Security-Efficient Routing For Highly Dynamic MANETS

S.Sharon Ranjini, G.Shine Let

Abstract*— The Goal of Position-based Opportunistic Routing (POR) is to solve the problem of delivering data packets for highly dynamic mobile adhoc networks in a timely manner. The protocol (POR) takes the property of Geographic routing. Here, the data packets are sent out from the source node and some of the neighbor nodes will be the forwarding candidates, if the best forwarder did not forward the packet in a particular period of time; the forwarding candidates will forward the packets. By using Virtual Destination-based Void Handling (VDVH) Scheme, the communication hole is avoided. In the existing system, the geographic routing property is used, the problem of delivering data packets for highly Dynamic mobile adhoc networks is solved. But there is a limitation that the nodes that is selected as the best forwarder is not checked whether it is secured or not. To overcome this problem a Security-efficient routing is proposed in which the nodes which have the higher trust value is considered as the best forwarder. The Selfish and normal nodes is differentiated by using the RREQ algorithm. The Selfish nodes do not forward the request. It will check the trust value, whether it is friend or stranger or acquaintances. In this approach, From the RREQ algorithm, Xrf, Xra, Xrs are the threshold values set for friends, acquaintances and strangers, as per the requirements of the application software. Random waypoint model is chosen as the movement.

Index Terms*— Mobile Adhoc Networks, *RREQ algorithm, Random waypoint model, Routing.

I. INTRODUCTION

The lack of any centralized infrastructure in mobile adhoc networks (MANET) is one of the greatest security concern in wireless networks. Communication in MANET functions properly only if the participating nodes co-operate in routing without any malicious intention[4]. By indulging in flooding attacks on their neighbors, some of the nodes may be malicious in their behavior. Some others may act maliciously by launching active security attacks like denial of service. A new trust approach based on the extent of friendship between the nodes is proposed which makes the nodes to co-operate and prevent attacks in an adhoc environment. The performance of the trust algorithm is tested in an adhoc network implementing the Adhoc-on Demand Distance Vector (AODV) protocol. Adhoc networks are simple peer-to-peer networks, self-organized with no fixed infrastructure. Security is a major concern in these networks. The wireless channels are vulnerable to various security attacks.

Manuscript received on April,2013.

S. Sharon Ranjini, PG Scholar**,** Electronics and Communication Engineering, Karunya University, Coimbatore, India.

G. Shine Let, Assistant Professor**,** Electronics and Communication Engineering, Karunya University, Coimbatore, India.

These unique characteristics of wireless ad hoc networks make traditional cryptographic mechanisms and assumptions inappropriate. Wireless ad hoc networks have received much research attention in both academia and industry in the recent years[6]. The Recent research indicates that wireless ad hoc networks are prone to malicious attacks. Besides the inherent insecurity of wireless communication networks, it also has been identified that wireless ad hoc networks are vulnerable to some specific attacks, due to their unique network characteristics. In wireless ad hoc networks, nodes are free to move. The arbitrary movement of nodes will change the network topology frequently. The dynamic network topology will result in significantly changing the status of trust relationship among the nodes. The security implementation based on trust is confronted with great challenges and in dynamic environment; the static security mechanisms are not applicable. The mobility of nodes may also cause frequent link breakage and data loss, so the nodes may join and leave the networks without any notification. So the connections among the nodes will not be guaranteed all the time. The intermittent transmission environment has great impact on information communication in wireless ad hoc networks, which will affect all applications along with the security implementation.

Mobile nodes of wireless ad hoc typically include portable devices, such as laptops, personal digital assistants (PDA), cellular phones and micro sensors. These devices are inevitably battery powered. The battery lifetime becomes crucial for wireless communication and mobile computing, which can be a target of malicious attackers. To launch an attack, malicious node may send an intensive computing task to other node in attempt to exhaust the target nodes' battery, and consequently block the network communications and services. Limited communication bandwidth may also be a target for malicious attacks, such as Denial of Service (DoS) attack[8]. To implement such attack, the malicious node may send vicious queries flooding to target nodes to consume the bandwidth and occupy the shared wireless media, which make the network service unavailable to other nodes.

II. RELATED WORKS

The limited transmission range of wireless network interfaces, multiple network "hops" may be needed for one node to exchange data with another across the network suggested by (J.Broch et al.1998).In recent years, a variety of new routing protocols targeted specifically at this environment have been developed, but little performance information on each protocol and no realistic performance comparison between them is available.

This paper presents the results of a detailed packet-level simulation comparing four multi-hop wireless ad hoc network routing protocols that cover a range of design choices: DSDV,

TORA, DSR, and AODV. We have extended the ns-2 network simulator to accurately model the MAC and physical-layer behavior of the IEEE 802.11 wireless LAN standard, including a realistic wireless transmission channel model, and present the results of simulations of networks of 50 mobile nodes.

