Enhanced Reliability Enabled Single-Hop Broadcasting in Mobile Ad-hoc Networks

Dr. S.K. Mahendran
Director, Department of Master of Computer Applications,
SVS Institute of Computer Applications,
Coimbatore, Tamil Nadu, India

Abstract -- A dependable unique hop transmission is an essential communication original in mobile ad hoc networks in which a message from the source node is definite to be brought to all nodes within the source node's transmission range. Despite the reputation of it, dependable one hop broadcast is not easy to achieve due to crashes in wireless networks known as Concealed Incurable Problematic. This paper presents a MAC protocol that not only guarantees reliable one hop broadcast but also accomplishes it efficiently by exploring as many simultaneous executions of the communication as possible. In addition to the data packets, the proposed algorithm exploits the control packages that prevent packet crashes, and at the same time, make the simultaneous communications possible to improve the network throughput. Simulation results show the effectiveness of the futureprocedure.

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) contains of a set of wireless mobile hosts (or nodes) that are allowed to move in any instructions at any rapidity. A MANET does not necessitate any preceding fixed substructures, and therefore it can be built on the fly. Subsequently nodes in a MANET [10-14] function on sequences and have limited transmission ranges, reducing needless infrastructures is vital to recover the network life and throughput. Due to the nature of wireless networks, a broadcast in the networks is essentially a onehop broadcast, in which a signal communicated from a node (source node) spreads all nodes within its broadcast range (neighbors of the source node). Numeroussignificant algorithms in MANETs forcefully depend on the presentation of one hop broadcasting. Some significant applications of one hop broadcasting are: Sensitive routing procedures in MANETs. In most sensitive algorithms in MANETs, if the source node does not have route information to the destination node, the source node floods the network with a special control packet, Route Request Packet (REQ) [1-5] , to learn a path to the boundary. This flooding technique is based on one hop communication and endures until the REQ feasts the terminus. Active routing algorithms that are based on Distance Vector Routing or Link State Routing. In applying an active algorithm, every node preserves routing material in its routing table through intermittent exchanges of its information with its neighbors. This exchange is usually done in the form of one hop broadcast. Topology control. By swapping necessary information with its neighbors, a wireless node regulates its broadcast range so that an efficient network topology is maintained for better vigorpreservation and network throughput. Procedures based on graded organization of nodes. Particularly, collection based algorithm needs one hop broadcasting when the nodes are in the procedure of forming groups. After a cluster is formed,the head of the group must transmission it's voting as a gathering head to all protuberances in its cluster using one hop broadcast as well.The procedures designated above work correctly provided that the one hop distribution is reliable, i.e., packet delivery from the source node to all its neighbor nodes is certain. Otherwise, imprecise and/or insufficient information may cause severe squalor of the procedures and therefore result in unwanted results. Although many procedures have been developed that necessitate reliable one hop distribution, thus far not many reliable one hop distribution protocols actually have been proposed.

2. RELATED WORKS

Achieving a dependable one hop transmission in wireless networks is not an easy mission due to the crashes caused by a singularity known as Hidden Terminal Problem. If a broadcast is between two nodes (i.e., point-to-point communication), then RTS – CTS protocol can resolve the problematic eventually [16]. However, point-to-point approach will be extremely inefficient and often useless if it is used for onehop broadcast in MANETs. Additional squalor of network throughput happens when nodes cannot discover possible simultaneous transmissions. An instance of this type is the Unprotected Terminal Problem that prevents two neighbor nodes from effective simultaneous transmissions. Countless communication procedures anticipated thus far are based on the single channel MAC protocols. However, IEEE 802.11 standard for wireless LAN provides multiple channels for communication between nodes in the network. [5-10].

When a node T in a wireless network communicates an indication, the indication spreads all instructions to the detachment usually relative to the broadcastinfluence. The partenclosed by the indicator is estimated by a circle pinpointed at T and is called broadcast range (or broadcast area) and is denoted as XYR. MR T is also used to represent the radius of the area, if there is no possibility of misperception. In this paper, it is assumed that every node has the identical maximum transmission range, and can adjust its transmission range depending on the packet type to be communicated. If a node T communicates a packet type P, then the communication range required for the communication is signified as XYR, P. If T uses its thorough going communication power, it is denoted as XYR, MAX or simply MRMAX.

