ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Three Way Techniques for Preventing Black Hole Attack in MANET Using AODV Protocol

Kavi Joshi, Er.Manoj Kumar

PG Student, Department of CSE, Yadwindra college of Engineering, Talwandi Sabo, Bathinda, India

Assistant Professor, Department of CSE, Yadwindra College of Engineering , Talwandi Sabo, Bhatinda, India

ABSTRACT: Mobile Adhoc Networks (MANET) are acquiring popularity today, as it offers wireless connectivity to the user irrespective of their geographical position. An Ad-hoc network does not have a centralized infrastructure. It is a wireless network where nodes communicate with each other through multiple hops. If nodes in the ad-hoc network changes there position dynamically, it is called Mobile ad-hoc network (MANET). It has characteristics like shard physical medium, autonomous terminal, limited physical security, infrastructure less communication, dynamic topology, large degree of Freedom, self-organizing capability. Such characteristics provide an open environment for the users to maintain connectivity irrespective of their geographical positions but, such types of network are vulnerable to various kind of attacks.

I. INTRODUCTION TO MANET

The field of Wireless networks has experienced rapid growth since 1970s. In fact, the combination of radio communications and computer networks were first introduced by the University of Hawaii in 1971 in an experimental network named ALOHANET. This was the first Wireless Local Area Network (WLAN) that offered star topology based bidirectional communications. During the 80s, the technology was drastically improved. At the end of the 90s, wireless networks made great revolution and reached a peak due to the constant growth of the Internet.

A Simple Wireless network

Mobile Ad-hoc networks (MANETs) have been widely researched during last few years, gathering lots of attention due to rapid increase in mobile devices. Today's world of dynamic changing technology of communication networks, MANETs play a vital role in wireless communication. MANETs are collection of wireless mobile nodes that acts as dynamic network without use of fix infrastructure and centralized control to authorize other entities in network. MANET comprises of mobile nodes that cooperate with each other using wireless connections to route both data and control packets within the wireless network.

Unlike a wired network, nodes in an ad hoc network can free to move in random and arbitrary direction, so frequent changes in topology. These networks are self-configuring network and nodes within MANETs provide a peer-level multi-hopping routing service because each node acts as a router. Also, source to destination communication may require routing information via several intermediate nodes to route a packet to the destination node due to limited transmission range of a node. Each mobile node that communicates with other node via radio wave and can communicate directly to those nodes that is in transmission range of each other. Each participating node in MANETs is

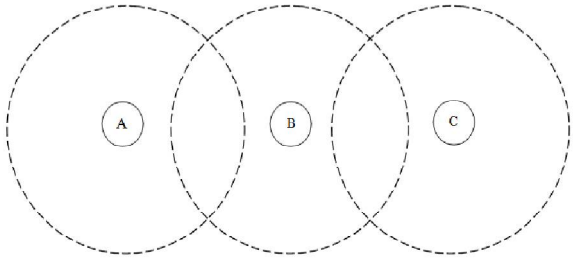
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

independent and makes routing decision like route request, route selection, route update and making new communication link with their neighbor's as well as serving old established. However, all network functions are based on the nodes mutual effort. A simple example of MANETs is shown below.



A simple MANETs with 3 participating nodes

In figure, node A wants to communicate to node C. However, node C is not in the direct transmission range of node A. So, node A and C must discover route through node B in order to communicate with each other. However, there is no dependency on infrastructure that makes it robust and low-cost. A MANETs has many benefits, such as and adaptability to highly variable characteristics, namely power, transmission conditions, traffic distribution variations, and load balancing. However, those benefits come with many challenges. New algorithms, protocols have to be designed and developed to create a truly flexible and decentralized network. The system may operate in isolation, or may have gateways to and interface with a fixed network.

1.2 Characteristics of MANETs

A MANET is an autonomous system of mobile nodes. MANETs node are equipped with wireless transmitters and receivers using antennas which may be highly directional (point to point), unidirectional (broadcast), possibly steerable, or some combination thereof. The characteristics of these networks are summarized as follow.

 Dynamic topology

MANETs are autonomous system of mobile nodes. Mobile nodes can move arbitrary in any direction thus network topology may change randomly and arbitrarily at unpredictable time intervals.

 Energy-constrained operation

Unlike wired network, Wireless links have significantly lower link capacity. In addition, channel capacity is often much less than a radio's maximum transmission rate so that the realized throughput of wireless communications after accounting for the effects of multiple access, fading, noise, and interference conditions, etc.

Bandwidth constrained, variable capacity link

Some or Each of mobile nodes in MANETs relies on battery that has limited power to operate continuously. Basically, optimization of energy conservation may be the important system design criteria for these nodes. A wireless connectivity in the form of a random, multi-hop exists between the nodes at a given point in time, depending on the nodes positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel Interference levels.

1.3 Advantages of MANETs

Some of the applications of MANETs are as follows.

