Position based Opportunistic Routing for Robust Data Delivery in MANETs

Shengbo Yang, Feng Zhong, Chai Kiat Yeo, Bu Sung Lee
Centre for Multimedia and Network Technology
School of Computer Engineering
Nanyang Technological University, Singapore 639798
Email: {yang0201, zhon0026, asckyeo, ebslee}@ntu.edu.sg

Jeff Boleng
Department of Computer Science
United States Air Force Academy
Email: Jeff.Boleng@usafa.edu

***Abstract*—Traditional MANET routing protocols are quite susceptible to link failure as well as vulnerable to malicious node attack. In this paper, we propose a novel protocol called Position based Opportunistic Routing (POR) which takes full advantage of the broadcast nature of wireless channel and opportunistic forwarding. The data packets are transmitted as a way of multicast (which is actually implemented by MAC interception) with multiple forwarders. A forwarder list determined by previous hop according to local position information is inserted into the IP header and the candidates take turn to forward the packet based on a predefined orders. This redundancy and randomness make it quite efficient and robust. In addition, inherited from position based routing, POR's control overhead is almost negligible which justifies its good scalability. Both theoretical analysis and simulation results show that POR not only achieves outstanding performances in normal situations but also yields excellent resilience in hostile environments.**

I. Introduction

Traditional MANET routing protocols are quite susceptible to link failure as well as vulnerable to malicious node attacks. One of the main reasons is due to the property that a predetermined route must be established before packet transmission. (It is realized through periodic update for every node in proactive routing, or on-demand construction in reactive routing.) Such kind of route discovery and establishment process inevitably introduce a variety of control messages which can become an attacker's target and can be easily intercepted, modified or just dropped. The QoS of the communication is thus degraded and even worse, the transmission could never be established.

Most existing mechanisms that protect the routing protocol from attack focused on protection of control messages, such as authentication of control packets, protection of mutable information in control packets [1], [2], etc. From this point of view, the control messages, which originally took the role of facilitating the establishment of communication, now become the source of vulnerability of routing protocols in adverse or even hostile environment. Hence position based routing is more resilient compared with other traditional protocols, because they do not use control packets [1] and potential multiple paths are available (for those broadcasting protocols).

Epidemic routing [3], a routing protocol designed for Delay Tolerant Network (DTN), is quite robust to nodes' failure as well as malicious nodes' misbehavior. Contrary to precomputing a single route, the delivery of packets is determined at run time – a node traversed who does not have a copy of the current packet maintain a copy. Several nodes keep copies and it is thus quite resilient to partial malicious nodes' dropping. Though it is forced to adopt such a store and forward routing mechanism because of the lack of end-to-end connectivity in DTN [4], [5], this property enhances survivability [6].

On the other hand, opportunistic routing [7], [8], which works in connected static ad hoc networks, is another kind of routing protocol that also determines the delivery of packets in real time. Both simulation results and real implementation illustrate that it is quite efficient and reliable. However, as the forwarding priority is determined according to the link delivery probabilities, a measurement of loss rate is necessary before transmission which is not easy to be implemented in mobile networks.

From the above scenarios we can conclude that the property of pre-determining an end-to-end route and unicast are two key sources of vulnerability in conventional MANET routing protocols. Owing to the unstable wireless channel, constantly changing network topology, and even malicious nodes' misbehavior, it is very difficult to maintain a deterministic route and discovery and recovery processes are too long. In fact, because of the broadcast nature of a wireless channel, when the next hop node on a route fails to receive the packet or is malicious and drops the packet, its neighbors might have eavesdropped the signal. In traditional routing protocols, these packets are simply dropped at the MAC layer. If these neighbors can forward the packet instead of the original next hop node, then communication continues, instead of being disrupted by node or link failure.

