Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Review of Various Routing Protocols in MANETs

Saivy Jain
Department of Information & Technology
AIET (Adesh Institute of Engineering and Technology), P.T.U

Abstract— Mobile Ad-hoc networks are composed of various interconnections among large number of nodes deployed for monitoring the system by means of measurement of its parameters. Recent research in wireless sensor networks has led to various new protocols which are particularly designed for routing in MANETs. To design these networks, the factors needed to be considered are the coverage area, mobility, power consumption, communication capabilities etc. In this paper a survey is given regarding the OLSR, TORA, AODV and DSDV routing protocols used in MANET. The paper attempts to explore the best suited routing protocol in various conditions and environments.

Keywords— Mobile ad hoc networks, Routing protocols OLSR, TORA and AODV

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is an autonomous system of nodes (MSs) connected by wireless links. They do not necessarily need support from any existing network infrastructure like an Internet gateway or other fixed stations. The network's wireless topology may dynamically change in an unpredictable manner since nodes are free to move. Each node is equipped with a wireless transmitter and a receiver with an appropriate antenna. When the nodes are close-by i.e., within radio range, there are no routing issues to be addressed but sometimes if nodes are not in range of each other they may face the problem in routing. In those cases nodes possibly build the connection by contacting the nearby accessible nodes up to the destination. Above figure1 shows the basic working of MANETs.

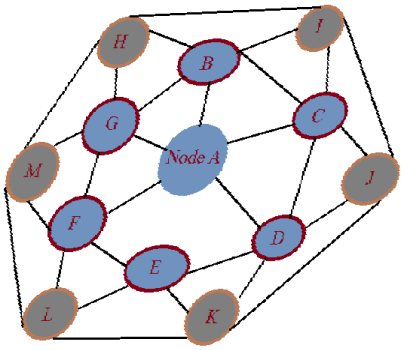

Figure 1: Mobile Ad-hoc Networks

Here we discuss some **examples** of MANETs which in used in our general life.

Military battlefield: **-** Ad-Hoc networking would allow the military to take advantage of common place network technology to maintain an information network between the soldiers, vehicles, and military information head quarter.

***Collaborative* work: -** For some business environments, the need for collaborative computing might be more important outside office environments.

Local level:- Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants. ***Personal area network and Bluetooth:-*** A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANETs such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.

***Commercial Sector*:-** Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or

Earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

II. ATTRIBUTES OF MANETs

Dynamic topologies:- Nodes are free to move arbitrarily in any direction thus the topology of the network change unpredictably.

Bandwidth constrained, variable capacity links:- The bandwidth available for wireless networks is generally low than that of wired networks. The throughput of these networks is generally low due various noises, fading effects.

Energy-constrained operation:- The nodes are portable devices and are dependent on batteries. This is the most important design consideration of the MANETs.

Limited physical security:- wireless networks are more prone to threats then wired networks. The increased possibility of various security attacks like eavesdropping, denial of service should be handled carefully.

Hidden terminal problem:- The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

Routing Overhead:- In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

III. CATEGORIZATION OF ROUTING PROTOCOLS

Routing protocols are those which set some rules and regulation for the transferring or receiving the data from one node to another node. Now, here in MANETs there are various types of routing protocols which are utilized according to the routing status or conditions. Above Figure2 shows the fundamental categories of routing protocols.

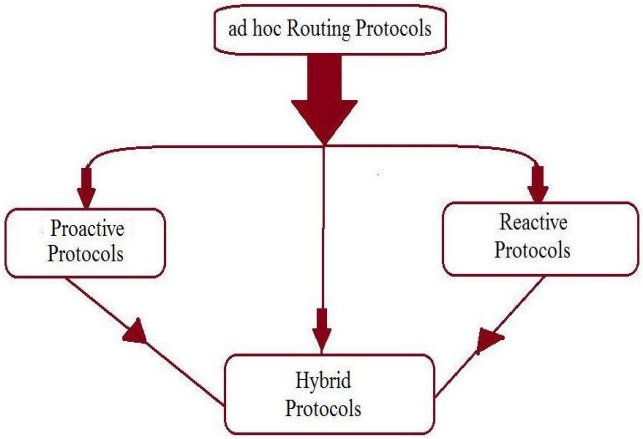

Figure 2: Categorization of routing protocols

Reactive routing protocol:- In this protocol route is discovered whenever it is needed Nodes initiate route discovery on demand basis. In this when a node want o communicate with another node then for establishing the route it follow these processes i.e. Route discovery and Route maintenance.