The ad hoc routing protocols that make forwarding decisions based on the geographical position of a packet's destination was reviewed by (M.Mauve et al.2001).Other than the destination's position, each node need know only its own position and the position of its one-hop neighbors in order to forward packets. Position-based routing works well even if the network is highly dynamic. This is a major advantage in a mobile ad hoc network where the topology may change frequently.

If geographic greedy forwarding fails to move a packet further towards its destination due to communication voids, then it will become an important issue for geographic routing in wireless networks was prescribed by (D.Chenet et al.2007). This article presents an overview of the void problem and surveys the currently available void-handling techniques for geographic routing. In the survey, it classifies these void-handling techniques into six categories, each designed with a different approach, that is, planar-graph-based, geometric, flooding-based, cost based, heuristic, and hybrid. For each category, it presents its basic principle and illustrates some classic techniques as well as the latest advances. It also provides a qualitative comparison of these techniques and discusses some possible directions of future research.

The Geographic routing protocols to allow stateless routing in mobile ad hoc networks (MANETs) by taking advantage of the location information of mobile nodes and thus are highly scalable. A central challenge in geographic routing protocols is the design of scalable distributed location services that track mobile node locations were introduced by (D. Son et al.2004) . A number of location services have been proposed, but little is known about the relative performance of these location services. Geographic routing has been introduced in mobile ad hoc networks and sensor networks. Under ideal settings, it has been proven to provide drastic performance improvement over strictly address-centric routing schemes. While geographic routing has been shown to be correct and efficient when location information is accurate, its performance in the face of location errors is not well understood.

Greedy Perimeter Stateless Routing (GPSR), a novel routing protocol for wireless datagram networks that uses the *positions* of routers and a packet's destination to make packet forwarding decisions. GPSR makes *greedy* forwarding decisions using only information about a router's immediate neighbors in the network topology were prescribed by(B. Karp et al. 2000). When a packet reaches a region where greedy forwarding is impossible, the algorithm recovers by routing around the *perimeter* of the region. By keeping state only about the local topology, GPSR scales better in per-router state than shortest-path and ad-hoc routing protocols as the number of network destinations increases. Under mobility's frequent topology changes, GPSR can use local topology information to find correct new routes quickly. Multihop wireless mesh networks are becoming a new attractive communication model due to their low cost. Routing protocols are critical to the performance and reliability of wireless mesh networks was described by (E. Rozner et al2009). In this paper, a Simple Opportunistic Adaptive Routing protocol (SOAR) to explicitly support multiple simultaneous flows in wireless mesh networks is proposed. SOAR incorporates the following four major components to achieve high throughput and fairness: 1) adaptive forwarding path selection to leverage path diversity while minimizing duplicate transmissions, 2) priority timer-based forwarding to let only the best forwarding node forward the packet, 3) local loss recovery to efficiently detect and retransmit lost packets, and 4) adaptive rate control to determine an appropriate sending rate according to the current network conditions. Its implements SOAR in both NS-2 simulation and an 18-node wireless mesh test bed. The evaluation shows that SOAR significantly outperforms traditional routing and a seminal opportunistic routing protocol, ExOR, under a wide range of scenarios.

III. PRELIMINARIES

Geographic routing protocols will allow stateless routing in mobile ad hoc networks (MANETs) by taking advantage of the location information of mobile nodes and thus are highly scalable. A central challenge in geographic routing protocols is the design of scalable distributed location services that track mobile node locations was described by (S. Das et al2005). A number of location services have been proposed, but little is known about the relative performance of these location services. It presents a quantitative model of protocol overheads for predicting the performance tradeoffs of the protocols for static networks. It then analyzes the performance impact of mobility on these location services. Finally, It compare the performance of routing protocols equipped with the three location services with two topology-based routing protocols, AODV and DSR, for a wide range of network sizes. The study demonstrates that when practical MANET sizes are considered, robustness to mobility and the constant factors matter more than the asymptotic costs of location service protocols. In particular, while GLS scales better asymptotically, GHLS is far simpler, transmits fewer control packets, and delivers more data packets than GLS when used with geographic routing in MANETs of sizes considered practical today and in the near future. Similarly, although XYLS scales worse asymptotically than GLS, it transmits fewer control packets and delivers more data packets than GLS in large mobile networks.

Geographic ad hoc networks use position information for routing. They often utilize stateless greedy forwarding and require the use of recovery algorithms when the greedy approach fails was suggested by (N. Arad et al2009). We propose a novel idea based on virtual repositioning of nodes that allows increasing the efficiency of greedy routing and significantly increasing the success of the recovery algorithm based on local information alone. It explains the problem of predicting dead ends.

