Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Power Awared DSR Protocol in MANET

Deepti Chauhan*
Asst. Professor,CSE Deptt,YIET Gadholi
Kurukshetra University, Haryana, India

Ruchi Bawa
M.Tech Scholar,CSE Deptt YIET Gadholi
Kurukshetra University, Haryana, India

Abstract— MOBILE ad hoc networks (MANETs) are collections of mobile nodes, dynamically forming a temporary network without pre-existing network infrastructure or centralized administration [1]. The dynamic nature of mobile ad-hoc networks make traditional routing protocols unsuitable for MANETs. Various routing protocols designed for ad-hoc networks fulfilling a unique set of requirements are viz ADODV, DSDV, TORA, TBRPF and DSR. The Dynamic Source Routing is a simple and robust protocol designed for use in multi-hop wireless ad-hoc network of mobile nodes [8]. Under DSR protocol, adhoc network nodes have to co-operate in packet forwarding and route discovery procedures for the network to operate. Some nodes though, in order to save resources, may exhibit a selfish behavior and not co-operate, thus damaging the efficiency of entire network [10]. This paper proposes a set of minor extensions to the DSR protocol proposed by the IETF MANET working group, by implementing the reputation based scheme on it, that enable to increase the performance of the network. The proposed mechanism allows a node to autonomously evaluate the "reputation" of its neighbors based on the completion of the requested services. This very reputation based technique is used for obtaining route discovery for fruitful results. Simulations will show the increase rate packet receiving and lower in packet loss.

Keywords: DSR, ADODV, DSDV, TORA

I. Introduction

A Mobile Adhoc Network is a group of wireless mobile computers in which nodes cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range. Application such as disaster relief, military excersices and mine site operation may benefit from adhoc networking, but a secure communication is a necessarily required for such applications. Wired networks are less vulnerable to attacks as compared to MANETS due to open medium, cooperative algorithms, dyanamic changing network topology,lack of clear line of defense and lack of centralized monitoring. Security is a process which is secure as its weakest link. So, in order to make MANETs, they can be secured by identifying all its weak points and by making solutions to all those weak points safe. So Security issues in MANETs will remain within a realm of possibility in its research area in future.

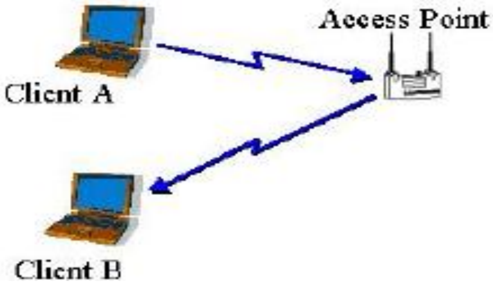

Fig 1. Infrastructure base network

Mobile Adhoc Network (MANET) consists of those independent mobile nodes which communicate to each other through radio waves. There is a direct communication of mobile nodes in a radio range, whereas some intermediate nodes are required to route the packets . These networks can work at any place without the help of any infrastructure and are also fully distributed. Hence these networks highly flexible and robust. The characteristics of these networks are summarized as follows:

- Communication via wireless means.
- The roles of both hosts and routers can be performed by the nodes.
- There is no centralized controller and infrastructure.
- Intrinsic mutual trust.
- Dynamic network topology.
- Frequent routing updates.

Advantages and Applications

Some of the advantages of MANETs are:

- These networks can be set up at any time and place.
- Despite of geographic positions they provide access to services and information.

Some of the applications of MANETs are:

- Disaster relief operations.
- Millitary or police excersices
- Mine cite operations.
- Urgent Business meetings.

II. ROUTING

The routing protocols of traditional wired world are different from the routing protocols used in MANETs. Some of the reasons are listed below:

- Mobility.
- Frequent Route updates.
- Limited transmission range.

The performance criteria of wired networks is also different from that of performance criteria of nodes in MANETs. Some of the performance metrics of MANET routing protocols are :.

- Route Stability despite mobility.
- Energy consumption.

In majority, there are two catagories of Routing Protocols in MANETs:

- Reactive Protocols.
- Proactive Protocols.

Reactive Routing protocols helps in finding routes between two nodes, whenever required. It is different from traditional Proactive Routing Protocols in which in order to maintain routes the nodes periodically sends messages to each other. Reactive Protocols are extensively studied and used in MANETs. From different types of Reactive Routing Protocols, the two of them are given below.

III. DYNAMIC SOURCE ROUTING

Dynamic Source Routing (DSR) uses source routing in which packets can be delivered from one node in a network to some other node. In terms of intermediate nodes in every packet the source node adds the full path to the destination. This information is used by intermediate node to determine whether to accept the packet and to forward it to whom.

IV. ADHOC ON-DEMAND DISTANCE VECTOR ROUTING

Adhoc On demand Distance Vector routing (AODV) is a on-demand protocol. It makes use of routing tables at intermediate nodes rather than relying on source routing. The routing table entries of all reachable nodes in the network are maintained by the nodes. The entries in routing tables are of the form: < Destination, No.of hop, next hop, Sequence Number>. Freshness is maintained by sequence number. The route table is used to route data packets destined for a particular node and to respond to ROUTE REQUEST. A data packet does not need to contain whole route to the destination and so is the advantage of AODV over DSR.