Suppose node T in is currently transmitting a packet. Also suppose node N wants to communicate a packet as well. If X knows T is communicating, X will not twitch its own broadcast, subsequently it does, and it causes collision at C. Conversely, subsequently node X is not within the communication range of T, X cannot recognize that T is transmitting. Henceforth, X initiates its transmission, which causes collision at node C. This problem is known as the Hidden Terminal Problem. To avoid the Hidden Terminal Problem, RTS–CTS protocol was proposed. In RTS–CTS protocol, a communicating node, says T in, has a data packet to send to C. Then, T sends a control packet called Ready-To-Send (RTS) to C prior to data packet transmission. The RTS contains the source ID (S in this example), the destination ID (D in this example), and the size of the data packet to be sent to node C. On receiving the RTS, C sends a control container called Clear-To-Send (CTS) if it is ready to receive a data packet from T. The CTS also contains the source ID (T), the destination ID (C), and the size of the data packet from T to C. On receiving the CTS, S starts sending the data packet. An interesting feature of RTS–CTS protocol is that the CTS also reach the nodes in C's communication range, for example node X. Therefore, from the information in the CTS, X calculates the duration of the transmission time of data packet from T to C, and does not transmit any packet during the time to avoid crashes. Inappropriately, RTS–CTS are not a perfect solution for the Hidden Terminal Problem. The following two scenarios show the cases when RTS–CTS may not stopsmashes. Park and Palasdeokar [3] have industrialized a dependable one hop broadcasting procedure called ROB that develops only one station for both control packets and data packets. ROB does not require any control packet communication previous to data packet broadcast. When a node T transmits a data packet, if a node in T's communication range detects a crash, the node transmits a NACK control packet representative that it did not receive the packet. Consequently, if T does not receive any NACK or smash, the one hop communication could be regarded as completed. Otherwise, Tendures transmitting the same data packet until it does not receive any NACK or accident. The process is simple but gives rise to new difficulties such as TransmissionComprehensiveProblematic that presents additional difficulty in noticing the completion of one hop communication caused by NACKs. Although interested by and usages comparable vocabulary and perceptions of the procedures in [8–10], the anticipated procedure presents a significant development over the procedures by exploring as many parallel executions of the one hop distribution as possible, which foodstuffs far better presentation in the network amount.

3. PROPOSED WORK

This subdivision benevolences a new one-hop dissemination procedure, entitled Enhanced Reliable Single-Hop Broadcasting that assurances the achievement of Single-Hop distribution, i.e., all nodes in the source's transmission range will receive the broadcast message. Expectations made in this paper are: All nodes have the similar maximum broadcastvariety. Thus, all relations could be bidirectional. All protuberances are capable of regulating their broadcast power, and consequently, their communication ranges. All node apparatuses multiple channels and is accomplished of swapping between them. Nodes obtain correct data, except there is a collision. Allnodesknow its position and its poignant speed using putting devices such as GPS. Poignanthustles of nodes are moderate; otherwise, no procedure would work. Each node is accomplished of applying CSMA/CA.

Enhanced Reliable Single-Hop broadcasting usages the basic notation, definition and implementation similar to that of GOB , as designated below. Two types of packets are used in Enhanced Reliable Single-Hop Broadcasting: control packages and data packets. Data packets contain the data to be Single-Hop transmission, and regulator packets are used to improve the efficiency of the data packet communication. Although control containers may not be essential, the network throughput is usually advanced with them due to their control over packet crashes. For example, using RTS and CTS control packets may harvest higher network amount. Enhanced Reliable Single-Hop Broadcasting uses only a solitary type of controller packet called Broadcast-In-Progress to prevent collisions for achieving steadfast Single-Hop broadcast. A Broadcast-In-Progress is produced and used in two cases. Prior to Single-Hop broadcast of a data packet, the node transmits a BIP to secure not only the broadcast area but also broadcast threatening area as well to avoid possible smashes. On receiving a BIP, a node that is currently involved in any other communication generates and communicates a BIP to warn other nodes in its broadcast threatening area not to initiate data package communication.