IV. SECURITY-EFFICIENT ROUTING

In Position-based opportunistic approach, the problem identified is that the nodes that are selected as the best forwarder might be trustable or not trustable. Best forwarder is not analyzed or checked whether it is secured or not. So in the enhancement work, the trust value is estimated for each node. In the proposed work the node which has the higher trust value will be considered as the best forwarder. The

Project work shows the enhancement of the previous work done. In the previous work done a best forwarder node is selected from the geographic routing and greedy forwarding. In the enhancement work, the node that is selected as the best forwarder is seen whether it is trustable node or malicious node. The trust value is calculated by using RREQ algorithm which sets the threshold value for friends, acquaintances and strangers. The participating nodes should know in advance regarding the type of security attack in the network and run the corresponding algorithm to detect the misbehavior nodes in the network. All the nodes in an adhoc network are categorized as friends, acquaintances or strangers based on their relationships. During network initiation all nodes will be strangers to each other. A trust estimator is used in each node will be strangers to each other.

Accordingly, the neighbors are categorized into:

- Friends(Most trusted)→0.5-1
- Acquaintances(Trusted)→0.3-0.5
- Strangers(Not Trusted)→0-0.3

During route discovery phase of the dsr protocol, the extended system also computes the aggregate trust along different paths to the destination . From this the most trusted path between the source and the destination is found out before establishing the data transfer. The segregation of the neighboring nodes into friends, acquaintances and strangers is the outcome of the direct evaluation of trust. From the RREQ Algorithm Xrf,Xra and Xrs are the threshold values set for friends, acquaintances is too low. A Trust level is a function of various parameters like length of the association, ratio of the no. of packets forwarded successfully by the neighbor to the total no. of packets sent to that neighbor.

A. STRANGER

A Node has never sent/received messages to/from other node.Any new node entering ad hoc network will be a stranger to all its neighbors.There are high chances of malicious behavior from stranger nodes.

B. ACQUAINTANCE

A Node has sent/received few messages from other node. Their mutual trust level is neither too low nor too high to be reliable.The chances of malicious behavior will have to be observed**.**

C. FRIEND

A Node has sent/received few messages from other node. The trust levels between them are reasonably high probability of misbehaving nodes may be very less.

The nodes in an adhoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighbor node. From the RREQ ALGORITHM, Xrf, Xra and Xrs are the threshold values set for friends, acquaintances and strangers. The acquaintances and the stranger nodes won't forward the data packets, since the mutual trust level for the stranger and acquaintances is too low. Randomly selecting 5 selfish nodes in program coding. To differentiate from the selfish nodes from the normal nodes, reducing the quelength,for selfish nodes reducing the quelength to 2 and for normal nodes the quelength will be 300.The selfish nodes which has the quelength 2 does not forward the request. It will check the trust value, whether the node is a friend, stranger or compromised nodes. The friend node that has value ranging from 0.5 to 1 will forward the candidate. The friend node will be the best forwarder. Selfish nodes and compromised nodes will be neglected.

During route discovery phase of the DSR protocol, the extended system also computes the aggregate trust along different paths to the destination by the "path semiring" algorithm as proposed in [1]. From this, the most trusted path between the source and the destination is found out before establishing the data transfer. The segregation of the neighboring nodes into friends, acquaintances and strangers is the outcome of the direct evaluation of trust.

The lack of trusted environment in an ad hoc network results in many security lapses. This is considered as one of the major concerns in the large scale deployment of ad hoc networks [4]. Many trust establishment algorithms [5, 6, 7] have been developed which addresses few of the security attacks possible in an ad hoc network. The participating nodes should know in advance regarding the type of security attack in the network and run the corresponding algorithm to detect the misbehaving nodes in the network.

The Secure Ad hoc On-demand Distance Vector (SAODV) routing protocol presented in [8] is based on public key infrastructure which is not suitable for an ad hoc environment where there is no centralized infrastructure. Some of the cryptographic protocol schemes [9,10] presented clearly have the overheads associated with the secure routing at all times.

If X_{rs}, X_{ra}, X_{rf} be the RREQ flooding threshold for a stranger, acquaintance and friend node respectively, $X_{rf} > X_{ra} > X_{rs}$. If Y_{rs}, Y_{ra}, Y_{rf} be the DATA flooding threshold for stranger, acquaintance and friend node respectively then $Y_{rf} > Y_{ra} > Y_{rs}$.