Therefore, in order to enhance the resilience of MANET routing protocols in face of nodes' failure or malicious nodes' misbehavior, a certain degree of redundancy and randomness are important factors or requirements. Reduction in control messages can make it more difficult for malicious nodes to carry out attacks and redundancy can increase the survivability of the whole system. Hence it motivates us to introduce opportunistic routing in position based routing protocols [9]. Our simulation results show that in a moderate mobile ad hoc network with the presence of all nodes maliciously dropping forwarding packets with the probability of 50%, POR still enables more than 90% of the packets to be eventually delivered.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

The remainder of the paper is structured as follows: We present the design of POR in Section II and analyze its efficiency and robustness in Section III. In Section IV, we evaluate its performance and compare it with existing routing protocols. Section V concludes the paper and sketches out our future plan.

II. Position based Opportunistic Routing

The Position based Opportunistic Routing (POR) can be briefly described as follows:

1) The location information of nodes can be obtained with GPS-like equipment and neighbors' coordinates are updated periodically through one-hop beacon.

2) When a source node S sends a packet to the destination node D, it calculates the forwarder list according to the distance between its neighbors and the destination, and inserts the list into the packet header. The neighbor who is nearer to the destination will have higher priority. After that, the packet is sent out, taking the best forwarder as the next hop. Here, the size of the forwarder list can be set with respect to the requirement of the application, e.g. in our experiment we limit the forwarder list to five candidates.

3) All nodes within the sender's one-hop coverage may receive the packet. The receiver checks its position in the forwarder list. If there are n nodes ahead of it, it will wait for n time slots before forwarding that packet. If it hears the same packet being sent by other nodes before the dedicated time slot, it will discard the packet.

4) Subsequent nodes will do the same operation until the packet reaches the destination.

Here, multicast transmission and run time route decision are the two main points.

A. Position based Routing

POR is based on geographic routing, the only information exchanged is a node's location obtained via GPS-like equipment. When a source node wants to transmit a packet to the destination, it should get the location (x, y) of the destination through a location service. Here we assume that a location registration and look up service which maps node addresses to locations has already been available just as in [10]. It could be realized using many kinds of mechanisms [11]. In our scenario, some efficient and reliable way is also available. For example, the location of the destination could be transmitted by low bit rate but long range radios which can be implemented as periodical beacon. Another possible technique would be to use location replies when requested by the source.

Position-based property makes POR robust and scalable. The location information is actually used to limit the flooding range, other than accurate control message (such as the Reply in AODV) to determine the unique next hop. Moreover, the reduction in control packets and the almost stateless nature of POR underscore its excellent scalability. It only relies on the knowledge of the forwarding node's immediate neighbors and the state required is almost negligible.

B. Opportunistic Packets Forwarding

When a node sends or forwards a packet, it should select the next hop forwarders among its neighbors. Every node maintains a forwarding table for each destination of the packets that it has sent or forwarded. Before calculating a new forwarder list, it looks up the forwarding table to check if a valid forwarder list for that destination is still available. In case the number of forwarders is zero, the incoming packet will be cached and checked later to see if a new forwarding chance is available. These packets will finally get delivered or discarded when the corresponding timer expires.

When a node receives a packet and finds itself is not the first candidate in the forwarder list, it will cache the packet for a period of time according to its forwarding priority determined by the forwarder list. Every node maintains a packet list that contains the packets which have been cached and each packet is also attached a counter. The node will check the list periodically and the counter will be decreased by one every time. When the counter becomes zero, the packet will be forwarded. On the other hand, when a node receives a packet, it will look up an ID record table first to check whether the incoming packet has already been received before. If yes, this packet must be relayed by the node with higher forwarding priority, then the corresponding cached packet will be discarded and the incoming packet will also be dropped. The packet header format of location beacon and data are illustrated in Fig. 1.

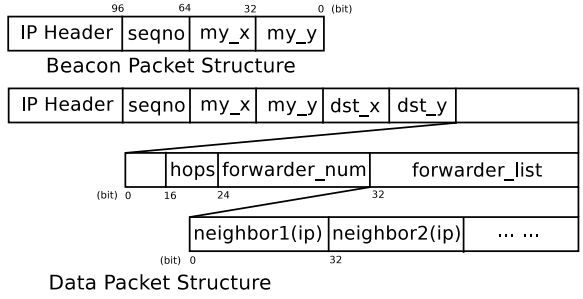

Fig. 1. Packet header structure

All control packets except one hop beacon are eliminated. For beacon packet, 12 Bytes are introduced; and for data packet, (24 + 4 $\times$ forwarder_num) Bytes are added to the IP header. The forwarder_num can be limited to achieve a balance between the robustness and overhead.

