Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Dynamic Source Routing Protocol (DSR)

Rajesh Sharma
AssistantProf. in CSE Department
BITM College, Dhurala Kurukshetra, India

Seema Sabharwal
Assistant Prof. in CSE Department
GEETA College, Kanipala Kurukshetra, India

Abstract: 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. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. The aim of this research is to provide a solution on the basis of reputation method to solve routing issues raised by misbehaving nodes.
Keywords:

I. Introduction

Mobile networking is one of the most important technologies supporting pervasive computing. During the last decade, advances in both hardware and software techniques have resulted in mobile and wireless networking. Generally there are two distinct approaches for enabling wireless mobile units to communicate with each other:

Infrastructure: Wireless mobile networks have traditionally been based on the cellular concept and relied on good infrastructure support, in which mobile devices communicate with access points like base stations connected to the fixed network infrastructure. Typical examples of this kind of wireless networks are GSM, WLL, WLAN, etc.

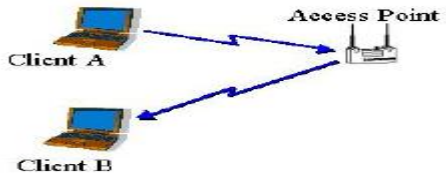

Figure: 1.1. Infrastructure base network

Infrastructure less: In infrastructure less approach, the mobile wireless network is commonly known as a mobile ad hoc network (MANET). A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. This is very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of wireless connections on the fly. Wireless ad hoc networks themselves are an independent, wide area of research and applications, instead of being only just a complement of the cellular system.

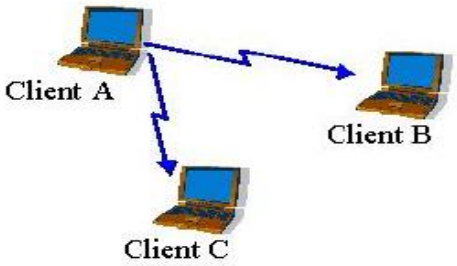

Figure: 1.2. Infrastructure less Adhoc network

Performance Evaluation Using Reputation Scheme

Reputation in MANET is collected information about one entity's former behavior as experienced by others. *Trust* expresses an entity's willingness to proceed with an action that might be harmful based on information like the risk, benefit and reputation of involved entities. Reputation systems collect ratings, process and consolidate this information and make it available upon request. This has two effects: They provide information that allows users to predict how someone may behave in future. Simultaneously, they influence the future by giving the incentive to behave well. A reputation is defined as an import of the past behavior of an entity. It has been used by the entities in the brick and mortar world to find out the probability of achieving the desired level of satisfaction from their transaction with the other entity whose reputation is being evaluated. The reputation was used in the networks in general and Internet in particular only in the late 1990. At a first glance it seems unreasonable to base trust in information spread by a user on his reputation, because he may only pass on what he has learned from someone else. However, reputation systems should motivate users to verify information before spreading it further or to mark it as uncertain. Most existing approaches to use reputation systems for mobile ad-hoc networks concentrate on solving routing issues raised by misbehaving nodes. They also neglect the dynamics of a scenario with highly mobile nodes where the chance to meet someone again is low. In the majority of cases privacy issues are completely ignored. Especially when a human user as the owner of a device is involved, reputation is sensitive personal information. Often it contains detailed information about the entity's former transactions including and it is critical for an entity not to lose reputation by false accusation.

II. Related Study

Prashant Dewan and Partha Dasgupta, "*Trusting Routers and Relays in Ad hoc Networks*." Proceedings of the 2003 International Conference on Parallel Processing Workshops. [1].

This paper provides the mechanisms for trusting routers & relays. It enumerates the issues involved in using reputation in Adhoc networks. It protects the end to end by public key infrastructure. It discussed some designed goal on which the paper is basis. Like if a node is malicious then the collaborating node must not with them if it so then whole network will collapse. Node should not fake in the sense that it should of the same networks. Node should be punishing on bad reputation. It provides solution to the routes in trusting. A threshold mechanism is used for reputation in this paper.

Po-Wah Yau and Chris J. Mitchell, "*Reputation Methods for Routing Security for Mobile Ad Hoc Networks*"[2].

