Journal of Southeast University (English Edition) Vol. 23, No. 1, pp. 16 – 21 Mar. 2007 ISSN 1003—7985

Improved approach to enhanced Internet connectivity for mobile ad hoc networks

Shen Bin[1] Li Bo[2] Shi Bingxin[1]

([1] Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, China)
([2] School of Information Science and Engineering, Yunnan University, Kunming 650091, China)

Abstract: An improved internetworking approach is proposed to enhance the Internet connectivity which is deteriorated due to unidirectional links and blind rebroadcasting of gateway discovery packets for mobile ad hoc networks. The hybrid gateway discovery scheme that combined the advantages of a proactive and reactive gateway discovery approach is used to achieve high connectivity while keeping overhead costs low. By exchanging ad hoc on-demand distance vector (AODV) hello packet which includes additional fields named symmetric neighbor list and asymmetric neighbor list, unidirectional links are removed from route computation and broadcast storm can also be relieved simultaneously. Performance results using ns-2 simulations, under varying numbers of unidirectional links and node speeds, show that this improved Internet connectivity approach can provide better performance than others.

Key words: mobile ad hoc networks; Internet connectivity; gateway discovery; unidirectional link; broadcast storm

The internetworking of Internet and mobile ad hoc networks (MANETs) can be used to eliminate dead zones in wireless networks and enrich the application range of ad hoc networks. The challenge in such hybrid ad hoc networks stems from the need to inform MANET nodes (MNs) about available gateways in an extremely changing scenario while making a minimal consumption of the scarce network resources. So, an efficient gateway discovery approach for MANET becomes one of the key elements to enable the use of hybrid ad hoc networks in future mobile and wireless networks.

Several schemes to enhance ad hoc routing protocols to support an MN accessing Internet have been developed in the literature up to now. However, each of them is only suited for a limited range of network conditions and the performance can vary dramatically as the network conditions change[1]. The proactive approaches[2] are based on the periodic flooding of gateway advertisement messages (GWADVs), allowing MNs to create routes to Internet in an unsolicited manner. Although achieving good connectivity, proactive solutions heavily increase the gateway discovery overhead because the GWADVs are sent to the whole MANET every now and then. In reactive approaches[3], those nodes that require Internet connectivity proactively find Internet gateways by means of broadcasting some kind of gateway solicitation messages (GWSOLs) within the entire MANET. When these requests are received by a gateway, then it sends a GWADV which creates reverse routes to the gateway on its way back to the originator. Although reactive approaches tie the overhead of maintaining connectivity to external traffic patterns, their on-demand nature results in larger packet delay and poor scalability regarding the number of active sources willing to access Internet.

All the existing schemes rely on a broadcast routing mechanism to provide MNs with a multi-hop path to gateways and a common approach is to broadcast by flooding. In such schemes, GWADVs or (and) GWSOLs should be flooded to make MNs find available gateways. Within ad hoc clusters, most routing protocols (e. g., AODV[4]) also have relied on the same mechanism to maintain local connectivity. Although straightforward and direct, nodes rebroadcast their first heard broadcast packets blindly which may result in broadcast storm problem due to excessive redundancy, contention, and collision[5]. For example, in Fig. 1, node E, B and F should not rebroadcast their first heard GWADV packets because their rebroadcasting cannot provide additional coverage to GWADVs.

In the procedure of global and local route computation, existing gateway discovery approaches and most ad hoc routing protocols rely on the assumption that all

Received 2006-06-15.
Foundation item: The National Natural Science Foundation of China (No. 60362001).
Biographies: Shen Bin (1973—), male, doctor, lecturer, shenbinghust@hotmail.com; Shi Bingxin (1936—), male, professor.