C. Potential Multipath

In case the suboptimal forwarder is out of the range of a better forwarder as illustrated in Fig. 2 (B cannot hear A), it will relay the packet after a certain period of time. Then, the packet will be transmitted through a second path which can be seen as a backup. If the packet reaches a node (C) that has already received the same packet, it will be discarded and the two paths are merged. Otherwise, it may be delivered to the destination (D) independently. Though more resource might

978-1-4244-4148-8/09/$25.00 ©2009

be consumed in such potential mutipath scenarios, resilience is actually being improved.

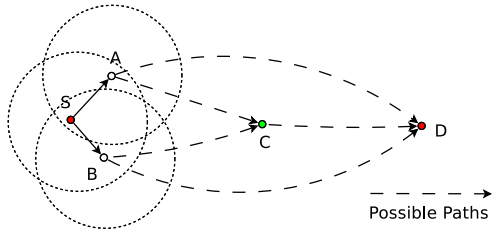

Fig. 2. Multipath in POR

D. Local Information Maintenance

1) Neighbor List: Every node maintains a neighbor location list. The list is generally updated by one hop beacon. However, with the previous hop's location piggybacked in the data packet's IP header, fewer beacon packets are required to be sent. When any node sends a data packet, it can then reset its inter-beacon timer. This reduction can be more significant when the traffic becomes heavier in the network. (It has been shown that even moderate data traffic can result in no required beacon traffic at all [12]).

2) ID Record: As the data packets are transmitted in a multicast like form, every node keeps an ID record in case of duplicate reception. The item of the record consists of source address and sequence number. The incoming packet will be checked whether it has been received before and the corresponding operation will be executed.

3) Forwarding Table: Compared with traditional MANET routing protocols, the routing table is replaced with a forwarding table as illustrated in Table I.

dst_ip	forwarder_num	forwarder_list
1	2	2 3
4	3	1 2 3
...	...	...

TABLE I
FORWARDING TABLE

The forwarding table is constructed during data packet transmissions and its maintenance is much easier than a routing table. It can be seen as a trade off between efficiency and scalability. As the establishment of the forwarding table only depends on local information, it takes much less time to be constructed. Therefore we can set an expire time on the items to keep the table relatively small. In other words, the table record only the currently active flows, while in conventional protocols, a decrease in the route expire time would require far more resources to rebuild.

4) Packet List: When a node receives a new packet and finds it has to wait for a certain time before forwarding, the packet will be inserted into the packet list. The list will be checked periodically and the packet in the list will be sent out at certain time slot or discarded if the same packet is received during the waiting period (this implicitly means a better forwarder has carried out the task).

5) Packet Buffer: If no forwarder is available, the packet will be cached in a packet buffer. In case a node receives a packet that has been received before, it will also check the packet buffer besides the packet list. If the previous hop's priority is higher than current node, the dedicated packet in the packet buffer will be removed.

E. MAC Modification and Extensions

1) MAC Interception: We leverage on the broadcast nature of 802.11 MAC: all nodes within the coverage of the sender would receive the signal. However, its RTS/CTS/ACK mechanism is only designed for unicast. It simply sends out data for all broadcast packets with CSMA. Therefore packet loss due to collisions would dominate the performance of multicast like routing protocols. Here, we did some alteration on the packet transmission scenario. In the IP layer, we just send the packet in unicast form, and take the best forwarder as the next hop. In this way, we make full utilization of the collision avoidance supported by 802.11 MAC. While on the receiver side, we do some modification of the MAC layer address filter: even when the data packet's next hop is not the receiver, it is also delivered to the upper layer, further processed by POR. This MAC interception takes advantage of both broadcast and unicast (MAC support).

