ISSN: 2321-7782 (Online)

Volume 2, Issue 11, November 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

An Efficient Data Transmission Strategy in Mobile Ad Hoc Network

S. Vennila[1]
PG Scholar / CSE
SNS College of Technology

I. Kala[2]
Associate Professor / CSE
SNS College of Technology
Coimbatore-35,India

Dr. S. Karthik[3]
Professor & Dean / CSE
SNS College of Technology
Coimbatore-35, India

Abstract -A Mobile Ad hoc Network (MANET) is a wireless network of mobile nodes without any fixed infrastructure. Due to unique characteristics, such as limited bandwidth and power, routing in a MANET is one of the challenging tasks compared to traditional network. At present many efficient routing protocols have been implemented. Even though due to presence of limited bandwidth and power in MANET, an efficient data transmission with fault detection mechanism is important. So various methods are survey and key ideas are listed.

Keywords— Mobile ad hoc networks, bandwidth, power, routing protocols.

I. Introduction

A Mobile Ad hoc Network (MANET) is a collection of mobile devices that can dynamically change the topology without the need for pre-existing network or central administration. Some of the characteristics of MANET are frequent host movement and multihop wireless link. Both the bandwidth and battery power are scarce resources at mobile nodes. So the conventional routing protocols could not be applied to MANET. Hence designing of the routing protocol for MANET becomes a vital issue. Many routing protocols [6] have been developed this protocols can be divided as table driven and on-demand routing. In table driven or proactive every node maintains the network topology in the routing table by periodically updating the routing information. On the other hand reactive or on-demand routing protocol does not maintain the network topology information. They establish the path only when it is required. Some of the applications of MANET are disaster relief, commercial application like personal area networks, emergency application, etc.

II. Literature Survey

In [1], the authors proposed a scheme (AODV-BR) Ad hoc On-demand Distance Vector Backup Routing to improve existing AODV [9] protocols by creating a mesh and providing multiple alternate routes. In AODV when route disconnects, the broken route nodes simply drop data packets, since no alternate path to the destination is available until a new route is established. Mesh structure is to provide multiple alternate paths to existing on-demand routing protocols without producing addition control messages.

Selection of alternative route when direct route breaks:

AODV-BR is motivated by duct routing scheme used at early 1980's.It has some disadvantage; many duplicate data packets are propagated, through multiple path at all instances, it create excessive redundancy which leads to congestion and collision. But in AODV-BR multiple alternate paths [7] is used only when primary route is disconnected. It has direct route and alternative route. Direct route is established between source and destination. An alternative route is established when path link of a particular node break, it selects any one of the node which is nearby within the radio propagation range. Both direct route and alternative routes together form mesh structure and that is similar to a fish bone.

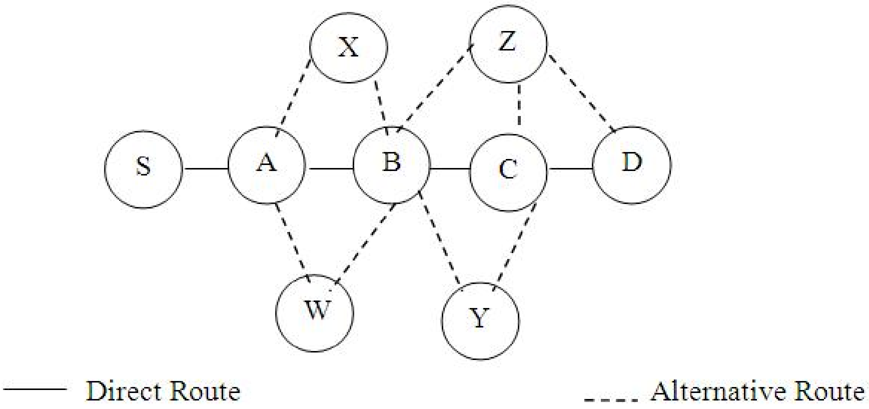

Fig1. An alternative path with the same path length as the direct route

Fig1. Shows how mesh and alternative routes are constructed and used. Here when RREQ reaches the node D, the direct route <S-A-B-C-D> is selected. So when node D send RREP to node C, the node Z and Y overhear the packet and make entry in its alternate route table. If the link between C and D is disconnected or breaks, it may choose either Z or Y (i.e. alternative route) and send the packet to B. If Z selects the route to send the packet, Y will not send the packet, since it learns that Z is going to send the data. Alternative path is used only when the packets cannot send through direct route. So this AODV-BR provides robustness to mobility and enhances the performance.