- Tactical networks
- Emergency services
- Commercial operation
- Education
- Entertainment

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

II. LITERATURE SURVEY

[1]Prevention of Black hole Attack on AODV in MANET using hash function (IEEE, 2014)
In this technique source node will sent the route request. Either destination node or intermediate node will receives the route request and sends back the route replies. Source node once will receives all the route replies will reject first reply and adopt second one. It will be very difficult for black hole node to become second to reply. Later one path will be adopted the authentication is done using SHA. Compute has say SHA-ONE, sent it to the destination. Destination computes hash at its send says SHA-TWO. If SHA-ONE =SHA-Two, route is safe else data packet error. Save the DPE route and adopt new for packet sending.

[2]Defending against Collaborative Att-acks by Malicious Nodes in MANETs: A cooperative Bait Detection Approach (IEEE, 2014)
This paper attempts to resolve the issue by designing a DSR i.e. dynamic source routing based. It uses a mechanism called as BBDS i.e. co-operative bait detection scheme. It integrates the advantage of security mechanism used in both reactive and pro-active protocols. It uses integrated approach of both these protocols. It provides better results in comparison to single reactive or proactive protocol.

[3]A Novel Blackhole Attack for Multi-path AODV and its Mitigation (IEEE, 2014)
According to this paper AODV based on multipath has less pronability to attack. Now a days AODV identify multiple paths from source to destination. If one path fails immediately second path will be adopted.Without identifying the second path individually. According to this paper intermediate position will be adopted by black hole node which affects more than one paths. Now to cope up this such, such paths will be adopted which has minimum no. of intermediate nodes and has less sequence no. than the total available sequence numbers.

[4]A Mechanism for Discovery and Prev-ention of Cooperative Black whole attack in Mobile Ad hoc Network Using AODV Protocol (IEEE, 2014)
This paper is focused on detection and prevention of black hole nodes. In MANET kind of network. This paper has given the research based on identifying the black hole by uses broadcast synchronization and relative distance method. In this mechanism the route replied node internal clock time and external clock time sequence is being compared threshold value. The clock time of normal node is greater than the threshold time initialization time duration.

Limitation of base paper
1. Cluster division is not possible in case of IDS detection.
2. It will be required to increase the address at header. I.e. cluster id also has to be increased
3. In result it will increase the data load on the network.
4. It also consumes the pre evaluation time to compare the previous and new route requests and route replies.
5. It requires large memory buffer to store the previous route requests and route replies.

III. PROPOSED WORK

By using our scheme we provide better solution to the black hole problem using AODV in MANET. In this paper we have tried to detect and prevent black hole by using technique called three way technique for preventing black hole attack in MANET using AODV. In our work we will identify three alternative routes to the destination, we will keep three paths. We send the packet on first selected route. If the destination sends the acknowdgement having sequence no match to itself, then packet will be considered successfully sent. Else path will be declared having black hole. And node identified will be purged from path list. Later on second alternative path will be taken for transmission of the packets.

REFERENCES

[1]. *Komal Joshi, VijayaSagvekar*; An efficient technique for preventing cooperative Blackhole attack in Manet using Aodv protocol, student member, dept. of computer engineering, P.V.P.I.T, Pune University,Pune,India;International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 2, April2013.
[2]. *Chang Wu Yu, Tung-Kiang Wu, Rei Hang Cheng, and Shun Chao Chang*; A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network; Department of Computer Science and Information Engineering, Chung Hua University, Hsinchu, Taiwan, R.O.C.
[3]. *Sanjay Ramaswamy, Hiring Fu, ManoharSreekantaradhya, John Dixon and Kendall Nygard*; Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks; Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105 .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

[4].*RambabuYercajana, A.K. Sarjr*, "A Timestamp Based Multipath Source Routing Protocol for Congestion in MANET", "International Advance Computing Conference, Communication" IACC, 2009
[5]. *Hongmei Deng, Wei Li, and Dharma P. Agrawal*, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzi ne, vol. 40, no. 10, October 2002.
[6]. *BounpadithKannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, and Abbas Jamalipour*, "A survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE wireless communication, 2007.
[7]. *Charles E. Perkins, and Elizabeth M. Royer*, "Ad-hoc On-Demand Distance Vector (AODV) routing," Internet Draft, November 2002.
[8]. *KimayaSanzgiri, Bridget Dahill, Brian Neil Leviney, Clay Shieldsz, Elizabeth M. Belding-Royer*, "A Secure Routing Protocol for Ad Hoc Networks", 10th IEEE International Conference on Network Protocols, 2002
[9]. *Tamilselvan L, Sankaranarayanan V*, "Prevention of Blackhole attack in MANET", 2nd International conference on Wireless Boardband and Ultra Wideband Communications, 2007
[10]. *Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEE*, "Wormhole Attacks in Wireless Networks", IEEE JSAC 2006
[11]. *Payal N. Raj, Prashant B. Swadas*, "a dynamic learning system against Blackhole attack in Aodv based Manet", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009
[12]. *KaminiMaheshwar; Divakar Singh*, "Black Hole Effect Analysis and Prevention through IDS in MANET Environment" Scholars Research Library, European Journal of Applied Engineering and Scientific Research, 2012, 1 (4):84-90
[13]. *Sanjay Ramaswamy, Hiring Fu*, ManoharSreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.