International Journal of Wireless Communication
ISSN: 2231-3559 & E-ISSN: 2231-3567, Volume 2, Issue 1, 2012, pp.-26-28.
Available online at http://www.bioinfo.in/contents.php?id=109

A REVIEW: MANET ROUTING PROTOCOLS AND DIFFERENT TYPES OF ATTACKS IN MANET

KUTE D.S., PATIL A.S., PARDAKHE N.V. AND KATHOLE A.B.

J.D.I.E.T, Yavatmal, Maharashtra, India.
*Corresponding Author: Email- dharti_kute@rediffmail.com, ankita.patil5@gmail.com, nilimapardakhe@gmail.com, atul.kathole1910@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- In the era of wireless devices, Mobile Ad-hoc Network (MANET) has become an indivisible part for communication for mobile devices. Therefore, interest in research of Mobile Ad-hoc Network has been growing since last few years. In this paper we have discussed some basic routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Sourced Routing, and Ad-hoc On Demand Distance Vector. Security is essential requirement in MANET and as compared to the wired network MANETs are more vulnerable to security attacks as they are infrastructure less and autonomous. Main objective of this paper is to address the different MANET routing protocols and different attacks in MANET. As security is big issue in MANET, this paper would be great help for the people who are conducting research for the problems in MANET .
Keywords- Routing Protocol, MANET, Attack, Security

Citation: Kute D.S., et al. (2012) A Review: Manet Routing Protocols and Different Types of Attacks In Manet. International Journal of Wireless Communication, ISSN: 2231-3559 & E-ISSN: 2231-3567, Volume 2, Issue 1, pp.-26-28.

Copyright: Copyright©2012 Kute D.S., et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Introduction

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile hosts without fixed network infrastructure and centralized administration. Communication in MANET is done via multi-hop paths. Lots of challenges are there in this area: MANET contains diverse resources; the line of defense is very ambiguous; Nodes operate in shared wireless medium; Network topology changes unpredictably and very dynamically; Radio link reliability is an issue; connection breaks are pretty frequent. Moreover, density of nodes, number of nodes and mobility of these hosts may vary in different applications. There is no stationary infrastructure. Each node in MANET acts a router that forwards data packets to other nodes. Therefore, selection of effective, suitable, adaptive and robust routing protocol is of utmost importance.

There are three types of routing protocols: Proactive Protocols, Reactive Protocols and Hybrid Protocols. Proactive protocols are table-driven that constantly update lists of destinations and routes. Reactive protocols respond on demand. Hybrid protocols combine the features of reactive and proactive protocols. The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency.

In this paper, Sections looks at working of routing protocols like Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR), and Ad-hoc On Demand Distance Vector (AODV) and description about different types of attack in MANET.

Different Routing Protocol

DSDV

DSDV is a Proactive gateway discovery algorithm where the gateway periodically broadcasts a gateway advertisement message which is transmitted after expiration of the gateways timer.

This protocol is based on classical Bellman-Ford routing algorithm designed for MANETS. Each node maintains a list of all destinations and number of hops to each destination. Each entry is marked with a sequence number. It uses full dump or incremental update to reduce network traffic generated by route updates. The broadcast of route updates is delayed by settling time. The only improvement made here is avoidance of routing loops in a mobile network of routers. With this improvement, routing information can always be readily available, regardless of whether the source

node requires the information or not. DSDV solve the problem of routing loops and count to infinity by associating each route entry with a sequence number indicating its freshness. In DSDV, a sequence number is linked to a destination node, and usually is originated by that node (the owner). The only case that a non-owner node updates a sequence number of a route is when it detects a link break on that route. An owner node always uses even-numbers as sequence numbers, and a non-owner node always uses odd-numbers. With the addition of sequence numbers, routes for the same destination are selected based on the following rules: 1) a route with a newer sequence number is preferred; 2) in the case that two routes have a same sequence number, the one with a better cost metric is preferred.

The list which is maintained is called routing table. The routing table contains the following:

1. All available destinations' IP address
2. Next hop IP address
3. Number of hops to reach the destination
4. Sequence number assigned by the destination node
5. Install time

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. As stated above one of "full dump" or an incremental update is used to send routing table updates for reducing network traffic. 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. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. In a fast-changing network, incremental packets can grow big so full dumps will be more frequent. Each route update packet, in addition to the routing table information, also contains a unique sequence number assigned by the transmitter. The route labeled with the highest (i.e. most recent) sequence number is used. If two routes have the same sequence number then the route with the best metric (i.e. shortest route) is used. Based on the past history, the stations estimate the settling time of routes. The stations delay the transmission of a routing update by settling time so as to eliminate those updates that would occur if a better route were found very soon. Each row of the update send is of the following form:

Destination IP addresses, Destination sequence number, Hop count> after receiving an update neighboring nodes utilizes it to compute the routing table entries. To damp the routing fluctuations due to unsynchronized nature of periodic updates, routing updates for a given destination can propagate along different paths at different rates. To prevent a node from announcing a routing path change for a given destination while another better update for that destination is still in route, DSDV requires node to wait a settling time before announcing a new route with higher metric for a destination.

