Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 19 (2013) 1068 – 1073

Procedia Computer Science

The 8th International Symposium on Intelligent Systems Techniques for Ad hoc and Wireless Sensor Networks (IST-AWSN)

Maintaining Path Stability with Node Failure in Mobile Ad Hoc Networks

Abedalmotaleb Zadin and Thomas Fevens[1]

Department of Computer Science and Software Engineering
Concordia University, Montréal, Québec, Canada

Abstract

As the demand for mobile ad hoc wireless network (MANET) applications grows, so does their use for many important services where reliability and stability of the communication paths are of great importance. Therefore, a MANET must be able to establish reliable communication channels which are protected by failure recovery protocols. One approach for existing failure recovery protocols is based on using backup paths, or multi-paths. This technique provides for more stable communication channels for wireless services, in particular for MANET applications. But work on such multi-path protocols has focused on stability in the presence of link failure for MANETs. In this paper, we extend such protocols to maintain connection stability in the presence of node failure. Our work is focused on protecting the route of mobile wireless communications in the presence of node failure in order to improve their use in MANETs applications by discovering efficient stable communication channels with longer lifetimes and increased number of packets delivered.

Selection and peer-review under responsibility of Elhadi M. Shakshuki

Keywords: Mobile Ad Hoc Networks, Path Stability, Node Protection

1. Introduction

Wireless networks are formed with interconnecting devices communicating wirelessly within a relatively limited area. Mobile ad hoc networks (MANETs) are a type of wireless network where mobile devices are themselves responsible for communicating with each other without the presence of a centralized infrastructure. Devices in MANETs can typically move in any direction they want and therefore links between them and other devices may frequently change such that the topology of a MANET can be very dynamic [1]. Each device in a MANET is not only responsible for network traffic related to itself but also has to forward unrelated traffic as an intermediary. A crucial problem in multi-hop routing in MANETs is finding an efficient and correct route between a source and a destination, due to the dynamic nature of the network topology in MANETs. One of the important traits of a reliable system is the stability of the connection between a pair of wireless nodes interested in communicating.

[1] Corresponding author: fevens@cse.concordia.ca

Selection and peer-review under responsibility of Elhadi M. Shakshuki
doi:10.1016/j.procs.2013.06.150

To increase the stability of routing in MANETs and provides a reliable end-to-end route one approach would be for each node to choose the most stable route from its options [2]. For example, Wang *et al.* [3] discover a trusted route among friendly nodes by routing considering communication reliability and path length. Song *et al.* [4] propose a routing scheme that chooses between different routing protocols based on estimated link stability. Alternatively, to improve the stability along the path in the presence of expiring links, where neighboring nodes along a path may move out of transmission range, another approach is to maintain multiple paths along the connection. In particular, a reliable connection could be achieved by protecting the links between each pair of nodes participating in the primary path by maintaining local backup paths in parallel with each link in the path to be used when that link expires. Yang *et al.* [5] achieve a reliable connection by protecting the links between each pair of nodes participating in the primary path by maintaining local backup paths in parallel with each link in the path to be used when that link expires. We study, in particular, the latter approach using multi-paths.

In additional to link expiry, another major reason for a connection to break down is when an intermediate node or destination node becomes unreachable. The node can become unreachable due to several reasons such as running out of energy, node failure, or when a node becomes unresponsive. To the best of our knowledge, there has been no stability routing algorithms for MANETs that include both node protection, to ensure the connection is not broken when a node fails, and link protection, ensuring the connection is not broken when a link fails. In this paper, we introduce a combined node and link protection protocol to establish improved stable connections in terms of path stability, packet delivery rate, and connection throughput.

The rest of this paper is organized as follows. Section 2 gives an overview of the routing protocol in MANETs. In Section 3, we will give a brief description about multi-path route discovery in MANETs. In Section 4, we propose our connection survival schemes. Experimental results are given in Section 5. Finally, concluding remarks are made in Section 6.

2. Routing in MANETs

Routing is the process of path selection on which network traffic is send. To be able to define how connections between communicating nodes are established in MANETs, we first define our network model of a MANET and discuss how routes are determined in this model.

