International Journal on Emerging Technologies (Special Issue on *RTIESTM-2016*) **7**(1): 94-98(2016)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Enhance the efficiency of data transmission and security for Black hole attack in the MANETs using IDSDV and MDSR routing protocols: A Review

Kiranpreet Kaur**, Jasleen Kaur** and Vishali Bansal**
**M.Tech. Student, Department of CSE, AIET, Faridkot, (PB), INDIA.*
***Assistant Professor, Department of CSE, AIET, Faridkot, (PB), INDIA.*
****Assistant Professor, Department of CSE, AIET, Faridkot, (PB), INDIA.*

(Corresponding author: Kiranpreet Kaur)
(Received 04 October, 2015 Accepted 04 November, 2015)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: 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 deploy an infrastructure is not very cost effective. The popular IEEE 802.11 "WI-FI" protocol is capable of providing ad-hoc network facilities at low level, when no access point is available. 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. Routing is a significant issue and challenge in ad hoc networks. Many routing protocols have been proposed like IAODV and IDSR so far to improve the routing performance and reliability. A black hole attack in ad hoc network refers to an attack by malicious nodes, which forcibly acquires the route from a source to destination by falsely advertising shortest hop count to reach the destination node. In current Work we are going to make the enhanced version of with IDSDV and MDSR so that black hole attack and other attacks can be handled.

Keywords: MANET, IDSDV, DSR, MDSR

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any challenging and interesting research areas. Mobile ad-hoc networks can turn the dream of getting connected "anywhere and at anytime" into reality. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places. As an example, we can imagine a group of peoples with laptops, in a business meeting at a place where no network services is present. They can easily network their machines by forming an ad-hoc network. This is one of the many examples where these networks may possibly be used.

A. Features of Mobile Ad-hoc Networks

MANETs is an IEEE 802.11 framework. It is an interconnected collection of wireless nodes where there is no networking infrastructure in the form of base stations, devices do not need to be within each other‘s communication range to communicate, the end-users devices also act as routers, nodes can enter and leave over time, data packets are forwarded by intermediate nodes to their final destination.

B. Characteristics of MANETs

Mobile ad hoc network nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), Omni directional (broadcast), probably steer able, or some combination thereof [1].

At a given point in time, depending on positions of nodes, their transmitter and receiver coverage patterns, communication power levels and co-channel interference levels, a wireless connectivity in the form of a random, multichip graph or "ad hoc" network exists among the nodes. This ad hoc topology may modify with time as the nodes move or adjust their transmission and reception parameters.
The characteristics of these networks are summarized as follows:
-Communication via wireless means
-Nodes can perform the roles of both hosts and routers
-Bandwidth-constrained, variable capacity links
-Energy-constrained Operation
-Limited Physical Security
-Dynamic network topology
-Frequent routing updates

C. Advantages of MANETs
The following are the advantages of MANETs:
-They provide access to information and services regardless of geographic position.
-These networks can be set up at any place and time.

D. Applications of MANET
Some of the applications of MANETs are as follows:
-Military or police exercises.
-Disaster relief operations.
-Mine cite operations.
-Urgent Business meetings.

II. MANETS ROUTING PROTOCOLS

Mobile Ad-Hoc Network is the rapid growing technology from the past 20 years. The gain in their popularity is because of the ease of deployment, infrastructure less and their dynamic nature. MANETs created a new set of demands to be implemented and to provide efficient better end-to-end communication.

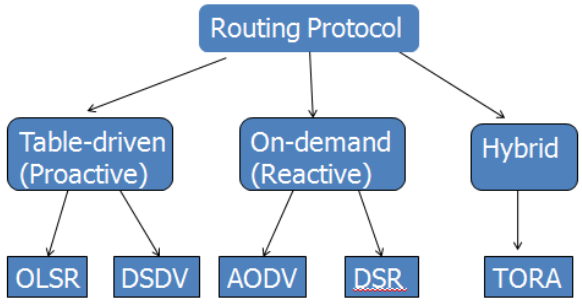

Fig.1. MANETs Routing Protocols.