D.RREQ ALGORITHM

Begin
If a node receives RREQ packet from node i then
1. if node 'I' is a friend and Y[i]=0 then
2. increment Y[i]
3. if Y[i]>Xrf
4. drop the RREQ packet and set Y[i]=1
5. else
6.forward the RREQ packet
7. if node'i' is an acquaintance and Y[i]=0 then
8.increment Y[i]
9. if Y[i]>Xra
10. drop the RREQ packet and set Y[i]=1
11.else
12. forward the RREQ packet
13. if node'i' is an stranger and Y[i]=0 then
14. increment Y[i]
15. If Y[i]>Xrs
16. drop the RREQ packet and set Y[i]=1
17.else
18. forward the RREQ packet
End

Let X[i] denotes the number of packets delivered from neighboring node i, where $1 \le i \le n$. X_{rf}, X_{ra} and X_{rs} are the threshold values set for friends, acquaintances and strangers. Let Z[i] is a Boolean array to activate or stop the prevention algorithm. The threshold values can be set as per the requirements of the application software. Each node starts at a random position and randomly moves to another position with a chosen velocity ranging from 0 m/s to 20 m/s. Random Waypoint model is chosen as the movement.

E.ADMISSION CONTROL

The number of transmitters on a route imposing interference upon a particular node on that route is termed as the node's contention count. In the 802.11 distributed co-ordination function (DCF) MAC scheme, transmissions are deferred if the channel is deemed busy, when the interference power exceeds a signal power-monitoring threshold called the carrier-sensing (CS) threshold.

CS neighbors [5], is termed as the nodes whose transmissions may actually cause each other to deem the channel busy. Before admitting any traffic, an accurate AC protocol should test whether the new traffic will be tolerable to each forwarding node's CS neighbors, since they would suffer increased interference, and hence, reduced channel access.

F.DEALING WITH NETWORK DYNAMICS

In the case of route failure, search for a new route or pause the packet generation and transmission at the data source of the affected sessions until a new route can be found, i.e., until the session is successfully readmitted. The protocol pro-posed in [12], multipath AC for MANETs (MACMAN), extends PAC [11] with a scheme that discovers and periodically tests the capacity of multiple disjoint routes to each admitted session's destination node. The protocol is related in the literature that combines AC that tests the CS-neighbor-hood's residual capacity with a mechanism to avoid restarting the admission process after route failure. Note also that, again, to the best of knowledge, only [9] and [10] have considered heterogeneous link rates in context of AC. However, these works did not improve upon the handling of mobility induced QoS constraint violations of the other protocols.

V. PERFORMANCE ANALYSIS AND SIMULATION RESULTS

A. PARAMETER ANALYSIS

The various simulation parameters used is shown in table1.In this paper, the number of nodes used for simulation is 40. DSR routing protocol is used in our simulation. The X-axis and Y-axis dimensions (range) are 1000. The time period given for the packet transmission is 0.5 to 200ms i.e., the simulation starts at 0.5 and the simulation stops at 200ms.

TABLE 1

Channel Type	Wireless Channel
Network Interface Type	Physical Interface
No. of nodes	40
Routing Protocol	DSR
X Dimension	1000
Y Dimension	1000
Start of Simulation Time	0.5
End of Simulation Time	100 sec

B. NETWORK SCENARIO

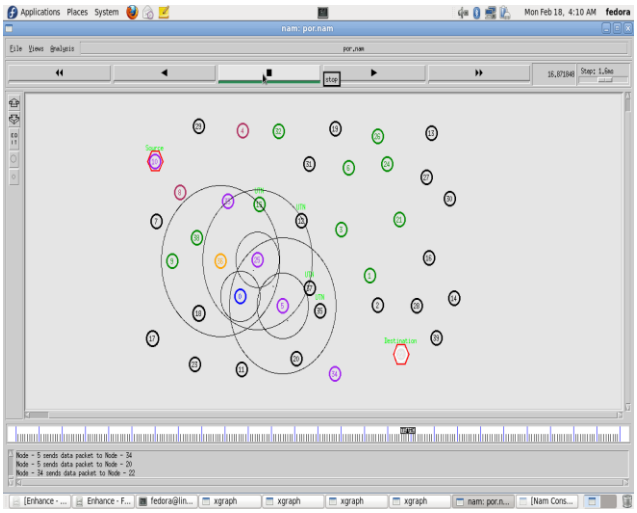

FIGURE 1. SELFISH NODES FROM NORMAL NODES

Here the node 12 sends route reply packet to node 33.The Node 33 sends route reply packet to node 10.The Node 10 sends data packet to node 33.