Route discovery:- In this phase source node initiates route discovery on demand basis. Source nodes consults its route cache for the available route from source to destination otherwise if the route is not present it initiates route discovery. The source node, in the packet, includes the destination address of the node as well address of the intermediate nodes to the destination.

Route maintenance:- Due to dynamic topology of the network cases of the route failure between the nodes arises due to link breakage etc, so route maintenance is done. Reactive protocols have acknowledgement mechanism due to which route maintenance is possible.

There are many types routing protocols are there in ad hoc networks i.e**. DSR, AODV and TORA** and so on.

Proactive routing protocol:- In this phase each node in the network maintains their own routing table that might be one or more. If there is any change in any topology of a network then each node start sending broadcast message to the entire network. This feature although useful for datagram traffic, incurs substantial signalling traffic and power consumption. These are not suitable for large networks as they need to maintain node entries for each and every node in the routing table of every node. They also maintain different number of routing tables varying from protocol to protocol.

There are various types of proactive routing protocols which are **DSDV, OLSR and WRP** and so on. In this above Figure3.Overview of routing protocols is there which are classified according to the basic categories of routing protocols.

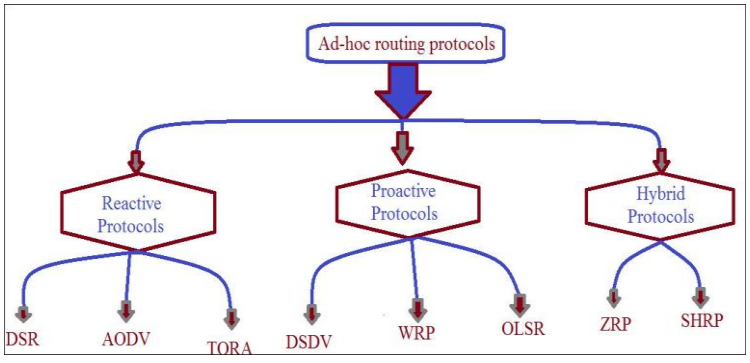

Figure 3: Classification of Routing Protocols

Hybrid routing protocol:- In this phase combination of reactive and proactive routing protocol is there. It is basically the trade-off between these two protocols. There are many problems in reactive and proactive protocols i.e. in proactive protocols large overhead and less latency is there but in reactive protocols huge latency and less overhead is there so to overcome this problem hybrid protocols are formed. It uses the route discovery mechanism of reactive protocol and the table maintenance mechanism of proactive protocol so as to avoid latency and overhead problems in the network. These are also suitable for large networks in which large numbers of nodes are present. These large networks are also divided into zones and different protocols are used for different zones.

There are various types of hybrid protocol which are **ZRP, SHRP and ABR** so on.

IV. REANALYZING OF ROUTING PROTOCOLS

Optimized Link State Routing Protocols (OLSR):-Optimized Link State Routing Protocol (OLSR) is a proactive link state protocol. In this table are already described for routing. In this link state is found in these above described states i.e. SYNC, ASYNC or LOST.

Synchronized (SYNC): It means if linkage is in synchronized form then further connections are proper or in continue form. The data that we send is definitely reach to the destination without any problem.

A synchronized (ASYNC): It means if linkage is in asynchronies form then further connections are not proper OR there is any type breakage in connecting links.

