active path moves, the upstream node of the broken link broadcasts a route error message to all active upstream neighbors. The node also invalidates the route for this destination in its routing table. Attackers could take advantage of this mechanism to launch attacks by sending false route error messages.

More sophisticated and subtle routing attacks have been identified in recent research papers. The black hole (or sinkhole), Byzantine, and wormhole attacks are the typical examples, which are described in detail below.

a) Wormhole attack: An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing

control messages is tunneled. This tunnel between two colluding attackers is referred to as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

b) Black hole attack: The black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrongdoing.

c) Byzantine attack: A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

d) Rushing attack: Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack . The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne.

e) Resource consumption attack: This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

f) Location disclosure attack: An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios. Traffic analysis, one of the subtlest security attacks against MANET, is unsolved. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security sensitive scenarios.

All the nodes in a mobile Ad hoc network depend on battery power for their operation. The alternate power sources are assumed to be absent. The adversary can send huge traffic to the target node. The target node may be continuously busy in handling these packets; this will cause the battery power to be exhausted. This will cause a denial of service (DOS) attack because now the node will not be able to provide services within the network. Sometimes the attackers ask the nodes to perform some meaningless time-consuming computation causing its battery power to be lost. Some nodes may behave as selfish nodes . A selfish node does not cooperate when running some common algorithm. For example consider a cluster based intrusion detection technique where a cluster of nodes cooperatively detects the intrusion. A node is selected as a monitor when it wishes to do this. A malicious behavior simply avoids being the monitor. When majority of nodes behave selfishly, the whole system will collapse.

The scalability of the mobile ad hoc network keeps changing all the time. It is very difficult to predict the number of nodes in a mobile ad hoc network at some future time. The protocols and services designed for MANETs must be made compatible to this changing scalability.

IV. REFERENCES

[1] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, Vol. 6, No. 2, pp. 46-55, April 1999.

[2] C.E. Perkins and P. Bhagwat, "Highly Dy-namic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Comp. Comm.

Rev., Oct. 1994, pp.234-244. http://www.svrloc.org/~charliep/txt/sigcomm94/paper.ps

[3] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel" Proc. IEEE SICON'97, Apr.1997, pp.197-211. http://www.ics.uci.edu/~atm/adhoc/paper-collection/gerla-routing-clustered-sicon97.pdf

[4] S. Murthy and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Net-works", ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communica-tion Networks, Oct. 1996, pp. 183-97. http://www.ics.uci.edu/~atm/adhoc/paper-collection/aceves-routing-winet.pdf

[5] Tsu-Wei Chen and Mario Gerla, "Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks" Proc. IEEE ICC'98, 5 pages. http://www.ics.uci.edu/~atm/adhoc/paper-collection/gerla-gsr-icc98.pdf

[6] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks" IEEE Journal on Se-lected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1369-79. http://www.cs.ucla.edu/NRL/wireless/PAPER/jsac99.ps.gz

[7] M Joa-Ng and I.-T. Lu, "A Peer-to-Peer zone-based two-level link state routing for mobile Ad Hoc Networks" IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, Aug. 1999, pp.1415-25.

[8] Mingliang Jiang, Jinyang Li, Y.C. Tay, "Clus-ter Based Routing Protocol" August 1999 IETF Draft, 27 pages.