2.1. *Network Model of MANETs*

MANETs can be modeled using a graph $G = (V, E)$ where V represents the set of nodes/vertices, and E represents the set of links/edges. Each node in the MANET will have a unique identifier and know its geographic position. In the real world, we will assume that the location of the nodes in a MANET will be tracked using Global Positioning System (GPS) and/or Location Services (LS) [7, 5]. We will assume the nodes are arranged in a two dimensional $2D$ Euclidean space such that G is a geometric graph. Each edge in G represents a link between two neighboring nodes within the transmission range which we will assume, for this paper, to be the same for all nodes. Two nodes are considered to be neighbors if they are within the transmission range of each other and an edge exists between them. We will denote the neighbors of a node v_i by $N(v_i)$. A path of length n between a source node S and a destination node D is denoted by $(S = v_0, v_1, v_2, \ldots, v_n = D)$ where $v_i \in V$ and $v_i \in N(v_{i-1})$. A path which is used as the first choice while transmitting from source to destination is called a primary path, denoted as P_p.

2.2. *Position Based Routing*

In position-based routing each network node is informed about its position, its neighbors' positions, and position of the destination. In the design of ad hoc networks the development of dynamic routing protocols that can efficiently find routes between two communicating nodes is of paramount of importance, in order to build a stable path. In this paper, to discover a route from source node S to destination D, the position-based local routing algorithm GPSR [8] is used. GPSR is a greedy algorithm in which the current node, starting from S, determines the next node on the route based on its position, the position of its one-hop neighbors, and the position of the destination. While constructing the route, the current node looks among its neighbors for the node which is closest to the destination as its next hop. If no neighbor is closer to the destination than the current node, the routing protocol switches to perimeter forwarding, traversing the face of a planar sub-graph using the right-hand rule until it recovers from the local maxima, and the greedy algorithm can continue, terminating at the destination node if it is reachable.

3. Multi-Path Route Discovery Protocol for Link Protection in MANETs

The basic multi-path route discovery protocol we describe in this section was originally presented by Yang *et al.* [5]. The protocol presented by Yang *et al.* is called the Greedy-based Backup Routing Protocol (GBR). First a path is discovered from the source node S to the destination D using GPSR as described above. The path discovered is termed the primary path. We also need to determine the backup paths that provide link protection for the links of the primary path. Since these backup paths have to survive after the link expires we need to know the lifetimes of both individual links and paths as a whole. Following [5], we denote these lifetimes, respectively, as Link Expiration Time $LET(v_i,v_{i+1})$ for the link v_iv_{i+1}, and Path Expiration Time $PET(P)$ for a path P. $LET(v_{i-1}, v_i)$ is defined as

$$LET(v_{i-1}, v_i) = \frac{-(pl + qd) + \sqrt{(p^2 + q^2)R^2 - (pd - lq)^2}}{p^2 + q^2} \tag{1}$$

where $p = \tau_{i-1} \sin\theta_{i-1} - \tau_i \sin\theta_i$, $q = \tau_{i-1} \cos\theta_i - \tau_i \cos\theta_i$, $l = X_{i-1} - X_i$, $d = Y_{i-1} - Y_i$, and (X_i, Y_i) are the node coordinates, τ_{i-1} and τ_i are the node velocities, θ_{i-1} and θ_i are the direction angles, and R is the transmission range. All nodes maintain a neighbor table, which stores the ID and position of each neighbor; a primary path table, which stores primary path information for a destination node; a backup path table, which stores local-backup path information for the links in the primary path; a Route Request (RREQ) table, which stores information about all received RREQs; and a data cache. As part of the protocol, at regular intervals, all nodes send HELLO messages containing their ID and position information to their neighbors.

During the primary route discovery, each node v_i in the discovered route, $P_p = (S = v_0, v_1, v_2, \ldots, v_n = D)$, unicasts an RREQ to D message to its neighbors, starting from S. The RREQ contains the IDs and positions of v_i and D, the velocity of v_i, and $LET(v_{i-1}, v_i)$. Each node v in $N(v_i)$ adds the RREQ to its RREQ table, and each v except v_{i-1} and v_{i+1} starts back-up path determination and discards the RREQ. The neighbor v_{i+1} calculates $LET(v_i,v_{i+1})$ and adds the reverse path to its primary path table. If v_{i+1} is not the destination, it adds the $LET(v_i, v_{i+1})$ and its velocity and position information to the RREQ message, whereupon it continues the primary route discovery by unicasting the RREQ. When the RREQ is received by the destination, it will send back the Route Reply Message (RREP) back through the reverse route in the RREQ. And when the source S and the intermediary nodes receives this RREP they set up the primary path to destination D according to the RREP. Once finished, S will start to transmit to the destination D.

