International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Adaptive Approach to find a Stable Path between Nodes in MANET

Gagandeep Singh Hundal[Å*], Sunil Kumar Gupta[Å] and Rajeev Bedi[Å]

[Å]CSE Dept., BCET Gurdaspur, Punjab, India

Accepted 16 August 2014, Available online 25 Aug 2014, **Vol.4, No.4 (Aug 2014)**

Abstract

MANET stands for Mobile Ad hoc Network. Mobile ad hoc network is an arrangement of wireless nodes which are free to move and are not controlled by any centralized mechanism. Nodes in mobile ad hoc network act both as hosts as well as routers. The nodes establish a dynamic network. Due to this dynamic nature of topology, Link Failure problem often degrades the network performance. This paper outlines link failure problem in Mobile Ad hoc Network. A new method has been proposed to eliminate link failure in Mobile ad hoc network by using signal strength parameter in AODV and provide a stable path for data transmission.

Keywords: *MANET, link failure, AODV, signal strength.*

1. Introduction

Mobile Ad-hoc Networks (MANET) are future wireless networks consisting entirely of mobile nodes that communicate on-the-move without base stations. Nodes in these networks will both generate user and application traffic and carry out network control and routing protocols. Rapidly changing connectivity, network partitions, higher error rates, collision interference, and bandwidth and power constraints together pose new problems in network control particularly in the design of higher level protocols such as routing and in implementing applications with Quality of Service requirements. The routers are free to move randomly and organize themselves arbitrarily thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Sensor nodes consist of sensing, data processing, and communication components and typically form ad hoc networks.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. Even it very useful in the today's world but it has some limitations because of its some security issues and performance.

*Corresponding author **Gagandeep Singh Hundal** is a M.Tech Student; **Dr. Sunil Kumar Gupta** is working as Associate Professor; **Rajeev Bedi** as Assistant Professor

2. Literature Review

Jeroen Hoebeke *et. al* [2005], discussed about application of mobile ad-hoc networks and the challenges being faced. In this paper, a complete introduction has been given about the wireless networks. Moreover this paper provides an insight into the potential applications of ad-hoc networks and discusses the technological challenges being faced by network and protocol designers. Most prominent of the challenges are routing, resource and service discovery and security. Different attacks pertaining to security are deletion, fabrication, replication and redirection of data packets. But despite challenges, mobile ad-hoc network opens a new business opportunity for service providers.

Umesh Sehgal *et. al.* (2009), analyzed the demands of Ad-hoc environment. This paper focuses on three areas of Ad-hoc networks, key exchange and management, Ad-hoc routing, and intrusion detection. Intrusion detection is a critical security area. But it is a difficult goal to achieve in the resource deficient Ad-hoc environment. But the flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application. Public key systems are generally espoused because of its upper hand in key distribution. Third party (trusted) called Certification Authority (CA) is used for key management.CA has a public/private key pair, with its public key known to every node and signs certificates binding public keys to nodes. The trusted CA has to stay online to reflect the current bindings.

Li-Li PAN (2010), put forward a secure Ad Hoc on Demand Routing (SAHODSR) protocol which adapts for Ad hoc network aiming at the mobile ad hoc network (MANET) routing protocol attacks and typical routing scheme of security Problems. This protocol uses serial

number of destination node, list session keys of neighbor nodes between the mobile nodes and message authentication code (HMAC) based on hash Function to verify the validity of routing discovery and route reply. Neighbor nodes defend against a variety of attacks through binding MAC address with its ID. SAHODSR protocol can defends and resist a variety of attacks, such as denial of service attacks, forgery attacks on the source node and destination node, tampering attacks, black hole attacks, wormhole attacks. It achieve better safety performance through the costs of paying more route discovery time than the DSR, slightly longer average route length and longer transmission delay.

Yudhvir Singh *et. al.* (2010), evaluated On Demand multicasting routing protocols in Mobile ad hoc network based on the performance metrics like Packet Delivery Ratio, End to End delay and average throughput.Nodes are free to move, independent of each other which makes routing much difficult. The routing protocols in MANET should be more dynamic so that they quickly respond to topological changes. On-Demand Multicast Routing Protocol is a protocol for routing multicast and unicast traffic throughout adhoc wireless mesh networks. ODMRP creates routes on demand so they suffer from a route acquisition delay, although it helps reduce network traffic in general [18]. The simulation results shows that Average throughput of ODMRP is better than AODV and FSR with the varying number of nodes and also with the increase in mobility. Packet delivery ratio for AODV is better than that of ODMRP and FSR with the changing number of nodes as well as with changing mobility.