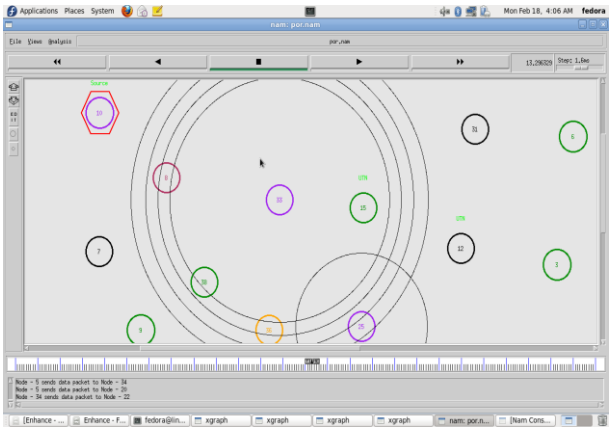

FIGURE 2. FLOODING BETWEEN NEIGHBOR NODES

Node 10 floods the Accusation message (alarm message) about the detection of malicious node in the network, to its neighbor 33.Node 10 floods the Accusation message about the detection of malicious node in the network, to its neighbor 29.Node 10 floods the Accusation message about the detection of malicious node in the network to its neighbor 8.

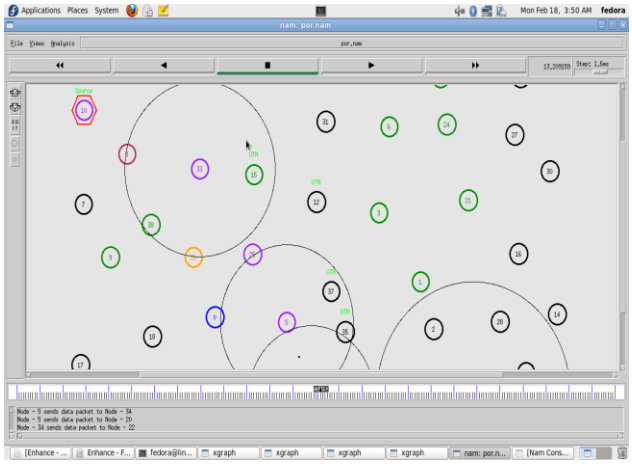

FIGURE 3. UNTRUSTABLE NODES

The black and Green Color nodes are untrustable nodes (Selfish Nodes).These nodes do not forward the request. Only the friend nodes whose range is from 0.5 to 1 will forward the candidates. Here the node 5 sends Route Reply packet to node 25.The Route Reply packet is not sent to selfish nodes since its quelength is less, avoiding the data transmission through untrustable nodes, the data transmission is done through the friend nodes.

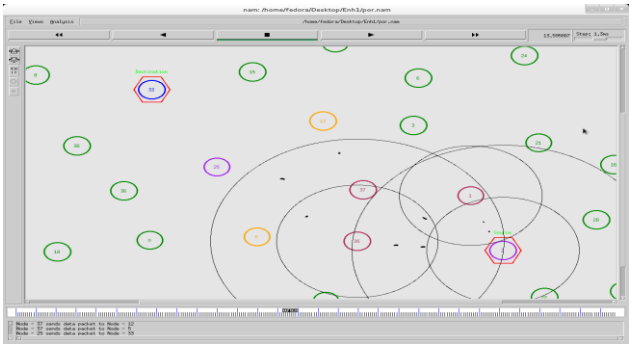

FIGURE 4. ADMISSION CONTROL

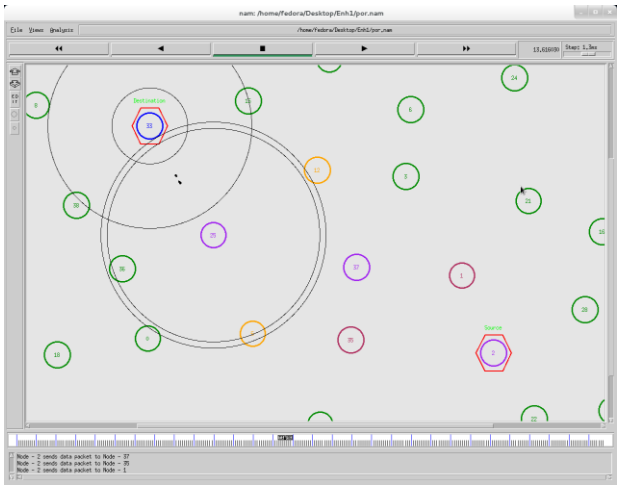

FIGURE 5. DROP RATE

The data rate is fixed among the nodes. If the date rate is not fixed, the nodes will check for the loss. By increasing the drop ratio, the data rate will not be fixed. The date rate will increase dynamically. The data packet is increased for each and every 10 seconds.