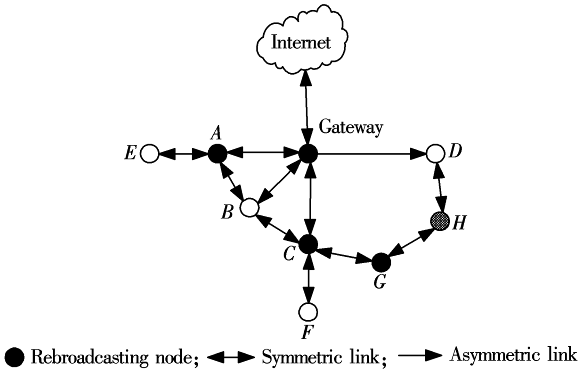

Fig. 1 Internetworking MANET with Internet containing asymmetric links

network links are symmetric (i. e. bidirectional). However, the asymmetric (i. e. unidirectional) links caused for many different reasons, such as in radio transceiver capabilities of nodes and wireless channel interference experienced by different nodes, can be quite common. If no additional protocol actions are taken to remove unidirectional links from route computations, the performance of hybrid ad hoc networks will be affected negatively. For example, due to the unidirectional link between the gateway and node *D* in Fig. 1, the reverse path set up by node *D* as a response to receiving GWADVs originated by the gateway is not valid. And data packets along such global routes would never arrive at the gateway. Furthermore, if node *H* received the GWADVs rebroadcast by node *D*, it would draw the conclusion that there was a 2-hop path to the gateway and so, 3-hop global route via node *G* would be refused to setup. As a result of broadcasting without taking unidirectional link into consideration, *H* loses the last chance to access Internet.

The contribution of this work is the design and evaluation of an improved hybrid internetworking approach with mechanisms to enhance Internet connectivity for MANET. First, the hybrid gateway discovery approach is used to provide good connectivity while keeping the overhead costs low. Secondly, by exchanging hello packets extended with additional fields, unidirectional links are removed from route computations and redundant rebroadcasting of route control packets are inhibited simultaneously in the procedure of gateway discovering. Performance results using ns-2 simulations show that this enhanced internetworking approach can provide better performance than others.

1 Protocol Design

The AODV protocol is modified to route packets not only within ad hoc clusters but also between MANETs and wired networks. Each MN is configured with a global effective IP address and offers connectivity information by broadcasting local hello packets which include all nodes from which it can hear hello packets, i. e., its set of neighbors periodically. Such neighbors are classified under two subclasses, i. e., symmetric neighbors and asymmetric neighbors. Correspondingly, the AODV hello packets are extended with two new fields named symmetric neighbor list and asymmetric neighbor list to include such two kinds of neighbors respectively.

1.1 Data structure

1.1.1 Neighbor node list

Each MN, say *x*, maintains a neighbor node list (NNL) to store its local connectivity information. When *x* receives a hello packet originated by another node, say *h*, it creates an entry for *h* in its NNL and inserts the IP address of *h* (If this entry has existed before, it will be updated). Associated with the entry for *h* is a Symmetric_Link, a Share_Neighbor and a Lifetime. Symmetric_Link field indicates whether the wireless link between *x* and *h* is symmetric. If this link is symmetric, node *x* defines node *h* as its symmetric neighbor; otherwise, as its asymmetric neighbor. If *x* learns *h* is one of its symmetric neighbors, Share_Neighbor field will be set to indicate whether *x* has different symmetric neighbors from *h*. Finally, the Lifetime represents the minimum frequency required for *x* to receive hello packets from *h*. In terms of set, *x* maintains its set of neighbors, denoted by N_x, in its NNL. And according to whether the link between *x* and its neighbor is symmetric, N_x is divided into two subsets, denoted by N_x^a and N_x^s, respectively, where N_x^a is the set of asymmetric neighbors and N_x^s is the set of symmetric neighbors.

1.1.2 Broadcast ID cache

Every MN maintains a broadcast ID and increases it by 1 when this node originates a broadcast packet. To avoid duplicate broadcast packets, every broadcast packet includes its originator's last broadcast ID and every node also remembers the last known IP address as well as the broadcast ID of the originator from which a broadcast packet has been received. When an MN receives a broadcast packet, it first checks to determine whether it has already received such a packet with the same originator IP address and broadcast ID. MN will discard the newly received broadcast packets if it finds that such a broadcast packet has already been received.