Wojciech Galuba et-al in [2] proposed the protocol Continuously Adapting Secure Topology Oblivious Routing (CASTOR), which does not use any control messages except the acknowledgements and routing decisions are taken independently without exchanging any routing state with other nodes. This protocol provides high packet delivery rates in large and volatile networksCastor, (i) packets does not have routes, thus packet length is less than that of network size,(ii) It has only data and acknowledgement and no route discovery control packets,(iii) Each node kept communication reliability information locally and not at the source,(iv)Castor does not seek to identify and exclude attackers,(v) It relies on the simple trust management assumption. Thus this protocol is more powerful to attacks than the existing secure communication protocol.

The authors of [3] proposed a Adaptive Load Balancing Routing Algorithm based on Gossiping mechanism (ALBR-G). Most of the routing algorithm in MANET based on some flooding mechanism. But ALBR-G combines the load balancing and the gossip-based routing and is effective for load balancing and reduces the routing overhead in the network.

ALBR_G is grouping of load balancing and gossip-based routing:

ALBR-G is based on AODV which is an on-demand routing protocol that has two phases: route discovery and route maintenance. It uses the Helloe packets and adds the load intensity function (LIF) to it. Before sending Helloe packets to intermediate node it first checks the current LIF and updates the Helloe packet. When source node starts to find route by broadcasting route request(RREQ) packet to intermediate node .it checks whether RREQ received is new packet or not.

Hop count parameter is set. If the RREQ is new, it is compared with the parameter. If it is smaller than hop count parameter than RREQ will be forwarded to prevent death of RREQ. Else it will not discard immediately; it is cached for a period of time. If same RREQ received from neighbor nodes, we can believe that there are adequate nodes to join in route establishment. Then RREQ is discarded from cache. When destination receives the first RREQ, it sends RREP to source node. Once source node receives RREP, then it starts to send the data. The route maintenance phase of ALBR-G is similar to AODV[9]. When node link is break, the upstream node sends the route reparation. If it fails, then a route error (RERR) packet is send to source to restart the route discovery procedure. So this algorithm adjusts the income RREQ messages according to the distribution and load status of nodes in route discovery phase.

In [4] the authors described about ad hoc on-demand multipath distance vector (AOMDV) which guarantees loop freedom and disjointness of alternate paths. It also reduces packet loss and routing overhead. It is the extension of AODV [9].In AODV source node floods the RREQ to destination and waits for RREP. When intermediate node receives RREQ, it sets the reverse path by using the previous hop and if there is valid route to destination, it unicast a RREP back to source. Only first copy of RREQ is received and duplicate copies are discarded. The destination on receiving RREQ, it sends the RREP through the reverse path. When link failure occurs it sends RERR (route error packets). So when source receives RERR it initiates a new route discovery.

In AOMDV RREQ is propagated from source to destination in multiple reverse paths both at intermediate nodes and at destination. This multiple path discovered is loop free and disjoint.

In [5] the authors proposed the secure message transmission (SMT) and its alternate, the secure single-path (SSP) protocols. Both SMT and SSP find the transmission failures continuously configure their operation to avoid and tolerate data loss. The aim of SMT and SSP is to secure the data transmission. The main difference is that SMT utilizes multiple paths simultaneously whereas SSP use single path operation.

SMT uses an active path set (APS) which comprise node disjoint paths at the source. Here source send data which has limited redundancy to the data, so that it divide the information into piece. At destination side only some of them are received and some of the message pieces are lost or corrupted. After a period of time destination send the feedback about the lost data. So the source again re-transmits the lost pieces. After a period of time the destination send the feedback again to the source.