2) MAC Callback: When the MAC layer forwarding of a data packet exceeds a certain time, the function implemented in POR – mac_callback will be executed. The forwarder list to that destination in the forwarding table will be deleted and the best forwarder in the neighbor list will be removed too. The packet will be given a second chance to reroute (i.e. compute new forwarders). In case that packet appears again (pulled back from the lower layer), it will be dropped. As the location information of the neighbors is updated periodically, some items might become obsolete very quickly especially for nodes with high mobility. This scheme introduces a timely update which enables more packets to be delivered.

3) Interface Queue Inspection: One of the main points of POR is when intermediate nodes receive a packet with the same source address and sequence number, which means a better forwarder has already taken over the function, it will drop that packet from its packet list. Besides maintaining a packet list, we also check the interface queue located between the LL layer and MAC layer. We do this because when the packet arrives at the IP layer, the same packet might have already been sent down by current node. By additional inspection of the interface queue, we further decrease the duplicated packets appearing in the wireless channel.

III. ANALYSIS

A. Resilience to Dead-end

In GPSR [10] like geographic routing, a node's void will lead to greedy forwarding's failure and such a problem is called a "dead-end". As illustrated in Fig. 3, Node A that has no neighbors nearer than itself to the destination D will be selected by Node S as the next hop and thus the greedy forwarding stops. In fact, the packet might be routed through

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

Node B. The spotted area together with the shaded area is called Node A's void area. This 'void' area looks very large for unicast geographic routing. However in POR, due to its multicast mechanism, the spotted area is now covered and is no longer a void zone, leaving only the shaded area where nodes such as Node B can reside. This remaining void zone is therefore much smaller than that of other unicast protocols. In fact, if there are other sub-optimal forwarders, such as Node C nearby, even this small void zone (shaded area) can be partially covered.

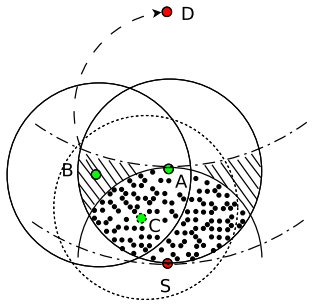

Fig. 3. Dead-end in POR

In case a dead-end appears, we argue that in a mobile network without huge obstacles, it has little adverse effects on routing, especially in a highly dynamic network. As a node's void will most likely be recovered by a node's movement in a very short time, it might be better to cache the packets for a while before discovering a new forwarder than routing around via a farther path [13].

In order to prove this proposition, we simulate the performance of GPSR with and without perimeter mode in different mobile networks with various node density and mobility (in Section 4). The results show that perimeter mode could increase the packet delivery ratio to some extent (no more than 1%). However, additional delay caused by suboptimal routes can increase the packet transmission delay significantly, especially in large scale and highly dynamic networks. From this point of view, it is not worthwhile to pay much attention to the dead end problem which only gets serious in static network with huge obstacles such as mountains. This fact not withstanding, in POR, the node's void is actually shrunk greatly because of multicast.

B. Resilience to Selective Forwarding

Here, we only consider selective forwarding attack. Malicious nodes behave like normal nodes most of the time but selectively drop packets. There are two parameters: one is the malicious nodes' proportion (p_m) and the other is the probability that a malicious node drops forwarding packets (p_d). Then there is a probability of $x = p_m p_d$ that a data packet will be dropped at every hop.

For GPSR and AODV like unicast routing protocols, suppose the percentage of *i* hops transmission is m_i and the corresponding packet delivery ratio is P_i, then the whole packet delivery ratio in normal situations will be

$$P = \sum_{i=1}^{N} m_i P_i \tag{1}$$

Here, we assume the maximum number of hops is N.

In critical environment with selective forwarding, the ratio will become

$$P_{unicast} = \sum_{i=1}^{N} m_i P_i (1-x)^{i-1} \tag{2}$$

Assume $P_i = 1$ $(i = 1, \ldots, N)$ for simplicity, we get

$$P_{unicast} = \sum_{i=1}^{N} m_i (1-x)^{i-1} \tag{3}$$

For POR like multicast routing protocol, suppose every node has n candidate forwarders and the distance from the source to the destination for multi-hop transmission is $\overline{N}$ ($\overline{N} \geq 2$) hops on average. (It has been verified by simulation that for moderate packet drop probability, $\overline{N}$ remains almost constant.) The probability that the *k*-th candidate forwards the packet is:

