International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Study for IAODV and IDSDV Protocol under Black Hole Attack

Mohit[1], Praveen[2]

[1]Apex Institute of Management and Technology, Gorgarh, Haryana, India

[2]AP, Apex Institute of Management and Technology, Gorgarh, Gorgarh, Haryana, India

Abstract: ***Wireless networks are gaining popularity day by day, as users want wireless connectivity irrespective of their geographic position. MANETs consist of mobile nodes that are free in moving in and out in the network. Mobile Ad hoc Network (MANET) is a collection of mobile nodes in which the wireless links are frequently broken down due to mobility and dynamic infrastructure. Routing is a significant issue and challenge in ad hoc networks. Many routing protocols have been proposed like IAODV and IDSDV so far to improve the routing performance and reliability. Current Work make a comparison of these routing protocol based on the performance metrics like packet delivery fraction, end–to–end delay, throughput. Simulation is done in NS2 (Network Simulator version2).***

Keywords: MANET, IAODV, IDSDV etc.

1. Introduction

An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multi-hop paths through the network to any other node [1]. This idea of Mobile ad hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. A mobile ad-hoc network is a collection of mobile nodes forming an ad-hoc network without the assistance of any centralized structures. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deployment of an infrastructure is not very cost effective. There are quite a number of uses for mobile ad-hoc networks [2]. For example, the military can track enemy tanks as it moves through the geographic area covered by the network. Your local community can use an ad-hoc network to detect your car moving though an intersection, checking the speed and direction of the car. In an environmental network, you can find out the temperature, atmospheric pressure, amount of sunlight, and the relative humidity at a number of locations.

2. Literature Survey

Meenakshi Mehla, *et al.* [3] this paper based on PKI with IODMRP here the study help in making protocols more robust against attacks and standardize parameters for security in routing rotocols. PKI, PGP and SPGP plays the vital role in terms of security.It is easy to manage the security of a fixed network but for a mobile and dynamically changing network it is very cumbersome. Thus in this paper focus is on the security with Public key infrastructures and its various types that can help to maintain the security in the Mobile adhoc network.

Ashwini V. Biradar, *et al.* [4] worked on the new energy based AODV (EBAODV) protocol that will not only reduce the energy consumption but also takes node's remaining energy. Based on this it will forward the packets in MANET. Simulation results (using Network Simulator NS-2.34) show that significant performance enhancements of energy based AODV (EBAODV) protocol over the original AODV and DSDV protocols in terms of energy consumption and network overhead. Proposed EBAODV gives the acceptable level of packet delivery ratio.

Biswaraj Sen, *et al.* [5] worked on the performance evaluation of two routing protocols, AODV and DSDV,which has been done with respect to metrics viz. throughput, average end-to-end delay and normalized routing load under varying node density and varying pause time. From the result analysis, it has been observed that in high node density the performance of both protocols decreases significantly. It has been observed that in low node density the performance of AODV is better than DSDV in terms of throughput, whereas the performance of DSDV is better in high node density (upto 100 nodes). Another observation has been found from the result that increment of pause time does not affect much in the performance of DSDV where the performance of AODV varies significantly with the pause time.

Jashanvir Kaur, *et al.* [6] in this paper focus is on the security with Public key infrastructures and its various types that can help to maintain the security in the Mobile adhoc network.in this paper the design of secure techniques namely PGP and SBPGP with AODV protocol And observed that SBPGP provide better security as compared to other techniques of PKI.

Adel.S.El ashheb, *et al.* [7] here the two protocols AODV and DSDV have been simulated using NS-2 package and compared in terms of packet delivery fraction, end to end delay and throughput in different environment; varying

period of pause time and the number of expired nodes. Simulation results show that AODV routing protocol has better performance in terms of packet delivery fraction and throughput but, AODV suffers from delay.

3. Security Requirements

In any fixed or wireless network, the security is incorporated at three stages: prevention, detection and cure. Key parts of prevention stage are authentication and authorization. The authentication is associated with authenticating the participating node, message and any other meta-data like topology state, hop counts etc. Authorization is associated with recognition. Where detection is the ability to notice misbehaviour carried out by a node in the network, the ability to take a corrective action after noticing misbehaviour by a node is termed as cure. Different possible attacks on ad hoc networks are eavesdropping, compromising node, distorting message, replaying message, failing to forward message, jamming signals etc. There are several proposals available to solve these issues, but are not comprehensive in nature as they target specific threats separately. Therefore there is a strong need to have an efficient security regime which can take care of all the aspects of security.

4. Security Threats

The two broad classes of network attacks are active attacks and passive attacks.

1. **Passive Attack:** An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described as
   (a) **Eavesdropping:** The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a network topology between two workstations or tuning into transmissions between a wireless handset and a base station.
   (b) **Traffic analysis:** The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.
2. **Active Attack:** An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types masquerading, replay, message modification, and denial-of-service (DoS). These attacks are summarized as:
   (a) **Masquerading:** The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
   (b) **Replay:** The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
   (c) **Message modification:** The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
   (d) **Denial-of-service:** The attacker prevents or prohibits the normal use or management of communications facilities.

5. Problem of Black Hole Attack

In computer networking, a packet drop attack or blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDOS tool. Because packets are router routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

Thus there is a use of hybrid protocols which is the combination of two techniques IAODV (Improved Ad hoc on Demand Distance Vector Routing) and DSR(Dynamic Source Routing) which overcomes the problem of black hole attack.

References

[1] Shubhranshu Singh, Ashutosh Bhatia, “A DHCPv6 Based IPv6 Autoconfiguration Mechanism for Subordinate MANET”, IEEE 2008.
[2] Sachin Kumar Gupta & R. K. Saket, “Performance Metric Comparison of AODV and DSDV Routing Protocols in Manets using NS-2”, IJRRAS 7 (3) June 2011.
[3] Meenakshi Mehla, Himani Mann, “Sbpgp Security Model Using Iodmrp”, International Journal Of Computational Engineering Research IJCER May-June 2012 Vol. 2.
[4] Ashwini V. Biradar, Shrikant R. Tandle, Veeresh G. Kasabegoudar, “Detailed Performance Analysis of Energy based AODV Protocol in Comparison with Conventional AODV, and DSDV Protocols in MANET”, International Journal of Computer Applications Volume 49– No.10, July 2012.
[5] Biswaraj Sen, Sanku Sinha, “ A Simulation Based Performance Analysis of AODV and DSDV Routing Protocols in MANETs”, International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.4, July-Aug. 2012.
[6] Jashanvir Kaur and Er. Sukhwinder Singh Sran, “SBPGP Security based Model in Large Scale Manets”, International Journal of Wireless Networks and Communications Volume 4, Number 1 (2012).
[7] Adel.S.El Ashheb, “Performance Evaluation of AODV and DSDV Routing Protocol in wireless sensor network Environment”, 2012 International Conference on Computer Networks and Communication Systems (CNCS 2012).

Authors Profile

Mohit is a student at AIMT (Gorgarh), India

Mr. Praveen, AP, AIMT (Gorgarh), India