International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

REVIEW PAPER ON ENHANCEMENT IN DSR PROTOCOL FOR MULTICASTING IN MANET

Ramandeep Singh[1], Farminder Singh[2]

[1]*RIMT institute of Engineering and Technology, Mandi Gobindgarh , Punjab, India*
[2] *Asst. Professor, Department of Computer Science and Engineering,* Mandi Gobindgarh, Punjab, India

---

Abstract - *MANET is infrastructure less, decentralized multi hope network where the nodes are randomly to move in any direction, there each node works as a router and host to send packet to each other, there is no any requirement of fixed infrastructure. There are various challenges in MANET like security, QoS, routing etc. In this paper we survey on various routing protocols in MANET and proposed a new technique for enhancement in DSR protocol.*

Key Words: MANET- Mobile Adhoc Network, DSDV- Destination sequence distance vector, AODV- Adhoc on demand distance vector, DSR- Dynamic Source Routing, QOS-Quality of Service.

1. INTRODUCTION:

MANET is a mobile ad-hoc network. An ad-hoc network is set of wireless mobile nodes that have ability to communicate with each other without the help any centralized administration. MANET has a dynamic topology due to the mobility of nodes. Wireless network contain collection of mobile hosts (nodes) that are communicate with each other through the wireless links. MANET is infrastructure less, decentralized multi hope network where the nodes are randomly to move in any direction, there each node works as a router and host to send packet to each other, there is no any requirement of fixed infrastructure. MANET provide successful solution in several cases, where any wired or wireless infrastructure is not accessible damaged or destroyed and overloaded due to some reason such as military operations, emergency and Rescue operations, disasters relief efforts and tactical batter field; as well as conferences and class rooms or in research area like a sensor network . MANET is network which is fully distributed and able to work at anywhere without the help of any centralized administration or access points or base stations. It is self-configuring network which is infrastructure less in nature. The infrastructure less network does not need any infrastructure to work. In this network each node can communicate directly with other nodes. So in this network no access point is required. In MANET different mobiles are connected through wireless link. Each mobile are free to move i.e. no central controller available.

1.1 Challenges in MANET:

There are many challenges in MANET which are as follows:

1. Routing: The most common challenging issue in MANET is Routing data packets in between nodes when there is change in the topology. Another challenge for MANET is multicast routing because the nodes are move randomly in the network. Several of the protocol based on the reactive routing rather than proactive routing.

2. Security and Reliability: In an ad-hoc network security is a biggest problem due to the nasty neighbors that are relaying on the information. So there we need of some security mechanism such as the authentication and the management of key provides the security to each node in MANET. Another problem introduced in MANET is due to the wireless links that have finite transmission area is reliability.
3. Quality of service (QOS): The common challenge in changing environment is providing the different quality of service level. An adaptive QOS must be implemented over the traditional resource reservation to support the multimedia services.

4. Inter-networking: To interact with an ad-hoc network, inter-networking between MANET and infrastructure network is often expected in many terms. The coexistence of routing protocol for mobile hosts is a challenge to manage the speed of nodes.

5. Power consumption: For various light-weight mobile devices, the communication related function should be optimized for lean power consumption.

6. Multicast: Multicast is able to support multi-party wireless interaction. The multicast routing protocol must be able to deal with the speed of nodes that include any time leave or join the network, so the multicast tree is no longer static.

1.2 Routing Protocols in MANET:

Routing protocol specifies how to communicate with the help of routers. It shares information among intermediate nodes then with the whole network. It helps to search shortest route from source to destination. There are mainly two types of routing protocol available. These are as following:

1. Proactive Routing Protocol (Table-driven)
2. Reactive Routing Protocol (On- demand)

1.2.1 Proactive Routing Protocol:

Proactive protocol contains fresh list of the route and their destination from source. In this type of protocol one node contains more than one table for each node in the network. All the nodes are update regularly. If the topology frequently changes than update information propagate to every node of the network and update table. For example:

DSDV (Destination sequence distance vector): It is table driven routing protocol. The sequence number is used to distinguish stale routes from new ones and to avoid the loops formation. The periodically stations transmit their routing tables to their immediate neighbors. If a significant change has occurred in its table from the last update a station also transmits its routing table. If two routes have the same sequence number then the route with the shortest route is used.

1.2.2. Reactive Routing Protocol:

It is on-demand protocol. It is lazy approach in which all the node are not contains the information of the all the nodes and maintains table only on demand. To find the path route discovery process is follow. Reactive routing protocols are bandwidth efficient. In this, routes are built as and when they are required. This is achieved by sending route requests across the network. For example:

AODV (Adhoc on demand distance vector): AODV is reactive or on-demand protocol and Use bi-directional links. It is packet routing protocol designed for use in mobile adhoc network.

DSR (Dynamic Source Routing): DSR is a reactive routing protocol for ad hoc wireless networks. It also has on-demand features like AODV but it's not table-driven. It is based on source routing. The Dynamic Source Routing protocol (DSR) is a simple designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes and efficient routing protocol.

