ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

A survey on AODV routing protocol for AD-HOC Network

Parveen Kumar
Astt. Professor
Dept. of Computer Science
Lovely Professional University

Jatin Sharma
Research fellow
Dept. of Computer Science
Lovely Professional University

Kriti saini
Research fellow
Dept. of Information technology
Lovely Professional University

Abstract

Now a day, Ad-hoc network has become an indivisible part for communication for mobile devices. There are different types of topology for implementation of Ad-hoc network. AODV is one of them which are a reactive protocol that react on demand. Security occurs in every kind of network for protecting from various attacks. Those attacks are Wormhole attacks and black hole attacks etc. there is a summary about few topology and few attacks. Brief working of AODV. Security on AODV protocol thought Digital signature, authentication and access control and active attacks intrusion detection systems and cooperation enforcement mechanism are very useful.

1 Introduction

Ad-hoc – in the general term, ad-hoc is basically used in different field. Ad-hoc is from Latin language the meaning of ad-hoc is "for this". The different fields where the Ad-hoc is used are network, military, querying, science & philosophy. In the field of information science, ad-hoc reporting system, it allows the users to create specific and customized queries. Ad-hoc querying / reporting is a business intelligent subtopic along with OLAP (online analytical processing), data warehousing and data mining.

There is one term which is called networking by ad-hoc the means system of network elements that combine from the network .since the inception of wireless networking there have been two type of wireless network, first is infrastructure network and the other one is ad-hoc network. Both are the most important aspect of the networking there is some basic information about them

In the infrastructure network, there is an interconnected group of computer system linked by the various parts of a telecommunications arch. The infrastructure network may be either open or closed.

In the open arch. Internet comes and in closed one's private network comes. The very basic type of this network is one or more than one computer.[1] A internet connection and hub to both link the computer to the network connection

The basic thing in the ad-hoc network is that there is no access point for passing information .ad-hoc network are generally closed in that way they don't connect to the internet .this connection can be shared among other members of the ad-hoc network .

Ad-hoc network are common for portable video game system like the soney psp or the ds because they allow players to link to each other to play video games wirelessly it usually in a smaller office environment without the need for domains and the additional management.

2. The basic difference b/w ad-hoc network & infrastructure--

The basic idea runs behind b/w these network is that you want to communicate with your pc directly or through access point.

In ad-hoc network data in the network is transferred to and from wireless network adopters connected to pc. It's also called peer to peer network .the basic benefits of an ad-hoc network. It's very simple to set up and very inexpensive, it's very fast than other network.

In infrastructure network, we can increase the range of your wireless network by adding an access point, by the help of access point we can easily expand a wireless network capability.

If we can place multiple access point to the network .as you might in an office or home. User can roam b/w interlocking access point cells without losing the connection to the network.

3. Manet Routing Protocol and Wormhole Attack against AODV

1st There is a discussion between some protocols Like Destination Sequenced Vector, Dynamic Source Routing, Temporally –Ordered Routing Algorithm and Ad-hoc On Demand Vector, 2nd Securing the routing protocol Ad-hoc On Demand Distance Vector from the operation of Wormhole Attack.

In Ad-hoc network, all the nodes act as router and forwards data packet to the network. There is no fixed network infrastructure. All the communication done by the multi hop paths, topology change dynamically and unpredictably in this kind of network, losing connection is pretty common and frequent thing.

Proactive protocol, Reactive protocol, Hybrid protocols are the three types of Routing protocol. In that Proactive is also known as table driven protocol and Reactive protocol is On Demand protocol. In table driven protocol, it constantly updates lists of destinations and routers and in on demand protocol, it responds on demand, Hybrid protocols mange the features of both proactive and reactive protocols.[4]

Destination-sequenced Distance Vector- it was introduced by C.Perkins and P.Bhagwat

in 1994. It's helpful for solving the routing loop problem. In this DSDV, there is one or more tables that contain route information. DSDV is an enhancement of Bellman Ford algorithm Updating in table and sequence number leads to prevent problem like loops and count to infinity problem.[3]

Dynamic Source routing –this is a reactive kind of protocol which reacts on-demand. In that the source always knows the complete route from source to destination. There are two main methods, one is Route Discovery and other one is Route Maintenance. it allows multiple routes to destination node and routing is loop free here. In this any broken link is notified to the source node with an error message. Basically it used in large networks where rotes have not fixed topology.