Node in T's communication collection is presently difficult in data packet communication. Suppose there is a node, for example, C in T's communication range that is complicated in data packet transmission. Then, C prepares and transmits a BIP to warn T not to transmit data packet, since if T does, it would cause data packet collision at C. If there are two or more nodes that are involved in data transmission in S's transmission range, for example, C and D in, they all transmit BIPs to warn T. In this case, although T would hear a garbled message (i.e., garbled BIPs) that is not possible to decode correctly, T interprets the situation correctly and not to transmit data packet. Node in T's transmission range is currently involved in control packet transmission.While BIPs are very advantageous, they also may cause a thoughtful problem, called BIP Dissemination Problem, similar to Signal Propagation Problem.This observation had led us to develop the following data crash escaping scheme that guarantees the accomplishment of Single-Hop circulation even in the presence of node flexibility.

Suppose nodes X and T just started communicating data packages while moving near each other with the speed of SPEEDX and SPEEDC, respectively. Also, let TIMEX and TIMEC be the data packet transmission time of X and C, respectively. Note that this information is concealed from each other, since they even do not know the being of each additional. Our method to avoid the possible crash is to give enough coldness in advance between XYX, DATA and XYC, DATA so that they would not intersection during the data broadcast. That is, if the coldness between X and C is greater than SPEEDX TIMEX + SPEEDC TIMEC when they start communicating data packets, there would be no accident. Since we may not be able to regulator the mobility of nodes, the only way to secure the distance to prevent the collision would be adjusting the transmission range. Therefore, if C reduces its transmission range XYS, DATA by DS = SPEEDC TIMEC, data packet accident could be avoided from X's side. However, since both X and C are touching towards each other in the nastiest case, Xshould also reduce its transmission range XYS, DATA by DS = SPEEDS TIMES. Then, there will be no data packet crash, unless either SPEEDS or SPEEDXupsurges.

4. RESULTS AND DISCUSSION

The proposed protocol ERESHB is simulated with NS2 simulator with the below settings and also compared with the AODV, DSDV, DSR and MAODV in homogeneous and heterogeneous environment with the performance metric throughput. Results show that ERESHB outperforms better in all the aspects than the other protocol. The settings used for the simulation are as below:

No. of Nodes	50
Terrain Size	100 (in meters)
MAC	802.11b
Radio Transmission Range	150 meters
Simulation Time	100 seconds
Traffic Source	CBR (Constant Bit Rate)
Packet Size	128 Kbits
Mobility Model	Random Waypoint Model
Initial Energy	1 to 3 Joules
Speed	2.5 m/s
Environment	Homogeneous, Heterogeneous