C. SIMULATION RESULTS

i. NETWORK THROUGHOUT

Throughput is the average rate of successful message delivery over a communication channel. Figure 6 shows the average rate of successful message delivery.

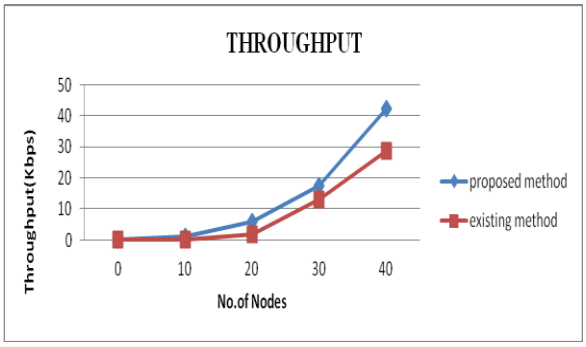

FIGURE 6. THROUGHPUT

ii. PACKET DROP

Packet loss is the total number of packets dropped during a transmission. As the number of nodes increases the number of packets dropping will also increase. The following shown figure 7 is the graphical representation of the packet loss as a function of number of nodes.

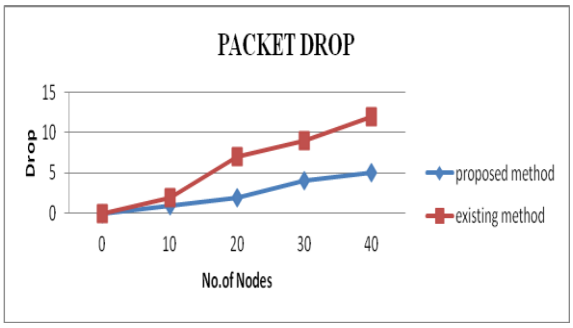

FIGURE 7. PACKET DROP

iii. PACKET DELIVERY RATIO

The ratio of the number of data packets received at the destinations to the number of data packets sent by the sources. The figure 8 shows the packet delivery ratio with respect to nodes.

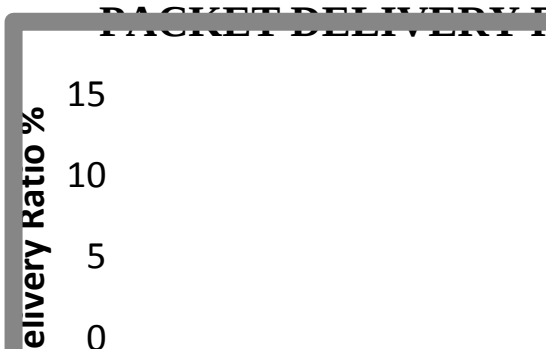

FIGURE 8. PACKET DELIVERY RATIO

iv PACKET DELAY

Packet delay is the difference in end-to-end delay between selected packets in a flow with any lost packets in a flow with any lost packets being ignored. This effect is sometimes referred to as gitter.

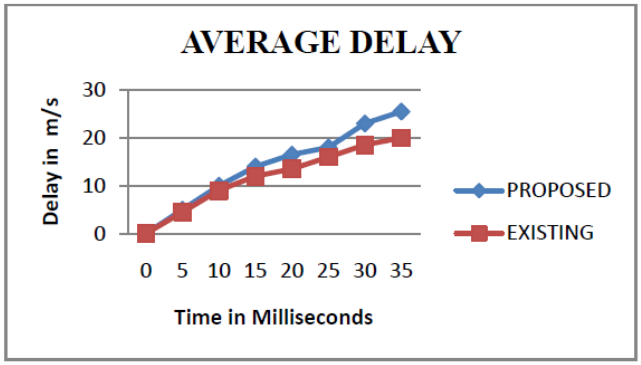

FIGURE 9. PACKET DELAY

D. CATEGORIZING THE NEIGHBORS (TRUST ESTIMATION)

The values from 0.5-1 means trustable, the values 0.3-0.5 means acquaintance and the values from 0-0.3 means stranger. The table 2 shows the neighbor relation between the nodes. For up to 0-39 nodes, the neighbor relation is achieved. The Nodes which has the trustable threshold values will be considered as the best forwarder. The table 3 shows stranger nodes which is not trustable and data will not be forwarded to that node. The stranger nodes have the high probability of becoming malicious node. The data forwarding will be neglected to these nodes.

TABLE 2 STRANGER NODES

NODE	NEIGHBOR-ID	RELATIONSHIP	RANGE
1	2	S	0
2	1	S	0
3	1	S	0
3	31	S	0
6	19	S	0
6	31	S	0
7	10	S	0
8	10	S	0
12	31	S	0
15	31	S	0
16	1	S	0

The table 3 shows the Acquaintance node where their mutual trust level will be neither too low nor too high. It will send or receive few messages to/from other node. The chances of malicious behavior will have to be observed.