2. LITERATURE SURVEY

Seung Yi and Robin kravets [1], had discussed about the public key cryptography which is most effective mechanisms for providing fundamental security services including authentication, digital signatures and encryption for dynamic networks. Effective managements of keys, or digital certificates is one of the key factors for the successful wide-spread deployment of public key cryptography. PKI (Public key Infrastructure) which is an infrastructure for managing digital certificates was introduced for this purpose. The most important component of PKI is the CA (Certificate Authority). CA is trusted entity in the system that checks the validity of digital certificates. The main technique in this approach is to use threshold cryptography to distribute the CA private key among many nodes that collectively act as the CA for the network.

Pradeep Kyasanur [2], had proposed a protocol extension of 802.11 to detect the selfish misbehavior in wireless networks. Selfish hosts that fail to adhere to the MAC protocol may obtain an unfair throughput share. For example, IEEE 802.11 requires hosts competing for access to the channel to wait for a "back off" interval. Selfish hosts may wait for smaller back off intervals than well-behaved hosts, thereby obtaining an unfair advantage. In this paper present modifications to the IEEE 802.11 protocol to simplify detection of such selfish hosts and analyze the optimality of the chosen strategy. It also proposed a penalty scheme for punishing selfish misbehavior and two misbehavior models to capture the behavior of misbehaving hosts. In this paper simulation results under these misbehavior models indicate that our detection and penalty schemes are successful in handling MAC layer misbehavior.

Yixin Jiang et.al [3], In this paper they have proposed a novel secure key sharing and distribution scheme for network mobility (NEMO) group communication. The scheme offers the capability of multiple key sharing and distribution for current and future application scenarios, threshold mechanism that effectively improves flexibility and robustness of the key sharing and distribution

process. Security and performance analysis are presented to demonstrate that the proposed scheme meets the special security requirements for NEMO group communications and is competent for key sharing and distribution service.

Caimu Tang et.al [4], proposed an efficient authentication scheme which is suitable for low-power mobile devices. It uses an elliptic-curve-cryptosystem based trust delegation mechanism to generate a delegation passcode for mobile station authentication. This scheme can effectively defend all known attacks to mobile networks including the denial-of-service attack. The mobile station only needs to receive one message and send one message to authenticate itself to visitor's location register. The proposed scheme only requires a single elliptic-curve scalar point multiplication on a mobile device. This scheme enjoys both computation efficiency and communication efficiency as compared to other known mobile authentication schemes.

Tien-Ho Chen and Wei-Kuan Shih [5], had discussed about importance of authentication in wireless sensor networks(WSNs). They also discussed about das protocol which proposed a hash-based authentication for wireless sensor networks which provides more security against the stolen-verifier, reply and guessing attacks. In this paper they had also discussed about the weakness of Das protocol in mutual authentication for WSN's preservation between users, gateway-node and sensor nodes. They had also proposed a secrecy improvement over Das protocol to ensure that a legal user can exercise a WSN in an insecure environment.

3. PROPOSED WORK

In this work, we mainly focus on to embed the approach of multicasting in DSR protocol for route establishment between source and destination. First of all we deploy the mobile ad hoc network with infinite number of mobile nodes. The mobile nodes are randomly deployed into the fixed area, after this the source and destination are selected for route establishment. For establish the route source node flood the route request packet in the network and route reply packets are send back to the source by the adjacent nodes. The route is established between source and destination on the basis of hop counts and sequence numbers. The existing technique will be implementing in NS2. The New proposed technique will be based on the location. The entire area in which the network is deployed is being divided into the region. The network is divided into the inner square, middle square parts. At inner square and middle square rely nodes are added. The rely nodes are responsible for route establishment. In the rely nodes information is stored about the nodes which are in inner square or on middle square. The proposed technique will be implemented in NS2 and compared with the existing protocol graphically.

4. CONCLUSION

Security is most important feature for wired and wireless network communication. The success of MANET strongly depends on security. We have a variety of attacks and weakness in the routing protocols. Now days, Routing of the network is most important and very biggest challenge in Mobile Ad-Hoc Network. Routing is responsible for degradation of the network performance. In this survey paper we proposed a new technique for enhancement in DSR protocol for multicasting in MANET which helps to improve the performance of network, security and Quality of services.

REFERENCES

[1] Seung Yi, and Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks", *10th IEEE* International Conference on Network Protocols (ICNP'02), No.1092-1648, 2002.

[2] Pradeep kyasanur "Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing,2005.

[3] Yixin Jiang Chuang Lin, Minghui Shi, Xuemin Shen "Multiple Key Sharing and Distribution Scheme With (n; t) Threshold for NEMO Group Communications", IEEE 2006.

[4] Caimu Tang, Dapeng Oilver, "An Efficient Mobile Authentication Scheme for Wireless Networks",IEEE.

[5] Tien-Ho Chen and Wei-Kuan, Shih , "A Robust Mutual Authentication Protocol for Wireless Sensor Networks ETRI Journal, Volume 32, Number 5, October 2010.