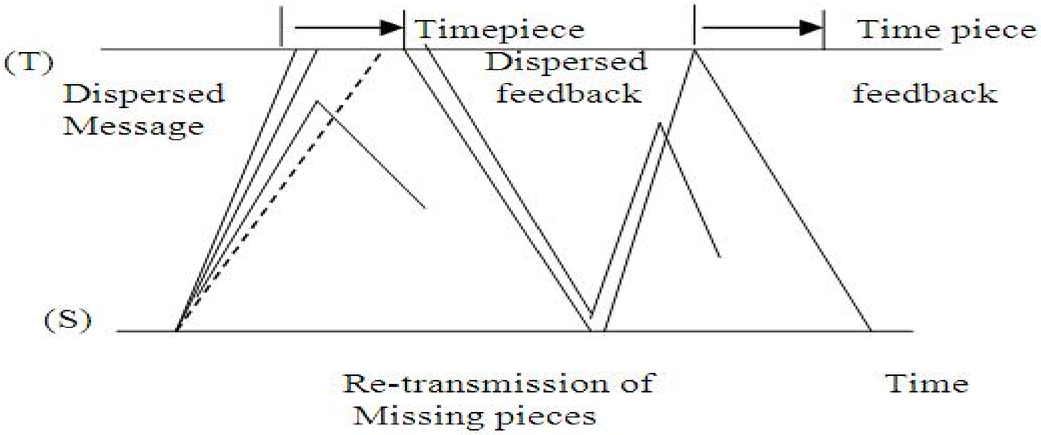

Fig2.SMT transmission of a single message

SSP also provides data integrity, authenticity and reply protection and is designed with same and to-end feedback and fault detection mechanisms. The main difference is that SSP transmit data across single route and does not perform data dispersion. So both the protocols are designed for secure data transmission in ad hoc networks.

Chai Keong Toh, et.al. of [6] proposed varies load metrics and load balanced routing protocols for ad hoc network. Ad hoc routing protocol mainly uses the shortest paths to transfer the packets. When this path is used frequently it leads to degrade in bandwidth, power, and battery energy and memory storage. It also leads to packet loss and overflow, resulting in longer end-to-end delay, decrease in throughput, etc, This load balancing routing protocols can be classified into three types,

Delay-based: By avoiding the nodes with high link delay load balancing can be achieved.e.g Load-Aware On-Demand Routing (LAOR).

Traffic-based: Here load balancing is achieved by equally distributing traffic load in the network e.g. Associativity Based Routing(ABR) , Traffic-Size Aware(TSA) and Load Balanced Ad hoc Routing(LBAR).

Hybrid-based: It is the combination of delay and traffic based techniques .e.g. Content Sensitive Load Aware Routing (CSLAR) and Load Aware Routing in Ad Hoc (LARA).

LAOR is the extension of ad hoc on-demand distance vector (AODV) routing. Load balancing can be achieved by total route delay and route hop count. Source send route request (RREQ).If it does not have proper route to destination, the intermediate node update the total delay to RREQ and routing table. Unlike AODV [9] if intermediate node receives duplicate RREQ with smaller total delay and hop count, it is updated in route table and it is used then destination sends the RREP to source.

***Three phases of ABR**:*

Path discovery, path reconstruction and route omission. A node first sends the broadcast query(BQ) .When intermediate node receive this BQ it append their address with it along with route relaying load(RRL) information into query packet. The destination node thus knows after receiving the first BQ at certain time, about all possible routes and qualities.

In CSLAR, the node sends the packet and if does not have no available path to destination, it floods to all intermediate nodes after it append their load values to the request message. But the intermediate nodes can’t send route reply back to source even if they have routes. The destination node then reply to route request based on route load value. Once source receives the route reply, then it uses the selected route for data transmission. Load metric is that how busy a node while forwarding and receiving the packets across the network. Different load metrics are:

Active path: Number of active routing used by a node.

Traffic size: This tells about the traffic load present at a node [6].

Packets in interface queue: Total number of packets buffered in a node both at sending and receiving the data.

Channel access probability: It refers to degree of channel contention with neighboring nodes.

Node delay: Delay take place at packet queuing, processing and successful transmission.