1.2 Gateway discovery and transmission of packets

In order to provide MNs with access to Internet, special nodes with both wired and wireless interfaces are configured to track and forward data to and from the MANET. To start an Internet connection, in the first step, gateways have to be discovered by MNs. To minimize the disadvantages of proactive and reactive gateway discovery, the two approaches are combined and result in a hybrid method for gateway discovery. According to this method, gateways are responsible for disseminating GWADVs to advertise their presence in the MANET periodically. However, the time-to-live (TTL) of those GWADVs is limited and so the periodical GWADVs are not flooded throughout the whole MANET but only sent to MNs that are in the vicinity of gateways[6]. Upon receipt of the GWADV, MNs that do not have global routes create reverse route entries for gateways and maintain such routes as default entries in their routing tables. MNs that already have a global route update their route entry for the gateway. On the other hand, MNs that are further away will have to additionally search for available gateways by issuing a request message named RREQ_I if they require global connectivity. When a gateway receives this RREQ_I, it unicasts a GWADV which creates reverse routes to the gateway on its way back to the originator. Note that both GWADV and RREQ_I are two newly introduced control messages. GWADV contains the IP address and broadcast ID of its originator and RREQ_I is identical to AODV RREQ messages[4] except for an additional flag (named I-flag).

Using the global route, source nodes relay their out-going data packets to gateways. The latter then route them to the destinations according to normal IP routing mechanisms. If source nodes find more than one gateway that can provide Internet service, MIPMANET cell switching[2] is applied for gateway selection and switching.

1.3 Acquiring local topology information

Because every MN offers its local topology information by broadcasting hello packets periodically, through receiving such packets, each MN, say x, can set up and update its set of neighbors N_x. Based on the sets included in every hello packet, unidirectional links can be discovered. For example, if x finds itself in the hello packet from another node, say h, it sets the Symmetric_Link about h in its NNL to mark the link from h as symmetric and h is one of its symmetric neighbors. Otherwise, h is marked as an asymmetric neighbor by x in its NNL. However, for relieving broadcast storm simultaneously, more accurate neighborhood information is needed, so each MN h divides its set of neighbors included in hello packets into two subsets, i. e., N_h^a and N_h^s, where N_h^a is included in the asymmetric neighbors list field and N_h^s is included in the symmetric neighbors list filed. Upon receipt the hello packets originated by h, N_h^a and N_h^s can be learned by x. In fact, if x finds $x \in N_h$, it will further subtract N_h^s and $\{h\}$ from N_x^s to learn whether $T = N_x^s - N_h^s - \{h\}$ is an empty set. If $T \neq \emptyset$, that means x has at least one different symmetric neighbor that not owned by h, the Share_Neighbor field of h will be set by x in its NNL.

1.4 Removing asymmetric links and relieving broadcast storm

Because the set of asymmetric neighbors at each node, say x, has indicated the set of nodes from which it has unidirectional links, later when x receives a route discovery packet (e. g., GWADV, RREQ_I, RREQ, and RREP) from one of the nodes in its N_x^a, it discards the route discovery packet to avoid forming a reverse path with a unidirectional link. For example, in Fig. 1, node D will add the gateway in N_D^a because it does not find itself in the hello packet originated by the gateway. Later when node D receives a GWADV from the gateway, it discards the GWADV to avoid forming a reverse path to the gateway with a unidirectional link. This creates a chance for a GWADV from an alternate path (e. g., via H in Fig. 1).

The basic idea of using hello packets to relieve broadcast storm is as follows. Node x will be allowed to rebroadcast a broadcast packet from h only if it believes that there exists at least one symmetric neighbor which may not have received the packet yet. In other words, unless the Share_Neighbor field of h in x' s NNL has been set, broadcast packets from h will never be rebroadcast by x. More formally, each node runs the following steps:

Step 1 Upon node x receiving a broadcast packet P from one of its neighbors, say h, for the first time, it checks its NNL to learn whether P has been received from an asymmetric link. If $h \notin N_x^s$, x gives up rebroadcasting P to avoid misadvising its neighbors (e. g., in Fig. 1, node H will think there exists a 2-hop path to the gateway via D if it receives the GWADV rebroadcast by D). If $h \in N_x^s$, proceed to step 2.

Step 2 x checks its NNL to learn whether the

Share _ Neighbor field about h is set. If it has not been set, proceed to step 5.

Step 3 Wait for a random number of slots, then submit P for transmission and wait until the transmission actually starts. Note that during this period, the same packet P can be heard again, if this happens, the broadcast ID cache can be used to distinguish and discard duplicate packets.

Step 4 Packet P is on the air. The procedure exits.