TABLE 3 ACQUAINTANCE NODES

NODE	NEIGHBOR-ID	RELATIONSHIP	RANGE
1	2	A	0.6
2	28	A	0.6
4	32	A	0.6
14	28	A	0.6
15	32	A	0.6
16	28	A	0.6
19	32	A	0.6
21	28	A	0.6
22	28	A	0.6
31	32	A	0.6
38	34	A	0.6
39	28	A	0.6

The table 4 shows the friend node that will send few messages from other node. The trust levels between them are reasonably high. The probability of misbehaving nodes may be very less. The friend node that has higher trust value is considered as the best forwarder. The other nodes which are stranger and acquaintance will be neglected since they have lower trust value. In the case of stranger node the trust value will be too low.

TABLE 4 FRIEND NODE (Best Forwarder)

NODE	NEIGHBOR-ID	RELATIONSHIP	RANGE
0	5	F	1
0	11	F	1
0	18	F	1
0	23	F	1
0	25	F	1
0	36	F	1
1	3	F	1
1	16	F	1
1	21	F	1
1	35	F	1
1	37	F	1
2	22	F	1
2	34	F	1
2	35	F	1
2	39	F	1
3	6	F	1
3	12	F	1
3	21	F	1
3	24	F	1
3	37	F	1
4	8	F	1
4	15	F	1
4	29	F	1
4	33	F	1
5	0	F	1
5	11	F	1
5	12	F	1
5	20	F	1
5	25	F	1
5	26	F	1
5	35	F	1
5	37	F	1
6	3	F	1
6	12	F	1
6	21	F	1
6	21	F	1
6	24	F	1
6	26	F	1
7	8	F	1
7	9	F	1
7	38	F	1
8	4	F	1
8	7	F	1
8	9	F	1
8	29	F	1
8	33	F	1
8	38	F	1
9	7	F	1
9	8	F	1
9	17	F	1

9	18	F	1
9	36	F	1
9	38	F	1
10	7	F	1
10	8	F	1
10	29	F	1
11	0	F	1
11	5	F	1
11	18	F	1
11	20	F	1
11	23	F	1
12	3	F	1
12	5	F	1
12	6	F	1
12	15	F	1
12	25	F	1
12	35	F	1
12	37	F	1
12	24	F	1
13	26	F	1
13	27	F	1
13	30	F	1
14	16	F	1
14	30	F	1
14	39	F	1
15	4	F	1
15	12	F	1
15	35	F	1
15	33	F	1
16	14	F	1

VI. CONCLUSION

The efficiency of the involvement of forwarding candidates against node mobility, as well as the overhead due to opportunistic forwarding is analyzed. Through simulation, the effectiveness and efficiency of POR is confirmed: high packet delivery ratio is achieved while the delay and duplication are the lowest. On the other hand, inherited from geographic routing, the problem of communication void is also investigated. By temporarily adjusting the direction of data flow, the advantage of greedy forwarding as well as the robustness brought about by opportunistic routing can still be achieved when handling communication voids. In the operation of POR, the best forwarder that is elected is not checked whether it is secured or not.

So in the enhancement work, the trust value is estimated among the nodes. The friend node that has trust value ranging from 0.5 to 1 will be elected as the best forwarder. The other nodes which are selfish and compromised will be neglected. Further enhancement will lead to the admission control. The drop ratio is increased by not keeping the data as constant. The data rate will increase dynamically depending upon the loss.

REFERENCES

[1] Broch J., D.A. Maltz D.A.,. Johnson D.B, Hu Y.-C., and Jetcheva J., (1998) “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols,” Proc. ACM MobiCom, pp. 85-97.

[2] Mauve M., Widmer A., and Hartenstein H.,(Nov./Dec.2001) “A Survey on Position-Based Routing in Mobile Ad Hoc Networks,” IEEE Network, vol. 15, no. 6, pp. 30-39.

[3] Chen D., and Varshney P., (Jan-Mar.2007) “A Survey of Void Handling Techniques for Geographic Routing in Wireless Networks,” IEEE Comm. Surveys and Tutorials, vol. 9, no. 1, pp. 50-67.

[4] Son Z., Helmy A., and Krishnamachari B.,(July/Aug.2004) “The Effect of Mobility Induced Location Errors on Geographic Routing in Mobile Ad Hoc Sensor Networks: Analysis and Improvement Using Mobility Prediction,” IEEE Trans. Mobile Computing, vol. 3, no. 3, pp. 233-245.