In [7] the authors described about multipath routing protocol called TOHIP (A topology-hiding multipath routing protocol).In TOHIP the packets will not carry any routing information’s. So the attacks like wormhole attack [11], black hole attack, rushing attack and Sybil attack can’t deduce network topology and can’t launch various attacks[12]. It finds multiple disjoint routes in a route discovery and excludes all unreliable routes before transmitting packets. A routing protocol is topology hiding when hop count between two node is greater than 2.There are three phases in TOHIP [4]they are, route request, route reply, route probe. Route request creates reverse route and it will be used in route reply phase. Route reply finds the node-disjoint routes and exclude at transaction time. Route probe detects the unreliable routes before transmitting the packets. Each node maintains the routing table (RT) and sequence number table (SNT).

RT will have the destination sequence number, RREQ sender, hop+1. In SNT each node will have unique sequence number which is used to avoid duplicate packets. Each node checks SNT and RT when node is transfer. If it’s a new node it is recorded in SNT and hop count is incremented and broadcast REEQ. If not it will be discard. So by using TOHIP has better performance in finding the rout

III. CONCLUSION

Due to mobile nodes in MANET, it has limited bandwidth and power. It leads to packet loss, delay, consumption of energy etc,. So various routing protocols were surveyed and in future it is useful to design data transmission strategy with fault a detection mechanism which is used to transmit the data in efficient manner.

ACKNOWLEDGEMENT

The author is greatly obliged to BCUD, Savitribai Phule Pune University Pune for the financial support through Minor Research Project Scheme. The author wishes to thank Dr. S. C. Mehrotra, Dr. J. B. Shinde and Prin. P. A. Lawande for valuable guidance and encouragement.

References

1. S.J. Lee, M. Gerla, and AODV-BR: backup routing in ad hoc networks, in: IEEE Wireless Communications and Networking Conference (WCNC), 2000, pp. 1311–1316.
2. W. Galuba, P. Papadimitratos, et al., Castor: scalable secure routing for ad hoc networks, in: IEEE Conference on Computer Communications (INFOCOM), (2010).
3. Zhu Bin, Zeng Xiao-ping, Xiong Xian-sheng, Chen Qian, Fan Wen-yan, Wei Geng., A Novel Adaptive Load Balancing Routing Algorithm in Ad hoc Networks., Journal of Convergence Information Technology Volume 5, Number 5, July (2010)
4. M.K. Marina, S.R. Das, Ad hoc on-demand multipath distance vector routing, Wirel. Commun. Mob. Comput.6:969-988(2006).
5. P. Papadimitratos, Z.J. Haas, Secure data communication in mobile ad hoc networks, J. Select. Areas Commun. 24 (2) 343–356 (2006).
6. C.K. Toh, A.N. Le, et al., Load balanced routing protocols for ad hoc mobile wireless networks, IEEE Commun. Magaz. 47(8)78–84 (2009).
7. Yujun Zhang, Tan Yan, Jie Tian , Qi Hu , Guiling Wang, Zhongcheng Li.,TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks., in Elsevier as Ad Hoc Networks 109–122 (2014).
8. M. Burmester, B. Medeiros, On the security of route discovery in MANETs, IEEE Trans. Mob. Comput. 8 (9) 1180–1188 (2009).
9. M.K. Marina, S.R. Das, Ad hoc on-demand multipath distance vector routing, Wireless. Communication. Mob. Comput.6:969-988(2006).
10. L. Abusalah, A. Khokhar, et al., A survey of secure mobile ad hoc routing protocols, IEEE Commun. Surv. Tut. 10 (4) 78–93 (2008).
11. MoutushiSingh,RupayanDas.,ASurveyofDifferetTechniquesforDetection of Wormhole Attack in Wireless Sensor Network.,in IJSER journal (2012).
12. S.Kannan, T.Kalaikumaran, S.Karthik, V.P.Arunachalam,A review on attack prevention methods in manet ,Journal of Modern Mathematics and Statistics 5(1),37-42.
13. Dr.L.S.Jayashree. I.Kala, Survey of Routing Protocols and Attacks for Mobile Adhoc Networks in CIIT Networking and Communication Engineering,Volume 3,No 15(2011).