MANETs works on TCP/IP structure to provide the means of communication between communicating work stations. Routing protocols in MANETs are a challenging and attractive tasks, researchers are giving tremendous amount of attention to this key area.
Routing protocols in MANETs are classified as:-

A. Reactive Protocols
Reactive protocols are also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. These protocols setup routes when demanded [1, 2].

B. Proactive protocols
In proactive protocols, each node maintains individual routing table containing routing information for every node in the network. Each node maintains consistent and current up-to-date routing information by sending control messages periodically between the nodes which update their routing tables. The proactive routing protocols use link-state routing algorithms which frequently flood the link information about its neighbors. Some of the existing proactive routing protocols are DSDV and OLSR [2].

C. Hybrid Routing Protocol
Hybrid routing protocol combines the advantages of both proactive and reactive routing protocols. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Some of the existing hybrid protocols are ZRP and TORA.

III. OVERVIEW OF PROTOCOLS

A. Ad-Hoc on Demand Distance Vector Protocol (AODV)
AODV is described in RFC 3561 [3]. It's reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network.

B. Route Discovery Mechanism in AODV
When a node "A" wants to initiate transmission with another node "G" as shown in the Fig. 2, it will generate a Route Request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forwarded to the neighbors, and those node forward the control message to their neighbors' nodes.

This process of finding destination node goes on until it finds a node that has a fresh enough route to the destination or destination node is located itself. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "B". Once the route is established between "A" and "B", node "A" and "B" can communicate with each other. Figure depicts the exchange of control messages between source node and destination node.

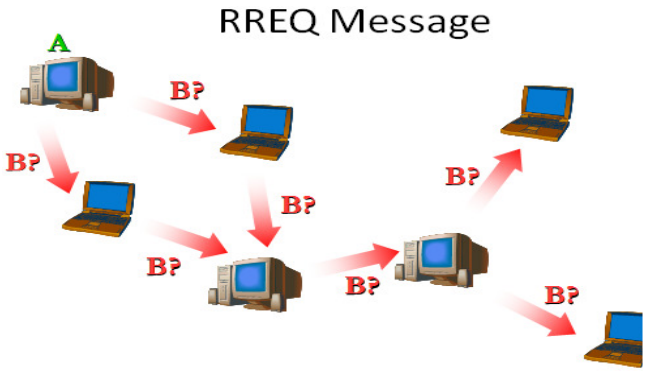

Fig. 2. AODV Route Discovery.

C. Improved Ad Hoc On-Demand Distance Vector Routing (IAODV)

AODV is basically an improvement of DSDV. But, AODV is a reactive routing protocol instead of proactive. It minimizes the number of broadcasts by creating routes based on demand, which is not the case for DSDV. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes in turn broadcast the packet to their neighbors and the process continues until the packet reaches the destination. During the process of forwarding the route request, intermediate nodes record the address of the neighbor from which the first copy of the broadcast packet is received. This record is stored in their route tables, which helps for establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. The reply is sent using the reverse path. For route maintenance, when a source node moves, it can reinitiate a route discovery process. If any intermediate node moves within a particular route, the neighbor of the drifted node can detect the link failure and sends a link failure notification to its upstream neighbor. This process continues until the failure notification reaches the source node. Based on the received information, the source might decide to re-initiate the route discovery phase.

Original AODV routing protocol is not resetting a new shortest routing path during expire time, because it must maintain it until disconnecting nodes. If it finds a new shortest routing path than already created path during expire time, it does not changing routing path because AODV routing protocol must maintain routing path during expire time Improved AODV routing protocol maintains expire time that created first. So expire time in routing table is not updating until expire time. Therefore, routing table updated in a cycle. Improved routing protocol ensures shortest routing path through fixed expire time. So the source packet sends to destination quickly than original AODV routing protocol.