When a neighborhood node m not on the primary path saves the RREQ, it starts calculation for the backup path [5, 9, 10] for a link using the calculation for PET given in Equation 2.

$$PET(v_i, m, v_{i+1}) = \min(LET(v_i, m), LET(m, v_{i+1})) \tag{2}$$

where m is a neighboring node to both v_i and v_{i+1}. To determine which m to use for the backup path, Yang *et al.* [5] use contention-based scheme using a heuristic to try to find the m creating a backup path with the overall largest PET. We will consider that the link between v_i and v_{i+1} has no backup path if we did not find a neighbor node which satisfies the above conditions.

4. Connection Survival Scheme Based on Node Protection

In this section we introduce a multi-path routing protocol that aims to handle both link expiration and nodes that become unresponsive in MANETs. Our protocol deals with mobility, break-down of wireless links and also the disappearances and reappearances of nodes. By adapting previous work for link protection, we introduce a node protection scheme for the route survival in MANETs can be considered also effective for link protection.

4.1. *Node Protection vs. Link Protection*

Furthering the work in [5, 11], we propose to improve the efficiency (in terms of network throughput) and overall communication stability of the routing by protecting intermediate nodes of the path instead of just the links between two neighboring nodes. Most previous research have considered both route length and/or link lifetime to achieve a high route stability by protecting the links between each pair during the communication [12]. However, the problem with this approach is when a node in the primary path fails or becomes unresponsive it will cause both primary and backup paths to break as in Figure 1. This will result in the recalculation of the entire path from the source to the destination, causing significant interruption, which is highly undesirable in critical systems. In contrast, with a multi-path node protection approach, even if the node on the primary path is unreachable, we will be able to utilize the backup path. Since our research is focused on increasing the communication reliability and path stability of MANETs, we study a multi-path approach to node protection as shown in Figure 2 in order to improve the ad hoc networks efficiency, which in turn will lead to higher throughput. Here, each node in the primary path can be bypassed in the event of failure by a backup path independent of this node between the previous and following nodes on the primary path. Thus, protecting the nodes instead of, or in complement to, protecting the links the result avoids the need to recalculate the complete path due to node failure during communication.

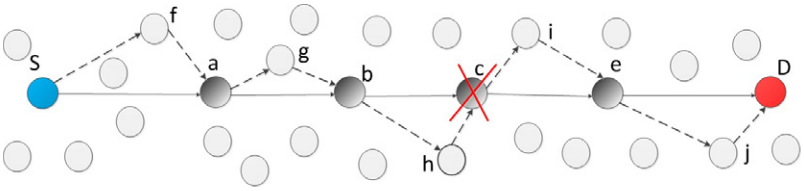

Fig. 1. An example of link protection.

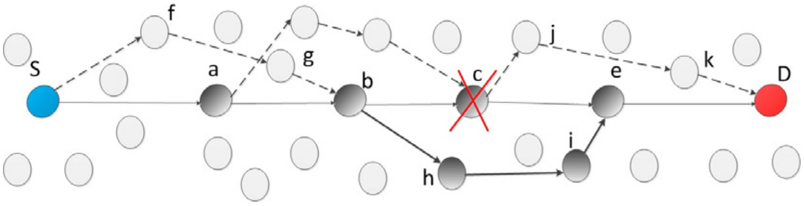

Fig. 2. An example of node protection.

4.2. *Node Protection Algorithm*

To determine the backup paths for node protection, we do the following. First, the primary path is determined as described above for GBR. During the transmission of the RREP back to S, when an intermediary node v_i, or S, receives this RREP, it computes a node protection backup path P_b for v_{i+1} from v_i to v_{i+2} using only links between nodes in P_b with LET greater than $PET(v_i, v_{i+1}, v_{i+2})$ while ignoring the node v_{i+1}. We will consider that the node v_{i+1} has no node protection backup path if we can not find a path P_b from v_i to v_{i+2} which is satisfies the condition of $PET(P_b) > PET(v_i, v_{i+1}, v_{i+2})$. We will call this protocol based on GBR but using node protection (NP) rather than link protection as GBR-NP.