$$Pr_k = x^{(k-1)}(1-x) \tag{4}$$

Assume on average the $\overline{k}$-th forwarder relays the packet for successful transmission, then

$$\overline{k} = \frac{\sum_{k=1}^{n} k Pr_k}{\sum_{k=1}^{n} Pr_k} \tag{5}$$

Neglecting the collisions and transmission errors, the probability that a packet can be successfully delivered to the destination is:

$$P_{multicast} = m_1 + (1-m_1)[1-x^n]^{(\overline{N}-1)} \tag{6}$$

Comparing equation (3) and (6), we can see that the multicast nature makes POR quite robust to node failure or attacks. The great improvement will be shown more clearly in the following section.

On the other hand, along with the increase in the proportion of malicious nodes, the end to end packet transmission delay of multicast routing protocols also increases.

$$t_{multicast} = t_0 + (1-m_1) \cdot (\overline{N}-1) \cdot (\overline{k}-1) \cdot \Delta T \tag{7}$$

Here, t_0 denotes the packet transmission delay in corresponding normal situations in which both p_m and p_d are 0. ΔT is the time slot.

On the contrary, the transmission delay of unicast routing protocols will be decreased. The reason is the high packet dropping probability will lead to the reduction of the number of hops that the data packet can go any further.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

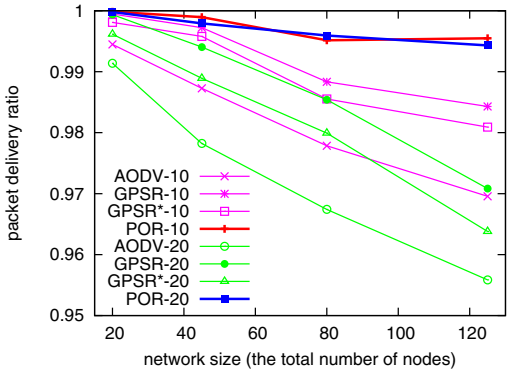

Fig. 4. Packet delivery ratio in normal situations

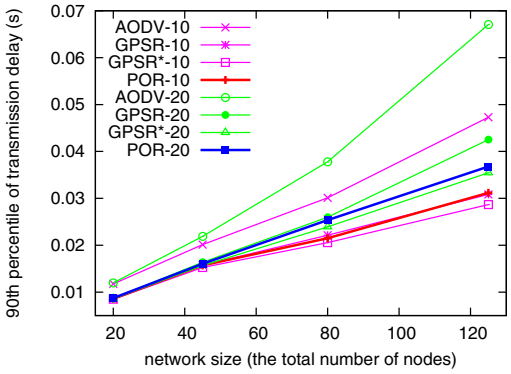

Fig. 5. The 90th percentile of transmission delay in normal situations

IV. Simulations

To evaluate the performance of POR, we simulate the algorithm in a variety of mobile network topologies in ns-2 [14], together with the famous geographic routing protocol GPSR (including the version with perimeter mode switched off, denoted as GPSR*) and on demand routing protocol AODV. Two network environments: the normal one without malicious nodes and the critical one with selective forwarding attack are simulated. Performance metrics include packet delivery ratio, the 90th percentile and average of packet transmission delay.

A. Normal Situations

Nodes	Region	CBR Flows	Max Speed
20	500 m×500 m	10	10 m/s, 20 m/s
45	750 m×750 m	10	10 m/s, 20 m/s
80	1000 m×1000 m	10	10 m/s, 20 m/s
125	1250 m×1250 m	10	10 m/s, 20 m/s

TABLE II
Simulated Topology Characteristics

We first evaluate the performance of POR in normal situations where all nodes are cooperative. Eight network topologies are simulated, as illustrated in Table II.