R. Ramesh *et. al* (2010), discussed about the advantages and disadvantages of using MANET. Increase in the number of nodes in the wireless computing environment leads to different issues like power, data rate, QoS, simulators and security. Among these, security is the peak issue faced by most of the wireless networks. Especially networks without having a centralized system (MANETS) face severe security issues. One of the major security issues is the wormhole attack while finding the shortest path. The author proposed an algorithm to find a secure shortest path against wormhole attack. Existing algorithms are mainly concentrated on detecting the malicious node but they are hardware specific like directional antennas and synchronized clocks. But the proposed algorithm is both software and hardware specific. RTOS is included to make the ad hoc network a real time application.

S. Albert Rabara *et. al.* (2011), discussed about the technical challenges MANET poses as well as the great opportunities offered by MANET. The special features of MANET bring great opportunities together with severe challenges. The paper points out some of the key research issues to promote the development and accelerate the commercial applications of the MANET technology. A special attention is paid on to highlight the integration of MANET with the significant features of IPv6 such as integrated security, end-to-end communication.

Sunil Taneja *et. al* [2011], demonstrated the performance based comparison of the two most widely used routing protocols, AODV (Ad hoc On Demand Distance Vector) & DSR (Dynamic Source Routing), used in mobile ad-hoc networks. Both these protocols have their own advantages. DSR (Dynamic Source Routing) does not uses periodic routing messages like AODV (Ad hoc On Demand Distance Vector), thereby reducing network bandwidth overhead. Moreover the routes are maintained only between nodes that need to communicate. Thus route maintenance overhead is reduced. AODV (Ad hoc On Demand Distance Vector) routing protocol favors least congested route instead of the shortest route. AODV (Ad hoc On Demand Distance Vector) is better performer when the medium is denser and thus enjoys a preference than DSR (Dynamic Source Routing) over mobile ad-hoc networks.

Praveen Joshi [2011], discussed security concerns in routing protocols in MANET (Mobile Ad hoc Network). The various routing protocols used can be broadly classified into proactive and reactive routing protocols. Cryptography, authentication, digital signatures can be used to prevent malicious attacks. Moreover intrusion detection systems and cooperation enforcement mechanisms can be used for this purpose. This paper provides an insight into the various attacks and the counter mechanisms employed against the malicious attacks.

Sunita Nandgave-Usturge (2012), discuss about the routing in mobile ad hoc networks. The main reason of link failure in mobile ad hoc networks is mobility, interference and congestion. Mobility means each node is free to move within its transmission range. In MANET congestion occurs when the amount of data sent to the network exceeds the available capacity. Such situation leads to increased buffer space usage in intermediate nodes, leading to data losses. Congestion is detected at transport layer. Congestion is main reason for performance degradation of TCP. Packet loss reasons are node mobility and link layer congestion. Cross layer approach is used to improve TCP performance. Cross layer approach is used to solve route failures. AODV has better congestion avoidance mechanisms. This paper addresses four signal strength based congestion control mechanisms AODV, Reliable AODV, MAODV, and CLS_AODV.

Reena Thakral *et. al.* (2012), proposed a routing protocol emphasizing to find out a path between source and destination keeping in view the available power of a node. The paper contains an improvement for the link failure for the mobile ad hoc network with minimum power consumption which further improves the quality of services. It is an extended version of link failure based on power failure. The parameters used in the proposed algorithm are TTL (Time to Live) and minimum required power for communication. The proposed solution is to determine the minimum available power between sources to destination. Based on this information the source node decides the path which has maximum available power between source to destination node.

Asha Ambhaikar *et. al* (2012), proposes a new technique for path updating and resolving link failure in AODV protocol. In this proposed scheme, each time a node discovers a new neighbor, information is exchanged between these two nodes. For each routing table