Step 5 Cancel the transmission of P that was submitted in step 2. Node x is inhibited from rebroadcasting P in the future. Then the procedure exits.

There are two main reasons why classifying all neighbors under symmetric neighbors and asymmetric neighbors, respectively.

First, if a hello packet, say that originated by h, only includes h' s neighbors set N_h instead of N_h^s and N_h^a, each receiver of this hello packet, say x, can only determine whether the link between it and h is symmetric (depending on $x \in N_h$ or not), but cannot relieve broadcast storm effectively. This is because x' s decision about rebroadcasting is based on $T = N_x - N_h - \{h\}$ instead of $T = N_x^s - N_h^s - \{h\}$, and then there maybe exists a node $n \in N_x^a$ which makes $N_x - N_h - x \neq \varnothing$. As a result, x maybe uselessly rebroadcast broadcast packets to n although the latter cannot hear it (see Fig. 2(a)). On the other hand, there also maybe exists a node $m \in N_x^s$ and $m \in N_h^a$ which makes $N_x - N_h - x = \varnothing$. This will lead x to cancel its rebroadcasting for the broadcast packets (e. g. GWADV) heard from h and then, m cannot set up the path to h via x (see Fig. 2(b)).

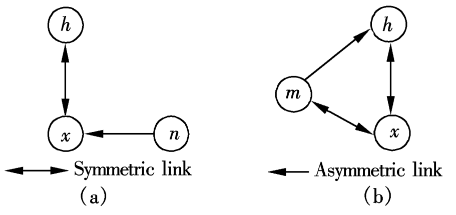

Fig. 2 Impact of unidirectional links on rebroadcasting

Second, if node x only includes its symmetric neighbors set N_x^s in its hello packets, dead-lock will occur because any receiver of this hello packet, say h, adds x in its symmetric neighbor set N_h^s unless it finds itself in the hello packet; however, it never happens before x has found $x \in N_h^s$. Waiting for each other to do it first make the protocol fall into a dead-lock state. So the conclusion can be drawn that, unless the neighbor set included in hello packets is classified into two subsets, i. e., symmetric neighbor set and asymmetric neighbor set, it is impossible to accomplish the discovery of unidirectional links and the relief from broadcast storm simultaneously.

2 Performance Evaluation

To evaluate the proposed approach, a prototype has been implemented in the Network Simulator 2[7] with mobility extensions. Under a varying number of unidirectional links and node speeds, the performance of the improved approach described in the previous subsection has been evaluated using the following performance metrics.

- Packet delivery fraction The number of data packets received by the destination compared with the number of data packets generated by the source.
- End-to-end packet delivery latency The average delivery delay of the data packets from the source to the destination.
- Broadcast control overhead The total transmission number of control broadcast packets. Each hop-wise forwarding of a control packet is counted as one transmission.

Networks consisting of 50 MNs, 2 gateways, 2 routers and 2 fixed nodes (FNs) that are placed in the simulation area of 800 m × 600 m are evaluated. The two gateways running both AODV and fixed IP routing protocols are placed on each side of the simulation area to provide Internet access to MNs, their x, y coordinates in meters are (50, 300) and (750, 300). There are two FNs on the wired network and each of them is connected to a gateway through a router. The two routers are also connected with wired links and the bandwidth of all wired links is 100 Mbit/s. Each node moves according to the random waypoint model[8].

To create unidirectional links, different values of the receiving threshold in the network interface have been set. A node can have either a short or a long range corresponding to high and low receiving threshold levels, respectively. In experiments, short, medial and long ranges in the TwoRayGround propagation model[7] are set to 100, 150 and 250 m, respectively. The fraction of different receiving threshold nodes is varied to vary the number of unidirectional links. In scenario 1, the radio range of all nodes is 150 m, but in scenario 2, the radio range of 2 gateways is 250 m and the others are 150 m. In scenario 3, the radio range of 2 gateways are 250 m, 35 MNs are 150 m and the remainder are 100 m.