Our simulations are for networks of 20, 45, 80 and 125 nodes with 802.11 WaveLAN radios, with a nominal 250-meter range and a density of 1 node per 12500 m^2. A radio range is nearly 200,000 square meters. As a result, there are an average of approximately 15 neighbors within the range of a node. We assume that 7 neighbors are located in the candidate area (e.g. the distance between those neighbors are nearer than the current node). As we set the maximum forwarder list in the IP header at 5 we can assume that there are 4 effective forwarders in the forwarder list on average. The nodes are initially placed randomly in a square region. All nodes move according to the random waypoint model [15], with a pause time of 5 seconds and maximum velocity of 10 m/s or 20 m/s. In traffic, we simulate 10 CBR flows and each flow sends at 4 Kbps with 256-Byte packets. The simulation results based on 25 independent runs are illustrated in Fig. 4 and Fig. 5 (<protocol>-<max speed>).

From Fig. 4 we can see that the delivery ratio of POR outperforms the other protocols, especially when the network is large and the mobility of the nodes increases.

On the other hand, the results in Fig. 5 show that the packet transmission delay of POR is comparable if not better at most cases, despite POR's higher packet delivery ratio. As a matter of fact, when the delivery ratio is higher, the packet transmission delay is usually larger, because packets that are not previously delivered by other protocols, are now being successfully delivered. Such packets usually incur long delay. Hence, from this point of view, POR performs very well.

Inherited from position based routing, POR's scalability is quite good. Both the performance of the packet delivery ratio and transmission delay only degrade slowly with the growth of the network size compared with the other protocols.

B. Critical Situations

With the above experiments, we demonstrate that POR performs well and even better than traditional geographic routing protocols (e.g. GPSR) and on demand routing protocols (e.g. AODV). We then drop some packets to simulate a critical wireless environment. The network topology we employ is 80 nodes in a region 1000m×1000m, with max node speed 10m/s. The traffic is the same as in normal situations. Here, we set the packet drop probability at 0.5 and compare the performance of the three protocols with different malicious nodes' proportion. The simulation results are illustrated in Fig. 6 and Fig. 7.

From Fig. 6 we can see that the multicast nature (actually implemented by MAC Interception) makes POR quite robust. As the proportion of malicious nodes increases, the delivery ratio of GPSR and AODV decreases significantly, more or less linearly, while POR maintains a high delivery ratio. Even when the proportion increases to 1.0 (which means all nodes are not cooperative in forwarding other nodes' data packets), the delivery ratio of POR is still above 90% (to be exact 91.0%). As a trade-off the packet transmission delay of POR also increases (Fig. 7). As mentioned, a high delivery ratio incurs higher delay in such challenged environment. For non-delay sensitive applications, this degree of delay is quite acceptable. On the contrary, the packet transmission delay of

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

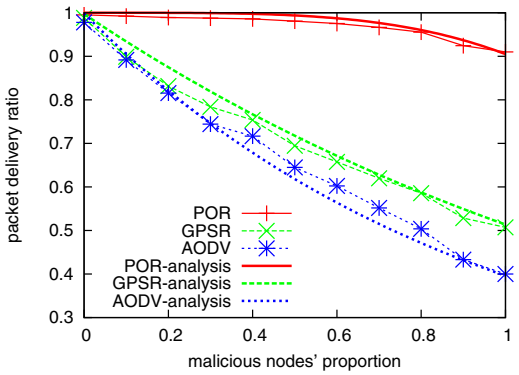

Fig. 6. Packet delivery ratio in critical situations

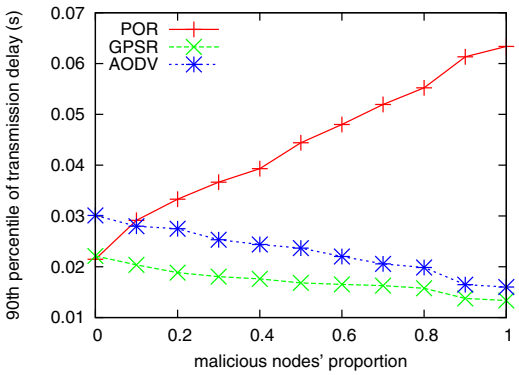

Fig. 7. The 90th percentile of transmission delay in critical situations

GPSR and AODV decreases when more nodes selectively drop data packets, just as analysed in Section 3.