Temporally-oriented routing protocol- it's made to find routes on demand. It creates and maintains directed acyclic graph rooted at the destination node. It can provide multiple routes for a single destination. There are main phases of the algorithm: Route creation, Route Maintenance, Route Erasure .the query packet is flooded all over the network and if routes exist, an update packet is sent back. Route Maintenance phase update packet reorient the route composition.

Ad-Hoc on Demand Distance Vector— it's a reactive protocol that reacts on demand. This is the modification of DSDV. It enables multi-hop, self starting and dynamic routing in network. ADOV never produces loops as there cannot be any loop in the routing table of any node because of the concept of sequence number counter borrowed from DSDV.

In AODV's route discovery process is started by node that wants to communicate with the other node and for that propose it broadcasts a HELLO message after a specific time interval, Thus a node keeps tracks of only its next hop. Whenever a node want to communicate with a node that is not its neighbor ,it simply broadcast RREQ massage that contain RREQ ID, Destination ip address, Destination Sequence Number, Source Ip address, Source Sequence Number and Hop count.

When the other node receives an RREQ, it checks that weather it has already received an RREQ with that node or not. If yes, it simply discards the request or if not, than it increment the hop count values in RREQ by one. Soon after the updating valid sequence number field in the route table entry is true.

After updating the information the intermediate node forwards the RREQ packet until a node is found that is the destination itself. Now this replies back to the source node with a route reply packet RREP. That RREP contain Destination ip address, Destination Sequence number, Originator ip address and Lifetime.

When the RREP reaches to the source node, it can now send the data packets thorough the route that is set up.

4. Security attacks against AODV.

There can be two kinds of attacks: passive attacks and active attacks .A passive an attack does not disturb the normal network operation while an active attack does it.

Active attacks can be internal or external. Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network.

Some attacks are described below

Black hole attacks—it's a malicious node that falsely replies for route requests without having an active route. It exploits the routing protocol to advertise itself as having a good and valid path. It may be internal and external; it's very harmful for personal and important data.

Wormhole attacks—the attacker disrupts routing by short circuiting the usual flow of routing packet. Generally two or more attackers connect via a link called wormhole attacks and it can be done by one node too. they capture packets at the one end and replay them at the other end using private session .its relatively easy to deploy but may cause great damage to the network .

5. Securing AODV

Security is always very important aspect in every field. its applied with the mixture of processes, procedures and systems which are used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation.To defend against passive attacks conventional approaches like Digital signature, encryption, authentication and access control and defend against active attacks intrusion detection systems and cooperation enforcement mechanism are very useful.
Secure Ad-hoc on Demand Vector is an extension of AODV in which digital signature and has chains mechanisms are used. Every node uses digital signature for authentication and integrity in routing message like RREQ, RREP, and RRER. This signature is verified by neighbor nodes that receive the message. Hash chains are used to secure hop –count mechanism. SAODV addresses security of routing message only;
Security of data exchange still remains unaddressed. Moreover, Due to digital signatures, messages get bigger. Also generating and verifying signatures add to the overhead. Especially when double signatures mechanism is used.

6. Conclusion

Its require a scalable, reliable, efficient most importantly, a secure protocol as they are highly insecure, self- organizing, rapidly deployed and they use dynamic routing. AODV is prone to attacks like modification of sequence number , modification of sequence numbers, spoofing and fabrication of error message .Although fabrication of source routes is not possible in AODV while DSR is prone to it .Wormhole attack is real threat against AODV protocol in MANET. Therefore, trustworthy techniques for discovering and detection of wormhole attack should be used. We should keep in mind that some require special hardware and some solutions are very expensive.

References

1.Raquel Lacuesta, Jaime Lloret senior member ,IEEE, Miguel Garcia Graduated Student member, Lourdes Penalver (2012) "A Secure Protocol for spontaneous wireless Ad- Hoc Network Creation", This article has been accepted for publication in a future issue of this journal.

2. Mihir Nyayate Electrical Engineering, IIT KANPUR, (U.P) India & Y.N. Singh Engineering, IIT KANPUR, (U.P) India "Dynamic safe transmit power MAC protocol in wireless ad-hoc MAC protocol"

3. I-Te Lin, Dilip sarkar, Tutomu Murase and Iwao Sasase "Dijkstra- Based Higher Capacity Route selection Algorithm using Bounded length and State Change For Automobiles

4. Rutvij H. Jhaveri, Ashish D. patel, Jatin D. Parmar "MANET Routing Protocol and Wormhole Attack against AODV" IJCSNS International Journal of Computer science and Network Security, VOL.10 NO.4 April 2010.