DSR

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. Dynamic Source Routing, DSR, is a reactive routing protocol that uses source routing to send packets. It uses source routing which means that the source must know the complete hop sequence to the destination. Each node maintains a route cache, where all routes it knows are stored. The route discovery process is initiated only if the desired route cannot be found in the route cache. To limit the number of route requests propagated, a node processes the route request message only if it has not already received the message and its address is not present in the route record of the message. As mentioned before, DSR uses source routing, i.e. the source determines the complete sequence of hops that each packet should traverse. This requires that the sequence of hops is included in each packet's header. A negative consequence of this is the routing overhead every packet has to carry. However, one big advantage is that intermediate nodes can learn routes from the source routes in the packets they receive. Since finding a route is generally a costly operation in terms of time, bandwidth and energy, this is a strong argument for using source routing. Another advantage of source routing is that it avoids the need for up-to-date routing information in the intermediate nodes through which the packets are forwarded since all necessary routing information is included in the packets. Finally, it avoids routing loops easily because the complete route is determined by a single node instead of making the decision hop-by-hop. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on demand, allowing the routing packet overhead of DSR to scale automatically to only what is needed to react to changes in the routes currently in use. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example, for use in load balancing or for increased robustness. With the help of Route Discovery process source node desires the route to the destination node. And with the help of Route Maintenance is to handle the route breaks.

AODV

It is descendant of DSDV and it is reactive protocol. Route discovery cycle used for route finding and Maintenance of active routing and with AODV protocol it provides unicast and multicast communication. And Sequence number used for loop prevention and route freshness criteria.

AODV belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbours and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbours periodically its whole routing table. So they can check if there is a useful route to another node using this neighbour as next hop. When a link breaks a Count-To-Infinity could happen. AODV is an 'on demand routing protocol' with small

delay. That means that routes are only established when needed to reduce traffic overhead. AODV supports Unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently. To characterize the AODV with the five criteria used by Keshav AODV is distributed, hop-by-hop, deterministic, single path and state dependent. AODV uses IP in a special way. It treats an IP address just as an unique identifier. This can easily be done with setting the Subnet mask to 255.255.255.255. But also aggregated networks are supported. They are implemented as subnets. Only one router in each of them is responsible to operate the AODV for the whole subnet and serves as a default gateway. It has to maintain a sequence number for the whole subnet and to forward every package. In AODV the routing table is expanded by a sequence number to every destination and by time to live for every entry. It is also expanded by routing flags, the interface, a list of precursors and for outdated routes the last hop count is stored.

Network Layer Attacks

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 are tunneled. This tunnel between two colluding attackers is referred 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. Blackhole attack

The blackhole 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.

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. Routing Attacks

There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Various attacks on the routing protocol are described briefly below.

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. IP Spoofing attack

In conflict-detection allocation, the new node chooses a random address (say y) and broadcast a conflict detection packet throughout the MANET. Any veto from a node will prevent it from using this address. If the malicious node always impersonates a member that has occupied the same IP address and keeps replying with vetoes, it is called an IP Spoofing attack.

G. State Pollution attack

If a malicious node gives incorrect parameters in reply, it is called the state pollution attack. For example, in best effort allocation, a malicious allocator can always give the new node an occupied address, which leads to repeated broadcast of Duplication Address Detection messages throughout the MANET and the rejection of new node.

H. Sybil attack

If a malicious node impersonates some nonexistent nodes, it will appear as several malicious nodes conspiring together, which is called a Sybil attack. This attacks aims at network services when cooperation is necessary, and affects all the auto configuration schemes and secure allocation schemes based on trust model as well. However, there is no effective way to defeat Sybil attacks.

Conclusion

In this paper we have discussed some basic routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Sourced Routing, and Ad-hoc On Demand Distance Vector. The major requirement in MANET is the security. MANETs are more vulnerable to security attacks as they are infrastructure less and autonomous. Main objective of this paper is to address the different MANET routing protocols and different attacks in MANET. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. This paper will give the brief idea regarding MANET to the people who are conducting researchs in MANET.

References

[1] Perkins C.E. and Bhagwat P. (1994) *Computer Communication Review*, 24(4), 234-244.

[2] Johnson D.B. and Maltz D.A. (1996) *Mobile Computing*, 153-181.

[3] Corson M.S., Maker J.P. and Cirincione G.H. (1999) *IEEE Internet Computing*, 3(4), 63-70.

[4] Perkins C.E. and Royer E.M. (1999) *Workshop Mobile Computing Systems and Applications* (WMCSA), 90-100.

[5] Kim D., Garcia J. and Obraczka K. (2003) *IEEE Transactions on Mobile Computing*., 2(2), 161-173.

[6] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei (2006) *Wireless/Mobile Network Security*.

[7] Shanthi N., Lganesan and Ramar K. *Journal of Theoretical and Applied Information Technology*.

[8] Sukla Banerjee (2008) *World Congress on Engineering and Computer Science*.