[5] Karp B., and Kung H.T., (2000) “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks,” Proc. ACM MobiCom, pp. 243-254.

[6] Rozner E., Seshadri J., Mehta Y., and Qiu L., (Dec.2009) “SOAR: Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh Networks,” IEEE Trans. Mobile Computing, vol. 8, no. 12 pp. 1622-1635, Dec. 2009.

[7] Balasubramanian A., Mahajan R., Venkataramani A., Levine B.N, and Zahorjan J., (2008) “Interactive WiFi Connectivity for Moving Vehicles,” Proc. ACM SIGCOMM, pp. 427-438, 2008.

[8] Zeng K., Yang Z., and Lou W., (July 2009) “Location-Aided Opportunistic Forwarding in Multirate and Multihop Wireless Networks,” IEEE Trans. Vehicular Technology, vol. 58, no. 6, pp. 3032-3040, July 2009.

[9] Das S., Pucha S., and Y. Hu, (Mar.2005) “Performance Comparison of Scalable Location Services for Geographic Ad Hoc Routing,” Proc. IEEE INFOCOM, vol. 2, pp. 1228-1239.

[10] Flury R., and Wattenhofer R.,(2006) “MLS: An Efficient Location Service for Mobile Ad Hoc Networks,” Proc. ACM Int’l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 226-237.

[11] Felemban E., Lee C.-G., Ekici E., Boder R., and Vural S.,(2005) “Probabilistic QoS Guarantee in Reliability and Timeliness Domains in Wireless Sensor Networks,” Proc. IEEE INFOCOM, pp. 2646-2657.

[12] Chen D., Deng J., and Varshney P., (Sept.2007) “Selection of a Forwarding Area for Contention-Based Geographic Forwarding in Wireless Multi-Hop Networks,” IEEE Trans. Vehicular Technology, vol. 56, no. 5, pp. 3111-3122.

[13] Arad N., and Shavitt Y.,(Feb.2009) “Minimizing Recovery State in Geographic Ad Hoc Routing,” IEEE Trans. Mobile Computing, vol. 8, no. 2, pp. 203-217.

[14] Han Y., R. La, Makowski A., and Lee S.,(2006) “Distribution of Path Durations in Mobile Ad-Hoc Networks - Palm’s Theorem to the Rescue,” Computer Networks, vol. 50, no. 12, pp. 1887-1900.

[15] Navidi W., and Camp T., (Jan/Feb.2004) “Stationary Distributions for the Random Waypoint Mobility Model,” IEEE Trans. Mobile Computing, vol. 3, no. 1, pp. 99-108.

[16] Y. Han, R. La, A. Makowski, and S. Lee, “Distribution of PathDurations in Mobile Ad-Hoc Networks - Palm’s Theorem to the Rescue,” Computer Networks, vol. 50, no. 12, pp. 1887-1900, 2006.

[17] W. Navidi and T. Camp, “Stationary Distributions for the Random Waypoint Mobility Model,” IEEE Trans. Mobile Computing, vol. 3,no. 1, pp. 99-108, Jan./Feb. 2004.

[18] R. Groenevelt, “Stochastic Models for Mobile Ad Hoc Networks,”PhD dissertation, Universite de Nice, Sophia Antipolis, France,2005.

[19] The Network Simulator ns-2, http://www.isi.edu/nsnam/ns,2011.

[20] M. Marina and S. Das, “On-Demand Multipath Distance Vector Routing in Ad Hoc Networks,” Proc. Ninth Int’l Conf. Network Protocols (ICNP ’01), pp. 14-23, Nov. 2001.

[21] J. Yoon, M. Liu, and B. Noble, “Random Waypoint Considered Harmful,” Proc. IEEE INFOCOM, pp. 1312-1321, 2003.

[22] S. Mueller, R. Tsang, and D. Ghosal, “Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges,” Performance Tools and Applications to Networked Systems, pp. 209-234, Springer, 2004.

[23] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, “Highly Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks,” ACM SIGMOBILE Mobile Computing and Comm. Rev.,vol. 5, no. 4, pp. 11-25, 2001.

[24] A. Valera, W. Seah, and S. Rao, “Improving Protocol Robustness in Ad Hoc Networks through Cooperative Packet Caching and Shortest Multipath Routing,” IEEE Trans. Mobile Computing, vol. 4, no. 5, pp. 443-457, Sept./Oct. 2005.

[25] B. Deb, S. Bhatnagar, and B. Nath, “ReInForM: Reliable Information Forwarding Using Multiple Paths in Sensor Networks,” Proc.Ann. IEEE Int’l Conf. Local Computer Networks (LCN ’03), pp. 406-415, 2003.