5. Experiments and Results

This section presents simulation results for node protection that show how well it performs on a MANET with mobile node in the presence of node failure. Specifically, we compare GBR-NP with the original GBR. The performance metrics that we are interested in are packet delivery ratio, and total number of packets delivered.

5.1. Experiments and Simulation Environment

For both algorithms GBR and GBR-NP, we constructed both the primary path and the backup path as described in Section 3. The simulation environment is modeled using network parameters that are a network area of size $2200m \times 2200m$; a varying number of nodes from $200, 250, 300, \ldots, 600$; a fixed transmission range of $R = 250m$. Each simulation ran for 600 seconds with enough packets assigned for the simulation time. There are 20 pairs of Constant Bit Rate (CBR) data flows in the network layer, and non-identical source and destination flows were randomly selected, each flow did not change its source and destination throughout the simulations. The direction in which a node can move is given randomly at the beginning of the simulation. However, when a node reaches the boundary, we reflect the node off the boundary using the formula $\alpha + \pi/2 + C$ [13]. For each different node density, randomly distributed 40 connected graphs were used as a starting network topology for each run of the simulation for all algorithms. This is done to get average performance results for better analysis. The velocity was chosen to be the same for all nodes at $V = 10$, and the HELLO beacon interval was set to 2 seconds.

In order to simulate recovery of node protection path when a primary path is broken, we switch off randomly a total of two nodes, each on a different path from the total of the twenty different (although not necessarily disjoint) paths. In link protection technique when the primary path is broken because one of the nodes participating in the path becomes unreachable the backup path will not be useful. A message will be sent back to the source and the source will recalculate the path again to the destination. However in node protection technique, when the primary path is broken because of one of the nodes participating in the path becomes unreachable so the last reachable node will locally use the backup path that will cover the unreachable node thus saving the overhead of recalculating the whole path again.

5.2. Results

This section shows the performance of the GBR-NP in comparison with GBR. In particular, due to space limitations, we will show only the experiments regarding the effective of varying node density. The performance metrics that we are interested in are the total packets delivered over the simulation and packet delivery ratio (PDR), which is calculated as $PDR = \#P_d/\#P_s$ where $\#P_d$ is the total number of packets delivered during the simulation, and $\#P_s$ is the total packets sent during the simulation. The error bars in each graph represent 95% confidence intervals.

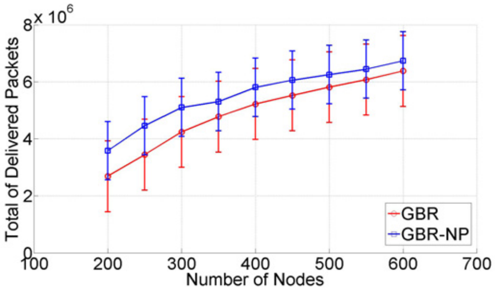

Fig. 3. A Total of Packets Delivered

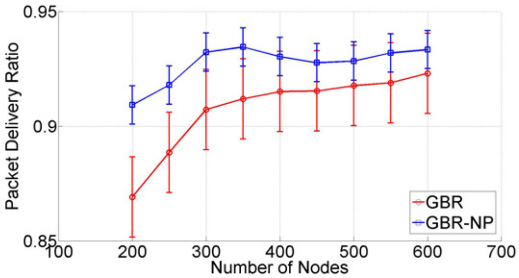

Fig. 4. A Packet Delivery Ratio

Figures 3 and 4 show the performance of the node protection protocol GBR-NP in comparison to link protection protocol GBR. The mobility of nodes causes randomness in the topology because a node can appear and disappear from transmission range without following any specific pattern which causes links between nodes to appear and disappear, then the advantage of our proposed algorithm GBR-NP scheme is apparent. In terms of total number of packets delivered, the results in Figure 3 indicate that the accuracy by protecting the link between two nodes is not as good as that of protecting the node between two nodes in terms of total packet delivered. This result leads to a fact that the node protection policy can achieve better bandwidth efficiency than the link protection policy even with nodes are mobile. In terms of the Packet Delivery Ratio (PDR), however, from Figure 4 we can observe that the total number of packets delivered with the link protection protocol is less than the PDR for the node protection protocol under the same network environments. Experimental results in both Figures 3 and 4 indicate that the presented approach of combining node and link protection shows much greater overall throughput efficiency in MANETs when the nodes are mobile and occasionally failing.