There are five constant bit rate (CBR) traffic sources distributed randomly within MANET. The destination of each of the data sessions is one of the two FNs, chosen randomly. The CBR data packets are 512 bytes and the sending rate is 10 packet/s. Node speeds are randomly distributed between zero and a maximum value, denoted by V_{max}. The pause time is always set to 5 s. All simulations are run for 600 simulated seconds. Each data point in the plots represents an average value of 10 runs with the same traffic models and V_{max}, but different randomly generated mobility scenarios. The parameter values for AODV and the hybrid gateway discovery approach are the same as those suggested in Refs. [4, 6]. HELLO_INTERVAL is 1 s, GWADV TTL is 2 and the GWADV sending interval is 5 s.

Internetworking approaches are evaluated in three different network scenarios where the number of unidirectional links is varied. There are no unidirectional links in the first scenario and unidirectional links only exist between the gateways and MNs in the second scenario. And in the third scenario, unidirectional links exist between gateways and MNs as well as within ad hoc clusters. Fig. 3 shows the basic hybrid approach which can provide excellent connectivity in scenario 1. However, once unidirectional links exist between MNs and gateways (scenario 2), the negative impact of unidirectional links on performance becomes very obvious, i. e., more packets are lost and a long delivery delay is also experienced. In scenario 3, the basic hybrid approach drops the highest number of packets and experiences the longest delay.

The new protocol is evaluated using the same parameters in scenario 3. As Figs. 4 (a) to (c) show, the improved protocol performs significantly better than the basic hybrid approach in terms of packet delivery, delay and broadcast control overhead. This is mainly because of two reasons. First, the basic hybrid protocol does not take notice of the unidirectional links and blindly creates routes with unidirectional links. When it learns those routes are useless after several failed attempts, route discoveries without any benefit will repeatedly be executed. Note that after these operations, most packets buffered for the destination at the source are dropped. However, the improved hybrid scheme can effectively overcome unidirectional links by exchanging hello packets. Another reason why the new hybrid scheme achieves good connectivity is that most unnecessary and harmful rebroadcasting is inhibited. Only broadcast packets that have been received from symmetric links and can cover additional symmetric neighbors are rebroadcast. Fig. 4 (c) shows that this leads to a very drastic drop in broadcast control overhead for the improved hybrid scheme compared to the basic one. Rebroadcasting broadcast packets intelligently can not only avoid misleading downstream nodes but also reduce the channel contention and message collision due to rebroadcasting. Also note that the total con-

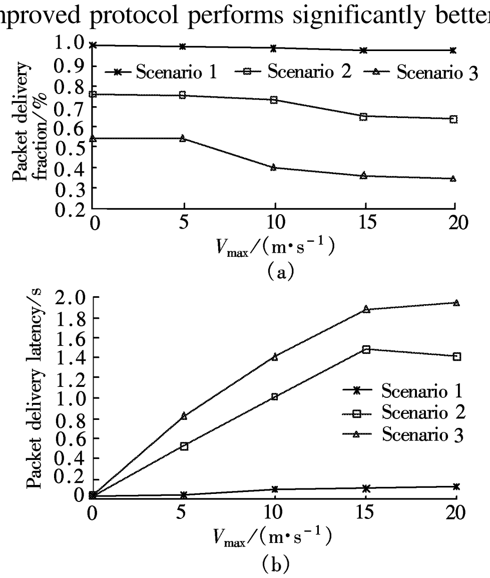

Fig. 3 Impact of unidirectional links on performance. (a) Packet delivery fraction; (b) Packet delivery latency

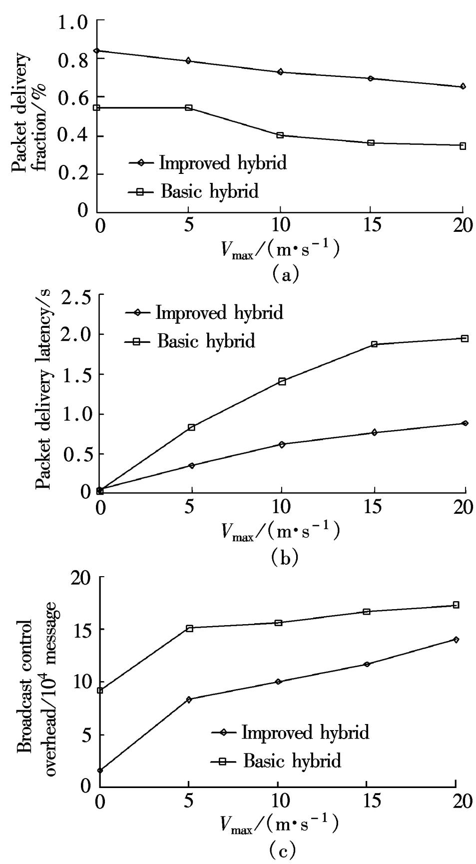

Fig. 4 Performance of the improved hybrid approach under varied speeds. (a) Packet delivery fraction; (b) End-to-end packet delivery latency; (c) Broadcast control overhead

trol overhead of the improved approach is also less than that of the basic hybrid scheme.