D. 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.

DSR has been implemented by numerous groups, and deployed on several test beds. Networks using the DSR protocol have been connected to the Internet. DSR can interoperate with Mobile IP, and nodes using Mobile IP and DSR have seamlessly migrated between WLANs, cellular data services, and DSR mobile ad hoc networks.

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 that 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. Other advantages of the DSR protocol include easily guaranteed loop-free routing, support for use in networks containing unidirectional links, use of only "soft state" in routing, and very rapid recovery when routes in the network change. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes, and is designed to work well with even very high rates of mobility.

E. MDSR

To keep the route cache up to date and fresh, a route expiration time is maintained in every node's cache which also reflects the transient and mobility behavior of MANET. In reality it is obvious that not all the nodes are all the time equally mobilizing.

Some nodes might be kept in some fixed places; some sensor devices might be fixed to a particular place for several hours or days. So we could treat such path/route as stable until any nodes in the path changes its location. For stable paths, it is not required to remove the corresponding route cache entry. In some cases all the nodes might arrive to stable state, which might lead the ad-hoc network to a stable network. So why do we use costly routing protocol which is suitable for highly mobile network to a network which is almost stable? Therefore, we introduce this concept in DSR caching policy. All nodes are required to send their movement information (for how long those nodes are stable) with route reply packet while route discovery. May be the nodes will know this information by Global Positioning System (GPS) technology. Therefore the originator could decide whether that path is stable or not.

IV. BLACK HOLE ATTACK

In computer networking, a packet drop attack or black hole 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 routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every n packets or every t seconds, or a randomly selected portion of the packets. This is rather called a gray hole attack. If the malicious router attempts to drop all packets that come in, the attack can actually be discovered fairly quickly through common networking tools such as trace route. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a specific time period or over every n packets, it is often harder to detect because some traffic still flows across the network The packet drop attack can be frequently deployed to attack wireless ad-hoc networks. Because wireless networks have a much different architecture than that of a typical wired network, a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host is able to drop packets at will. Also over a mobile ad hoc network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network.

V. LITERATURE REVIEW

For MANET, various routing protocols are available. Each has its own characteristics and some of them have derived characteristics. Depending upon the nature of application, appropriate routing protocol is implemented. In literature there exist a number of routing protocols in ad hoc networks: proactive protocol, reactive protocol, adaptive protocol, hybrid protocol, hierarchical protocol and geographical protocol.

However on the basis of routing of information primarily there are main classes of ad-hoc routing protocols: table based (Proactive) and on-demand (Reactive) protocols and hybrid protocol (which is the combination of reactive and proactive protocols). In table-based protocols [2] each node maintains a routing table containing routes to all nodes in the networks. Proactive type is operating routing path before sending data. If it changes topology of nodes, this information sends neighbor nodes. And neighbor nodes updated it. The well known proactive routing protocol is DSDV [1]. In on –demand protocols [3] nodes only compute routes when they are needed. Therefore, on-demand protocols are more scalable to dynamic, large networks. On-demand protocols consist of two main phases:

(1) Route discovery: it is the process of finding a route between two nodes.

(2) Route maintenance: it is the process of repairing a broken route or finding a new route in the presence of a route failure.

Both, proactive & reactive, routing protocols for ad-hoc networks may employ unipath and multicast routing. In unipath routing, only a single route is used between a source and destination node. Two of the most widely used routing protocols: Dynamic source routing (DSR) [4] and the ad-hoc on –demand Distance vector (AODV) [5,6] utilize implementation of routing mechanism on the basis of how information is routed. DSR is an on-demand routing protocol for ad hoc networks. Like any source routing protocol, in DSR the source includes the full route in the packet's header. The intermediate nodes use this to forward packets towards the destination and maintain a route cache containing routes to other nodes. AODV, an on-demand routing protocol for ad hoc networks, as opposed to DSR which uses source routing. AODV uses hop-by-hop routing by maintaining routing table entries at intermediate nodes. If it finds a new shortest routing path than already created path during expire time, it does not changing routing path because AODV routing protocol must maintain routing path during expire time. Improved AODV routing protocol reset a new shortest routing path during sending a packet [1].