This paper discusses the effect of malicious node behavior & also provides a solution on the basis of reputation method. It first discuses the two reputation protocols & then compares both of them. On the basis of these it provides a solution for analyzing the reputation values. Calculating the reputation values. Detecting the misbehavior of unwanted type provide a reputation Mechanism. Reputation system is also employed in the localized mechanism where both positive & negative behavior is severely affects the reputation values. It categorizes the nodes in to different scenarios a threat model for

Ad hoc routing protocols were described, classifying internal attacks into four categories — failed badly failed, selfish, and malicious nodes. Failed and selfish nodes are those which do not perform certain operations that the protocol specifies that they should, the former due to some unforeseen failure and the latter due to selfishness to conserve power.

P. Michiardi and R. Molva, "*CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks*," Proceedings of the 6th Joint Working Conference on Communications and Multimedia security, September 2002, pp. 107-121. [3]

CORE is another reputation-based solution. The authors regard a mobile ad hoc network as a community, in which only ones contributing own resources are entitled to use shared resources. In CORE, three types of reputations are employed. Subjective reputations values are obtained directly from a node's own observation of behavior of its neighbors. Contrary to CONFIDANT, more weight is assigned to past observations to prevent false detection caused by link breaks or collisions. Indirect reputation values are obtained from other nodes, and only positive values are considered to avoid denial of service attack (broadcasting negative ratings for legitimate nodes). Function reputation values are related to certain functions like routing and data forwarding. Global reputations are calculated in terms of subjective reputation and indirect reputation on different functions.

S. Marti, T. J. Giuli, K. Lai, and M. Baker, "*Mitigating routing misbehavior in mobile ad hoc networks,*" Proceeding of MOBICOM, Aug 2000 pp 255-265. [4]

This paper provides solution to packet lost problem caused by misbehaving nodes in mobile ad hoc networks. Two extensions are introduced to DSR to mitigate the effects of misbehaving nodes. The watchdog is in charge of monitoring neighbors to identify misbehaving nodes, and the path rater tries to prevent packets being delivered through these nodes.

After a node forwards a packet, its watchdog checks whether the next node on the path forwards the packet cooperatively. The watchdog performs this operation by listening promiscuously to the next node's transmissions. If the number of packets a neighboring node drops exceeds a threshold, that neighbor will be regarded as a misbehaving node. The watchdog needs to know the next two hops in order to monitor the next node's data forwarding behaviors. Therefore, watchdog is implemented based on DSR. The path rater in each node selects the most likely reliable route according to knowledge of misbehaving nodes and link reliability information. It calculates the route metric by averaging the rating of all nodes on a path and chooses the path with the highest metric. In this solution, the node rating is calculated in terms of link reliability rather than neighbor monitoring results.

International Journal of Computer applications (0975 – 888) Volume 47– No.4, June 2012. Reputation based Dynamic Source Routing Protocol for MANET[5]

This paper proposes a new reputation based routing protocol based on DSR (Dynamic Source Routing) and through simulation results proves that the proposed method performs well compared to normal DSR.

III Conclusion

This paper explained about the DSR routing protocol using reputation mechanism. Various approaches to calculate the reputation values of the nodes using simple formula have been studied. Any node is supposed to maintain a good reputation value in order to receive network services.

REFERENCES

[1] Prashant Dewan and Partha Dasgupta, "Trusting Routers and Relays in Ad hoc Networks." Proceedings of the 2003 International Conference on Parallel Processing Workshops

[2] Po-Wah Yau and Chris J. Mitchell, "Reputation Methods for Routing Security for Mobile Ad Hoc Networks"

[3] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Proceedings of the 6th Joint Working Conference on Communications and Multimedia security, September 2002, pp. 107-121.

[4] S. Marti et al., "Mitigating routing misbehavior in mobile ad hoc networks," Proceedings of Sixth Annual IEEE/ACM Intl. Conference on Mobile Computing and Networking, April 2000, pp. 255-265.

[5]. International Journal of Computer applications (0975 – 888) Volume 47– No.4, June 2012. Reputation based Dynamic Source Routing Protocol for MANET.