V. SECURITY BASICS

Before proceeding further, the reader should have the knowledge of following terminologies of Network Security:

- Public Key Cryptograpy.
- Symmetric Key Cryptograpy.
- Hash and Message Authentication Codes (MAC)
- Man-in-the-middle attack, Denial of Service Attack
- Authentication and Digital Signatures.

VI. LITERATURE REVIEW

Rajesh Sharma & Seema Sabharwal [1] to provide a solution on the basis of reputation method to solve routing issues raised by misbehaving nodes. The Dynamic Source Routing protocol (DSR) is a routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be self-configuring and self-organizing, without the need for any existing network administration or infrastructure. The protocol is composed of the two mechanisms of Route maintainance and Route discovery, which work together to allow nodes to maintain and discover source routes to arbitrary destinations in an ad hoc network.

Sangheethaa Sukumaran, Venkatesh. J, Arunkorath [8] in recent years mobile ad-hoc networks have become very popular because of their widespread usage. An important issue for communication in ad-hoc networks is due to the cooperation among the nodes But some nodes do not cooperate in communication and saves their energy and are known as selfish nodes. To deal with the selfish behavior of the nodes there are many methods in literature. Different methods available for reducing the effect of selfish nodes in mobile ad hoc networks are also compared in this paper. Some new approaches are also presented in this paper.

Renu Dalal, Manju Khari and Yudhvir Singh [3] provide the different ways to achieve trust in MANET (Mobile Ad-hoc Network) is hot spot for research due to its various advantages and disadvantages. It provides a safe communication between reorganization of the position of nodes, mobile nodes, handling misbehaviour, reducing overhead, and location updates are some difficult issues in ad-hoc network, so providing trust schemes is important in this network.There are some functions of MANETs like communication, routing, packet forwarding, network management etc over self organized network . As mobile nodes comes and leaves the network within a random period of time, it is because MANETs do not have a fixed topology. So, the energy, bandwidth and memory computations of network are being effected. As it doesn't have centralized infrastructure, providing trust in MANET is a crucial task. Different trust model schemes of MANET with their unique features, merits and demerits & findings are studied in this chapter.

Jiwen CAI1, Ping YI1, Ye TIAN, Yongkai ZHOU, Ning LIU1 [15]This author focuses on mobile ad hoc network's routing vulnerability and compares network performance under several attacks. Based on current research, firstly we put forward an enhanced type of black hole. Secondly, this attack can be implimented on DSR protocol, using NS 2, and another two attack patterns-- RREQ flooding attack for comparison and passive black hole. Finally, the authors draw the conclusion that flooding attack is more dangerous than black hole attacks and active black hole

Shakeel Ahmad [17] Ad hoc network is group of wireless nodes to establish a network without any fixed infrastructure or centralized supervision/management. In such types of networks , topology changes dynamically and due to limitations of transmission range, power routing, and bandwidth becomes an important issue. Since 1990 a lot of work has been done in the field of routing in ad-hoc networks . Dynamic Source Routing protocol (DSR) provides efficient and simple routing for multihop ad-hoc network of mobile nodes. A simulation based on performance analysis and comparison between extended DSR and traditional DSR is presented in this paper. A specially designed framework which builds on the Global Mobile Information System Simulator (GloMoSim) is also utilised . Some optimizations of DSR have already been implemented in GloMoSim. Several results have shown that performance got better by traditional (already implemented)

Krishna Paul, Dirk Westhoff [19] there can be several sophisticated attacks motivated by resource saving nature of nodes in a civilian co-operation and selfish nodes based ad-hoc network. Some distributed rating model can be useful to discourage selfish nodes from performing these attacks. It is hard to charge an accused node in a dynamic environment of ad-hoc network even if an attacker is detected. A large range of attacks on Dynamic Source Routing (DSR) protocol and the originator of the attack are detected in this paper and to provide a context aware inference scheme to blame the accused and to provide a mechanism to inform other nodes of the system about the accuse malicious accuser without doubt is also provided.