In this Optimized Link State Protocol (OLSR) comes under the category of proactive routing protocols and hence the routes are always available immediately when needed. It is based on the link state protocol and is an optimized version for wireless networks. The topological changes in the mobile nodes cause the flooding of the topological information to all available hosts in the network. To reduce the possible overhead in the network OLSR uses Multipoint Relays (MPR) which reduces the flooding of broadcasts by reducing the same broadcast in some regions in the network. The reduction in the time interval for the control messages transmission can bring more reactivity to the topological changes which are a desired feature as it reduces the control message bandwidth utilization. Also each node has the Multipoint Relay Selector set, which indicates which nodes has selected the current host to act as a MPR. When the node gets a new broadcast message which is to be sent throughout the network and the message's sender interface address is in the MPR Selector set, then the node must forward the message. Due to the possible change in the ad hoc network, the MPR Selectors sets are updated continuously using Hello messages.

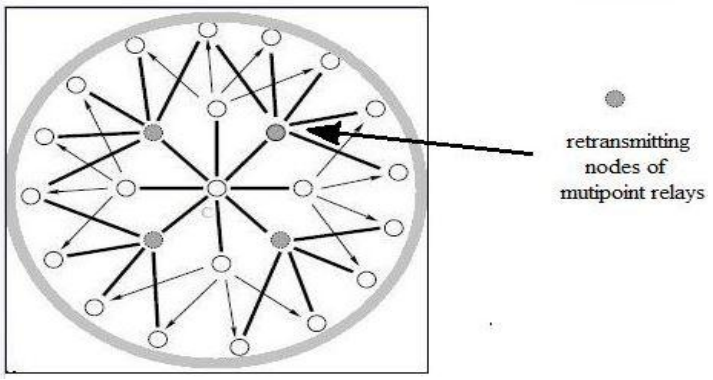

Figure 4: MPR flooding in OLSR

Temporally-Ordered Routing Algorithm Protocol (TORA):-TORA is reactive routing protocol which is also known as link reversal protocol. TORA uses an arbitrary height metric to establish a direct acyclic graph (DAG) and the length of the route that physically (DAG) rooted at the destination. In this if there are multiple routes are present from source to destination then instead of using shortest path it follows the stable path that may be very long. In TORA three steps are involved in establishing a network.

- Creating the routes from source to destination.
- Maintaining the routes.
- Erasing invalid routes.

Initially to create a route, the source node broadcasts a QUERY packet to its neighbours nodes. This QUERY packet is rebroadcasted through the network until it reaches the destination or an intermediate node that has a route to the destination. The recipient of the QUERY packet then broadcasts the UPDATE packet which lists its height with respect to the destination. When this QUERY packet propagates in the network each node that receives the UPDATE packet sets its height to a value greater than the height of the neighbour from which the UPDATE packet was received. This has the effect of creating a series of directed links from the original sender of the QUERY packet to the node that initially generated the UPDATE packet. When a node discover that the route to a destination is no longer valid; it will adjust its height so that it will be a local maximum with respect to its neighbors and then transmits an UPDATE packet. If the node has no neighbors of finite height with respect to the destination, then the node will attempt to discover a new route. As shown in Fig. 5, node 6 does not propagate QUERY from node 5 as it has already seen and propagated QUERY message from node 4 and the source may have received a UPDATE each from node 2, it retains that height.

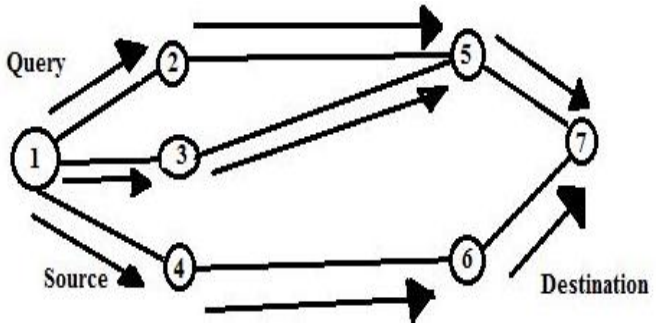

Figure 5: Route creation in TORA

When a node detects a network partition, it will generate a CLEAR packet that results in reset of routing over the ad hoc network. The establishment of the route is based on the DAG mechanism thus ensuring that all the routes are loop free. Packets move from the source node having the highest height to the destination node with the lowest height like top-down approach.