3 Conclusion

Simulation results show that the performance of the existing gateway discovery schemes degrades in the presence of unidirectional links and broadcast storm. With this in mind, an improved hybrid gateway discovery approach to enhance the Internet connectivity for MANETs is proposed. On the one hand, the hybrid gateway discovery scheme that combined the advantages of proactive and reactive gateway discovery approach is used to achieve high connectivity while keeping overhead costs low. On the other hand, through exchanging hello packets with additional fields named symmetric neighbor list and asymmetric neighbor list, unidirectional links are removed from route computation and broadcast storm also can be relieved. Performance results using ns-2 simulations, under a varying number of unidirectional links and node speeds, show that this improved Internet connectivity approach can provide better performance than others.

References

[1] Ros Francisco J, Ruiz Pedro M, Gomez-Skarmeta Antonio. Performance evaluation of existing approaches for hybrid ad hoc networks across mobility models[J]. *Journal of Networks*, 2006, **1**(2): 9 − 17.

[2] Jonsson U, Alriksson F, Larsson T, et al. MIPMANET: mobile IP for mobile ad hoc networks[C]//*IEEE/ACM Workshop on Mobile and Ad Hoc Networking and Computing*. Boston: IEEE Press, 1999: 75 − 85.

[3] Wakikawa R, Malinen J T, Perkins C E, et al. Global connectivity for IPv6 mobile ad hoc networks (work in progress), draft-wakikawa-manet-globalv6. txt-2006 [S]. IETF, 2006.

[4] Perkins C, Belding-Royer E, Das S. RFC 3561—2003 ad hoc on demand distance vector routing[S]. IETF, 2003.

[5] Ni S, Tseng Y, Chen Y, et al. The broadcast storm problem in a mobile ad hoc network[C]//*Proceedings of the 5th ACM/IEEE International Conference on Mobile Computing and Networking*. Seattle: ACM Press, 1999: 151 − 162.

[6] Ratanchandani P, Kravets R. A hybrid approach to Internet connectivity for mobile ad hoc networks[C]//*IEEE Wireless Communications, Networking and Computing*. New Orleans: IEEE Press, 2003: 1522 − 1527.

[7] Fall K, Varadhan K. NS manual [EB/OL]. (2002-04-24) [2006-07-01]. http://www. isi. edu/nsnam/ns/ns-documentation. html.

[8] Broch J, Maltz D A, Johnson D B, et al. A performance comparison of multihop wireless ad hoc network routing protocols[C]//*Proceedings of the 4th ACM/IEEE International Conference on Mobile Computing and Networking*. Dallas: ACM Press, 1998: 85 − 97.

一种增强移动自组网 Internet 连接的改进型方案

沈 斌[1] 李 波[2] 石冰心[1]

([1] 华中科技大学电子与信息工程系,武汉 430074)

([2] 云南大学信息学院,昆明 650091)

摘要:针对移动自组网因单向链路以及盲目转播网关发现分组而造成的与 Internet 互联性能下降,提出了一种增强型互联方案. 同时结合了先应和后应网关发现策略优点的混合网关发现策略被用来获取良好的 Internet 连接并保持低开销. 而通过交换携带有额外增加的对称邻居节点列表和非对称邻居节点列表字段的 AODV hello 分组,单向链路得以从路由计算中予以清除而广播风暴也同时得到抑制. 基于 ns-2 的仿真结果表明此改进型 Internet 连接方案在单向链路数量及节点移动速度均变化的应用环境下能取得较其他方案为优的互联性能.

关键词:移动自组网;Internet 互联;网关发现;单向链路;广播风暴

中图分类号:TP393