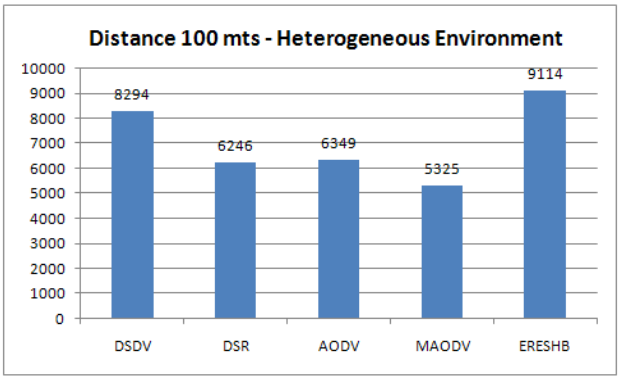

Fig.1. Distance Vs Throughput in heterogeneous environment

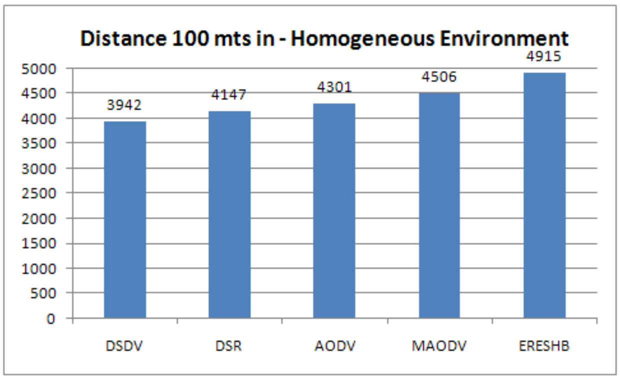

Fig.2. Distance Vs Throughput in homogeneous environment

5. CONCLUSION

Single-Hop transmission is an important communication embryonic in which the foundation node transports its package to all nodes within its communication range. Single-Hop transmission is very useful homogeneous and heterogeneous networks, particularly in wireless networks where every communication is a single-hop transmission by nature. Notwithstanding the reputation of it, it is hard to complete in wireless networks due to the accidents caused by Hidden Terminal Problem.This paper presents an procedure, called Enhanced Reliable Single-Hop Broadcast, that assurances the completion of Single-Hop transmission in wireless mobile ad hoc networks. In addition to data packages, ERESHB uses a single type of control packets, Broadcast-In-Progress (BIP), to prevent crashes. Alternative exceptional feature of ERESHB is to allow each node to adjust its transmission range so that as many simultaneous Single-Hop broadcasts are discovered as possible to enhance the network throughput and reliability. Other compensations obtained from the modification of communication ranges include power saving due to smaller communication range, less number of smashes, and longer network lifetime

Reference

[1] J. Lembke, Z. Ryne, H. Li, S. Park, Collision Avoidance in One-Hop Broadcasting for Mobile Ad-hoc Networks, in: IASTED International Conference on Communication, Internet, and Information Technology, 2005, pp. 308–313.
[2] Z. Tang, J.J. Garcia-Luna-Aceves, Hop-Reservation Multiple Access (HRMA) for ad hoc networks, in: Proc. of IEEE INFOCOM, 1999.
[3] S. Park, R. Palasdeokar, Reliable One-Hop Broadcasting (ROB) in mobile ad hoc networks, in: 2nd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN '05), 2005, pp. 234–237.
[4] M. Mohsin, D. Cavin, Y. Sasson, R. Prakash, A. Schiper, Reliable broadcast in wireless mobile ad hoc networks, in: Proc. of 39th Hawaii International Conference on System Science, 2006.
[5] A. Tzamaloukas, J.J. Garcia-Luna-Aceves, A receiver-initiated collision-avoidance protocol for multi-channel networks, in: Proc. of IEEE INFOCOM, 2001.
[6] J. Deng, Z. Haas, Dual Busy Tone Multiple Access (DBTMA): a new medium access control for packet radio networks, in: Proc. of IEEE ICUPC, 1998.
[7] IEEE 802.11 Working Group, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1997.
[8] V. Bharghavan, et al., MACAW: a media access protocol for wireless LAN's, in: Proc. ACM SIGCOMM, 1994.
[9] D. Allen, Hidden terminal problems in wireless LAN's, IEEE 802.11 Working Group Paper 802.11/93-96.
[10] P. Karn, MACA – a new channel access method for packet radio, in: ARRL/CRRL Amateur Radio 9th Computer Networking Conference, September 22, 1990.
[11] H. Lim, C. Kim, Multicast tree construction and flooding in wireless ad hoc networks, in: Proceedings of the Third ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), August 2000.
[12] J. Haas, A new routing protocol for the reconfigurable wireless networks, in: Proc. of IEEE 6th International Conference on Universal Personal Communications, vol. 97, 1997, pp. 562–566.
[13] P.-J. Wan, K.M. Alzoubi, O. Frieder, Distributed construction on connected dominating set in wireless ad hoc networks, Mobile Networks and Applications 9 (2) (2004) 141–149.
[14] Y. Li, M.T. Thai, F. Wang, C.-W. Yi, P.-J. Wan, D.-Z. Du, On greedy construction of connected dominating sets in wireless networks, Wireless Communications and Mobile Computing (WCMC) 5 (8) (2005) 927–932.
[15] Jie Wu, Fei Dai, Broadcasting in ad hoc networks based on self- pruning, in: INFOCOM, 2003.
[16] S. Park, R. Anderson, Guaranteed one-hop broadcasting in mobile ad- hoc networks. in: The 2008 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'08), July 14–17, 2008.