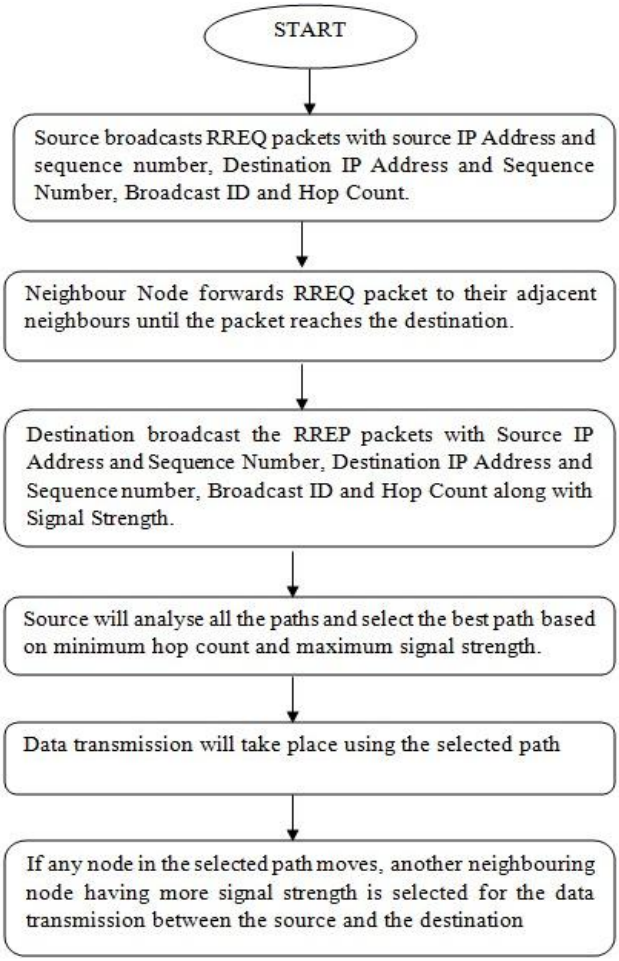

Fig. 1 Methodology used

destination address, no of hop towards the destination, sequence number and expire time of an entry is extracted. These extracted entries are exchanged with the new neighbor node. If a destination is found it means that beside the current path in routing table, there is a new path through the new neighbor node. The number of hops of the two paths is then compared. If the new path is better (with smaller number of hops) it will replace the current one. The improved AODV protocol provides better performance based on packet delivery ratio and end to end delay.

Vibhor Kumar Goal *et. al.* (2013), proposed a routing protocol which improves the link failure by using stability concept. The routing protocol uses parameters like TTL, Available power list and Available Band Width List for communication. The route request packet sent by the source node contains information like TTL, A_Power, A_Bandwidth, Broadcast ID, Source Address and Destination Address. When the neighbors receive this RREQ packet TTL value is checked first. If the destination address is the address of the current node, it consumes the packet and calculates the average power of the current path. If not it forwards the packet after entering the value of available power and bandwidth in this RREQ packet. This protocol aims at improving the link failure problem due to power between the source and the destination nodes.

3. Problem Formulation & Objectives

After going through the existing literature it has been observed that the existing techniques are not completely reliable. Stable and high speed routes are the demand of time to ensure better packet delivery ratio between the nodes. In order to maintain a stable path between source and destination, dynamic switching between the nodes has to be used. Whenever a node in the selected route moves, another neighboring node with highest signal strength is selected for data transmission. This technique not only ensures a stable path but also reduces the number of hops between the source and the destination as compared to the methods traditionally used.

4. Methodology

The methodology is show in figure 1.

Conclusion & Future Scope

In this paper, a technique has been proposed to provide more stability during data transmission in MANET after detection of broken links is done. Identification of Broken link will be done by using Request and Reply method. It leads to less routing overhead and high packet delivery ratio. Further, implementation of the proposed technique

will be done using network simulator (NS2). Also testing of the new scheme against parameters like throughput end-to-end delay, overhead, and packet loss will be done.

References

J. Hoebeke, I. Moerman, B. Dhoedt and P. Demeester (2004), An Overview of Mobile Adhoc networks: Applications and Challenges, Security Magazine, pp. 60-66.

U. Sehgal, M. K. Kaur and M. P. Kumar (2009), Security in Vehicular Ad hoc networks, IEEE Second International conference on Computer And Electrical Engineering, pp. 485-48

L.-L. PAN (2010), Research and Simulation for Secure Routing protocol based on Ad Hoc Network, IEEE Second International Conference on Education Technology and Computer, vol. V, pp. 46-4

Y. Singh, Y. Chaba, M. Jain and P. Rani (2010), Performance Evaluation of On Demand Multicasting routing protocol in Mobile Adhoc Networks, IEEE International Conference on Recent Trends in Information, Telecommunication and Computing, pp. 298-301

R. Ramesh and S. Gayathri (2010), RTOS based Secure Shortest Path Routing Algorithm in Mobile Ad Hoc Networks, IEEE, pp. 1-24.

S. Taneja, D. A. Kush and A. Makkar (2011), End to End Analysis of Prominent on Demand Routing protocols, International Journal of Computer Science and technology, vol. II, no. 1, pp. 42-46.

P. Joshi (2011), Security issues in Routing Protocol in MANET at Network Layer, Elsevier Procedia Computer Science, pp. 954-960.

M. S. Nandgave-Usturge (2012), Study of Congestion control using AODv and Signal Strength by Avoiding Link Failure in Manet, IEEE International Conference on Communication, Information and computing Technology, vol. IX, no. 12, pp. 1-5.

R. Thakral and R. Rani (2013), Improve link failure routing Protocol in Mobile Adhoc Networks, International journal of Advance Research in Computer Science and Software Engineering, vol. III, no. 6, pp. 1229-1233.

A. Ambhaikar, H. Sharma and V. Mohabey (2012), Improved AODV Protocol for Solving Link Failure In Manet, International journal of Scientific and Engineering Research, vol. III, no. 10, pp. 1-4.

V. K. Goal, R. Srivastava and V. Malik (2013), Algorithm for Improvement of Link Failure in Mobile Adhoc Network, International journal of Science and Emerging Technologies with Latest Trends, vol. X, no. 1, pp. 15-18.