On the basis of literature survey, it is observed that issues related to MANET are: routing, quality of service, security and power consumption. Among these issues, routing is the most fundamental yet challenging problem for MANETS because it must deal with limitations such as high power consumption, low bandwidth, high error rates and unpredictable movement of nodes.

VI. PROBLEM FORMULATION

We are going to make the enhanced version of MDSR with IDSDV so that black hole attack and other attacks can be handled. Result will be analyzed on the basis of the performance metrics like packet delivery fraction, end–to–end delay, and throughput.

VII. OBJECTIVES

The ad hoc routing protocols are promising routing protocols. They can be used in mobile ad hoc networks to rout packets between mobile nodes. The main objectives of the dissertation are:

(1) Study of MANET routing protocols.

(2) Implementation of IDSDV and MDSR routing protocols in NS2 under hybrid protocol scheme to improve the efficiency of data transmission and security for Black hole and other attacks in the MANETs.

(3) Performance calculation on the basis of Throughput, End to end delay and Packet delivery fraction.

(4) The performance study and comparison for varying type of traffic, for different number of sources, varying number of nodes, speed, and pause time for a number of performance metrics of various routing protocols.

VIII. PARAMETERS REQUIRED

Performance of the work can be calculated on the basis of following parameters:

-Packet delivery fraction

-End–to–end delay

-Throughput

IX. SIMULATOR TOOL REQUIRED

To implement and simulate the IDSDV and MDSR routing protocols NS2(Network simulator version 2) is used. Ns-2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks.

It consists of two simulation tools. The network simulator (NS) contains all commonly used IP protocols. The network animator (NAM) is use to visualize the simulations. Ns-2 fully simulates a layered network from the physical radio transmission channel to high-level applications. The NS-2 simulator has several features that make it suitable for our simulations.

-Supports networking Research and education

- Protocol design, traffic studies, etc.
- Protocol Comparison

-Provide a collaborative environment

- Freely distributed, open source
- Share code, protocols, models, etc.
- Allow easy comparison of similar protocols
- Increase confidence in results

-Multiple levels of detail in one simulator

REFERENCES

[1]. C.E. Perkins and E.M. Royer, "Ad-Hoc on Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.

[2]. C.M Barushimana, A. Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks",

[3]. Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[4]. C. Parkins, E.B. Royer, S. Das, A hoc On-Demand Distance Vector (AODV) Routing. July 2003, [Online]. Available: http://www.faqs.org/rfcs/rfc3561.html. [Accessed: April. 10, 2010]

[5]. T. Clausen, P. Jacquet , "Optimized Link State Routing Protocol (OLSR)", RFC 3626 October, 2003.

[6]. Lucas Guardalben, Joao B.M. Sobral, "A Performance Evaluation of OLSR and AODV Routing Protocols Using a Self-Configuration Mechanism for Heterogeneous Wireless Mesh Networks" guardalben,bosco@inf.ufsc.br 978-1-4244-2413-9/08/©2008 IEEE.

[7]. Dong-Won Kum, Jin-su-park," Mobility aware Hybrid Routing (MHR) approach for WMNs" {80kumsy, yzcho}@ee.knu.ac.kr, 2010.

[8]. Jing Xie, Yuming Jiang," Threshold-based hybrid routing protocol for Manets" ymjiang@ieee.org, 2007

[9]. Julian Hsu, Sameer Bhatia Mineo Takai," compare the Performance of AODV,DSR, OLSR, OLSR v2 and ZRP in REALISTIC SCENARIOS"