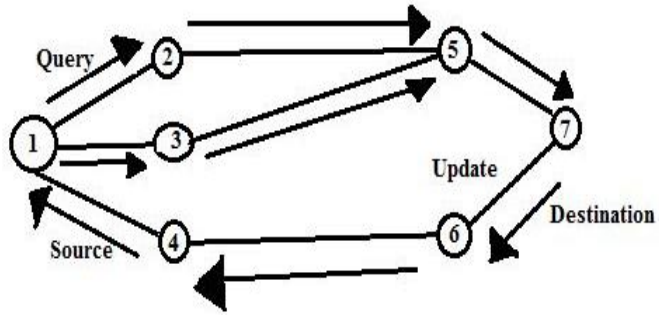

Figure 6 : Route updating in TORA

The Ad-hoc on demand Distance vector (AODV):- Ad hoc On-demand Distance Vector (AODV) is a reactive protocol. It is a combination of both DSR and DSDV. It follows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. It follows bellman Fords algorithium for routing. It is used to protect Route Discovery mechanism of AODV by providing security features like integrity, authentication and non-repudiation but it does not repair a broken path locally. When a link breaks, which is determined by observing the periodical beacons or though ACK messages, the source and the destination nodes are notified (end nodes). The source node then re-establishes the route with the destination using higher layers. AODV does not provide any type of security.

V. COMPARISON OF PROTOCOL

TABLE. 1

Parameters	Reactive protocol	Proactive protocol	Hybrid protocol
Routing philosophy	Flat	Flat/Hierarchical	Hierarchical
Routing scheme	On demand	Table driven	Combination of both
Routing overhead	Low	High	Medium
Latency	High due to flooding	Low due to routing tables	Inside zone low outside similar to Reactive protocols
Scalability level	Not suitable for large networks	Low	Designed for large networks

In this paper, we have presented and discussed the taxonomy of routing protocols in mobile ad hoc networks and provided comparisons between them. The protocols are divided into three main categories: (i) source-initiated (reactive or on-demand), (ii) table-driven (pro-active), (iii) hybrid protocols and different parameters are compared.

TABLE .2

Availability of routing information	Available when required	Always available stored in tables	Combination of both
Periodic updates	Not needed as route available on demand	Yes. Whenever the topology of the network changes	Yes needed inside the zone
Storage capacity	Low generally Depends upon the number of routes	High ,due to the routing tables	Depends on the size of Zone, inside the zone sometimes high as proactive protocol
Mobility support	Route maintenance	Periodical updates	Combination of both

VI. CONCLUSION

The analysis of the different proposals has demonstrated that the inherent characteristics of ad hoc networks, such as lack of infrastructure and rapidly changing topologies, introduce additional difficulties to the already complicated problem of secure routing. The main differentiating factor between the protocols is the ways of finding and maintaining the routes between source destination pairs. The comparison we have presented between the routing protocols indicates that the design of a secure ad hoc routing protocol constitutes a challenging research problem against the existing security solutions. We hope that the taxonomy presented in this paper will be helpful and provide researchers a platform for choosing the right protocol for their work.

REFRENCES

[1] A. K. Gupta, H. Sadawarti, and A. K. Verma, "Review of Various Routing Protocols for MANETS," *Int. J. Inf. Electron. Eng.*, vol. 1, no. 3, pp. 251–259, 2011.

[2] D. Kaur and N. Kumar, "Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV Routing Protocols in Mobile Ad-Hoc Networks," *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 3, pp. 39–46, Mar. 2012.

[3] P. Suganthi and a. Tamilarasi, "Performance Of OLSR Routing Protocol Under Different Route Refresh Intervals In Ad Hoc Networks," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 1, pp. 133–137, 2011.

[4] P. Suganthi and D. A. Tamilarasi, "A Novel Review on Routing Protocols in MANETs," *Int. J. Comput. Sci. Eng.*, vol. 1, no. 1, pp. 103–108, 2012.