N.Bhalaji, Dr.A.Shanmugam [13] Because of the rapid proliferation of wireless devices MANETs has become an important technology in recent years. Wired networks are less vulnerable to attacks as compared to MANETS due to open medium, cooperative algorithms, dyanamic changing network topology,lack of clear line of defense and lack of centralized monitoring. In this work we analyze the black hole attack which is one of the possible and common attacks in adhoc networks. In such types of attacks the malicious nodes have the shortest path to the destination. In our approach nodes are classified into 3 catagories based on their behaviour. There have been extensive experiments conducted using the network

S.NO.	SCHEME NAME	ADVANTAGES	FACTORS/BASED ON
1	Core	Used as basis of security mechanism that solves the problems due to misbehaving nodes.	Based on MAC address of every node and this address is received separately from each node.
2	ARM (account based reputation management system)	Used for detecting and eliminating selfish nodes in mobile adhoc networks.	Average system throughput ,throughput initiated by selfish nodes, reputation value vs throughput
3	Confidant	Identifies selfish nodes	Threshold value
4	COSR(cooperative on demand source route)	Handles most of the attacks	Based on MAC layer and network layer

VII. RESULTS

SIMULATE TIME	DSR	MODIFIED DSR-R
0	0	0
2.5	10	122

5	45	303
7.5	88	468
10	130	630
12.5	171	799
15	214	966
17.5	257	1133
20	299	1295

SIMULATE TIME	DSR packet_lost	MODIFIED DSR-R packet_lost
0	0	0
2.5	0	8
5	23	22
7.5	84	136
10	141	291
12.5	205	441
15	260	583
17.5	319	737
20	381	902

VIII. PROPOSED WORK

Methodology /Planning of work:

Dynamic Source Routing, DSR, is a reactive routing protocol that uses *source routing* to send packets. It is reactive like AODV, which means that it only requests a route when it needs one and does not require that the nodes maintain routes to destinations that are not communicating. It uses source routing, which means that the source must know the complete hop sequence to the destination. DSR routing protocol uses two procedures: route discovery and route maintenance.

Route Discovery

Route Discovery is used whenever a source node desires a route to a destination node. First, the source node looks up its route cache to determine if it already contains a route to the destination. If the source finds a valid route to the destination, it uses this route to send its data packets. If the node does not have a valid route to the destination, it initiates the route discovery process by broadcasting a *route request* message.

Route Maintenance

Route Maintenance is used to handle route breaks. When a node encounters a fatal transmission problem at its data link layer, it removes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache.

My proposed work is to apply reputation mechanism to DSR and evaluate its performance. In this work we also considering the malicious nodes, those are not only silently dropping the packet, but also attacking the routing layer. As attractive route having shortest number of hops to destination and higher DSR sequence number. I will use simulation tool to study the performance. The evaluation will be done according to the following metrics:

Packet delivery ratio: is defined as the number of received data packets divided by the number of generated data packets.

Data drop: which is caused, by dropping data packets that is forwarded to it and it drop without transmitting and abnormally under pause of time.

Throughput: it is the ratio of the number of packet delivered to the number of forwarded

IX. CONCLUSION

DSR is a widely used routing protocol for mobile ad hoc networks, but has very low delivery rates and poor performance in lightly loaded networks with high node mobility. This paper presents how the performance will be improved for the reliable data transmission in MANET by applying the reputation based scheme on the DSR protocol. The result will be calculated on the basis of some performance metrics by giving the network simulator parameters like packet received and packet loss. From the observations we conclude that the at different simulation time intervals the packet received in old DSR is at slower rate whereas at the same time interval the rate of packet received in reputation DSR-R is quite high. The packet loss at various simulation intervals is more in the old DSR whereas in the purposed approach DSR-R this loss of packet is quite low.

Thus we got with us fruitful results on comparing the old DSR with our purposed approach i.e DSR-R. This is achieved from the concept of the route discovery with the participation of only the reputed nodes.

REFERENCES

[1] Rajesh Sharma & Seema Sabharwal "Dynamic Source Routing Protocol (DSR)", IJARCSSE, Volume 3, Issue 7, July 2013

[2] Renu Dalal1, Manju Khari and Yudhvir Singh "Different Ways to Achieve Trust in MANET" International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012

[3] Sangheethaa Sukumaran, Venkatesh. J, Arun korath " A Survey of Methods to mitigate Selfishness in Mobile Ad hoc Networks" International Journal of Information and Communication Technology Research Volume 1 No. 2, June 2011

[4] Sangheetaa Sukumran, Venkatesh Jaganathan, Arun Korath "Reputation based Dynamic Source Routing Protocol for MANET" International Journal of Computer Applications (0975 – 888) Volume 47– No.4, June 2012

[5] N.Bhalaji, Dr.A.Shanmugam "ASSOCIATION BETWEEN NODES TO COMBAT BLACKHOLE ATTACK IN DSR BASED MANET", IEEE 2009

[6] Jiwen CAI1, Ping YI, Ye TIAN, Yongkai ZHOU1, Ning LIU1" The Simulation and Comparison of Routing Attacks on DSR Protocol" 2009

[7] Shakeel Ahmad, Irfan Awan, Athar Waqqas and Bashir Ahmad "Performance Analysis of DSR & Extended DSR Protocols", Second Asia International Conference on Modelling & Simulation IEEE & computer society 2008

[8] Krishna Paul, Dirk Westhoff "Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks" IEEE 2002

Managing Reputation over MANETs
Introduction
8-10, reference, literature, types of routing, on demand max., dsr advantages,
Security issue in manet,
Security goals requirement,
Literature review…. Reference 2013 paper drawback
Research objective…..
References……..25-30