C. Theoretical Comparison

By using the data obtained from the simulation of normal situation, we get three theoretical delivery ratio curves for POR, GPSR and AODV according to Eqns. (6) and (3), as illustrated in Fig. 6 (denoted as POR-analysis, GPSR-analysis and AODV-analysis, respectively). On the other hand, when we set the time slot to 0.01s, we can also get the theoretical delay curve for POR from Eqn. (7), which is shown in Fig. 8. Compared with simulation results, we find the theoretical analysis, though simple, predicts the performance quite well.

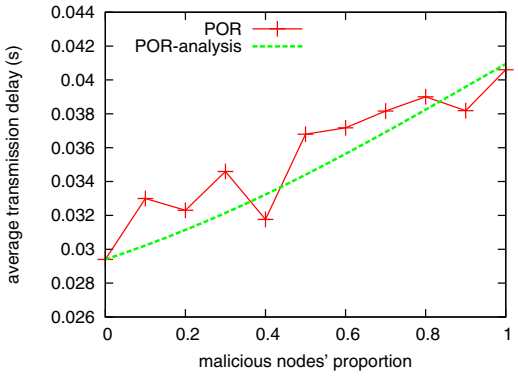

Fig. 8. Average transmission delay of POR in critical situations

V. Conclusion

Inspired by DTN and opportunistic routing, we propose a novel MANET routing protocol POR which takes full advantage of the wireless channel's broadcast nature. Through the introduction of a certain degree of redundancy and randomness in data delivery, the protocol is very robust as well as efficient. It performs well in normal situations and maintains high packet delivery ratio in critical environments where a large proportion of malicious nodes arbitrarily drop packets.

Benefiting from a priority based forwarding schedule, there are not many duplicate packets in the wireless channel despite the use of multicast-like transmission. The main cost here is increased computational resources since more packets will be delivered to the upper layer to be processed by the routing protocols. More buffer space will also be needed though it will not be too much as long as the time slot is properly selected.

In our future work, more extended analysis and simulation will be carried out, including the consideration of packet duplication and buffer consumption. The selection of time slot and the maximum number of forwarders will also be evaluated and more comparisons with other protocols will be conducted.

References

[1] L. Buttyn and J.-P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge University Press, November 2007.

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *Wireless Communications, IEEE*, vol. 14, no. 5, pp. 85–91, October 2007.

[3] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Duke University, Tech. Rep., 2000.

[4] K. Fall, "A delay-tolerant network architecture for challenged internets," in *SIGCOMM '03*. New York, NY, USA: ACM, 2003, pp. 27–34.

[5] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 4, pp. 145–158, 2004.

[6] J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine, "Surviving attacks on disruption-tolerant networks without authentication," in *MobiHoc '07*. New York, NY, USA: ACM, 2007, pp. 61–70.

[7] S. Biswas and R. Morris, "Exor: opportunistic multi-hop routing for wireless networks," in *SIGCOMM '05*. New York, NY, USA: ACM, 2005, pp. 133–144.

[8] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in *SIGCOMM '07*. New York, NY, USA: ACM, 2007, pp. 169–180.

[9] M. Mauve, A. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *Network, IEEE*, vol. 15, no. 6, pp. 30–39, Nov/Dec 2001.

[10] B. Karp and H. T. Kung, "Gpsr: greedy perimeter stateless routing for wireless networks," in *MobiCom '00*. New York, NY, USA: ACM, 2000, pp. 243–254.

[11] S. Das, H. Pucha, and Y. Hu, "Performance comparison of scalable location services for geographic ad hoc routing," *INFOCOM 2005*, vol. 2, pp. 1228–1239 vol. 2, March 2005.

[12] J. Boleng and T. Camp, "Adaptive location aided mobile ad hoc network routing," *IPCCC '04*, pp. 423–432, 2004.

[13] M. Grossglauser and D. Tse, "Mobility increases the capacity of ad hoc wireless networks," *Networking, IEEE/ACM Transactions on*, vol. 10, no. 4, pp. 477–486, Aug 2002.

[14] "The network simulator ns-2," http://www.isi.edu/nsnam/ns/.

[15] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications and Mobile Computing*, vol. 2, no. 5, pp. 483–502, 2002.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.