6. Conclusions

We have presented a node protection protocol, which allows for the establishment of stable connections in MANETs which experience occasional node failure. The proposed protocol was tested with simulations of model of mobility networks where mobile users with time variant locations and velocities which affect the communication reliability in MANETs, which we show leads to high network stability as well as a high packet delivery rate. The protocol was validated and compared against the a link protection protocol as implemented by the GBR protocol showing a significant improvement in number of packets delivered and delivery rate when nodes may occasionally fail. The advantage of GBR-NP is particularly noticeable for the graphs with fewer nodes. Hence, the presented node protection protocol can be used to improve the communication stability in MANETs under increasingly realistic conditions of node movement and occasional failure.

References

[1] B. Ishibashi, R. Boutaba, Topology and mobility considerations in mobile ad hoc networks, Ad Hoc Networks 3 (6) (2005) 762 – 776. doi:10.1016/j.adhoc.2004.03.013.
URL `http://www.sciencedirect.com/science/article/pii/S1570870504000289`

[2] R. Marie, M. Molnár, H. Idoudi, A simple automata based model for stable routing in dynamic ad hoc networks, in: 2nd Workshop on Performance Monitoring & Measurement of Heterogeneous Wireless & Wired Networks, 2007, pp. 72–79.

[3] J. Wang, Y. Liu, Y. Jiao, Building a trusted route in a mobile ad hoc network considering communication reliability and path length, Journal of Network and Computer Applications 34 (4) (2011) 1138 – 1149, ¡ce:title¿Advanced Topics in Cloud Computing¡/ce:title¿. doi:10.1016/j.jnca.2010.11.007.
URL `http://www.sciencedirect.com/science/article/pii/S1084804510002055`

[4] Q. Song, Z. Ning, S. Wang, A. Jamalipour, Link stability estimation based on link connectivity changes in mobile ad-hoc networks, Journal of Network and Computer Applications 35 (6) (2012) 2051 – 2058. doi:10.1016/j.jnca.2012.08.004.
URL `http://www.sciencedirect.com/science/article/pii/S1084804512001804`

[5] W. Yang, X. Yang, S. Yang, D. Yang, A greedy-based stable multi-path routing protocol in mobile ad hoc networks, Ad Hoc Networks 9 (2011) 662–674.

[6] L. Guo, L. Zhang, Y. Peng, J. Wu, X. Zhang, W. Hou, J. Zhao, Multi-path routing in spatial wireless ad hoc networks, Computers & Electrical Engineering 38 (3) (2012) 473 – 491, ¡ce:title¿The Design and Analysis of Wireless Systems and Emerging Computing Architectures and Systems¡/ce:title¿. doi:10.1016/j.compeleceng.2011.11.013.
URL `http://www.sciencedirect.com/science/article/pii/S0045790611001893`

[7] L. Barriére, P. Fraigniaud, L. Narayanan, Robust position-based routing in wireless ad hoc networks with unstable transmission ranges, in: 5th Inter'l Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, ACM, 2001, pp. 19–27.

[8] B. Karp, H. Kung, GPSR: Greedy perimeter stateless routing for wireless networks, in: 6th Annual International Conference on Mobile Computing and Networking (MOBICOM), ACM, 2000, pp. 243–254.

[9] Z. Wu, X. Dong, L. Cui, Ant-based stable multipath routing algorithm in mobile ad hoc networks, in: Third International Conference on Natural Computation, Vol. 4, IEEE, 2007, pp. 683–687.

[10] N. Wang, J. Chen, A stable on-demand routing protocol for mobile ad hoc networks with weight-based strategy, in: 7th Inter. Conf. on Parallel & Dist. Comp., 2006, pp. 166–169.

[11] L. Xi, J. Hong, F. Yu, Z. Ruiming, A fcm-based peer grouping scheme for node failure recovery in wireless p2p file sharing, in: International Conference on Communications, 2009, pp. 1–5.

[12] W. Grover, D. Onguetou, A new approach to node-failure protection with span-protecting p-cycles, in: 11th International Conference on Transparent Optical Networks, 2009, pp. 1–5.

[13] B. Pazand, C. McDonald, A critique of mobility models for wireless network simulation, in: Inter. Conf. on Computer and Information Science, 2007, pp. 141–146.